Doctoral Dissertation

A Study on Statistical Cryptanalysis of Stream Ciphers

（ストリーム暗号の統計解析に関する研究）

February 2019

Graduate School of Engineering,
Osaka University

Ryoma Ito

Supervisor: Professor Atsuko Miyaji

Doctoral Dissertation

A Study on Statistical Cryptanalysis of Stream Ciphers

（ストリーム暗号の統計解析に関する研究）

February 2019

Graduate School of Engineering,
Osaka University

Ryoma Ito

Supervisor: Professor Atsuko Miyaji

Abstract

A *stream cipher* is often used as a cryptographic scheme for processing communication data at a high speed. Therefore, it is important to evaluate the security of stream ciphers in keeping with the background that high-speed data processing is required with the development of the advanced information and communications society.

This dissertation presents *a study on statistical cryptanalysis of stream ciphers*, and focuses particularly on RC4. First of all, we investigate certain events with statistical weakness known as a *bias* or a *correlation* involving the secret key, the internal state, or the pseudorandom number sequence called the *keystream* of RC4. We then apply new events with statistical weakness to the existing attacks, for example, a plaintext recovery attack, a key recovery attack, and a state recovery attack, and attempt to improve them. Finally, we propose a countermeasure to avoid the occurrence of the events with statistical weakness, especially in WPA-TKIP, which uses RC4 stream cipher for encryption/decryption. Our purpose in this dissertation is to contribute to security evaluations of stream ciphers through cryptanalysis of RC4 in the future.

In Chapter 4, we focus on *Glimpse Correlations* between the keystream and the internal state. The existing Glimpse Correlations provide only cases with positive biases, and hold generally on any round. We then refine the existing Glimpse Correlations from two approaches. One is to investigate certain events with positive or negative biases on all values in addition to a known value in the existing Glimpse Correlations. The other is to investigate certain events with different biases on specific rounds from the new and existing Glimpse Correlations. As a result of our investigation, we provide six events with several new biases, and prove these events theoretically.

In Chapter 5, we investigate correlations between the unknown internal state and the *public* RC4 key in WPA-TKIP, which are referred to as *key correlations of the internal state variables*. One of the remarkable features of WPA-TKIP is that the first three bytes of the RC4 key are set from the *public* parameters, and our investigation uses this feature. As a result of our investigation, we provide 22 events with key correlations of the internal state variables, and prove these events theoretically. Our theoretical proofs make clear how TKIP induces biases in the internal state of generic RC4. We then discuss a countermeasure toward secure RC4 key setting in WPA-TKIP in such a way that it can retain the security level of generic RC4. As a result of our discussion, we demonstrate that the number of key correlations induced by our refined RC4 key setting can be reduced by approximately 70% in comparison with that in the original setting in WPA-TKIP.

In Chapter 6, we investigate correlations between two bytes of the RC4 key and the keystream in each round, where the RC4 key pairs are *iterated* every specific rounds. Such correlations are referred to as the *iterated RC4 key correlations*. As a result of our investigation, we prove new events with the iterated RC4 key correlations theoretically. Furthermore, we apply new events with the iterated RC4 key correlations to the existing plaintext recovery attacks on WPA-TKIP. As a result of our experiments, we achieve to recover the first 257 bytes of a plaintext on WPA-TKIP from approximately 2^{30} ciphertexts with a success probability of approximately 90.8%, whose probability is approximately 6.0% higher than a success probability of the existing best attack.

Finally, we conclude by summarizing our results and future works, and provide a direction to construct secure stream ciphers generally based on our statistical cryptanalysis of RC4 stream cipher.

Acknowledgments

I would like to thank everyone who has supported me to pursue my PhD.

First of all, I would like to express my gratitude to my supervisor, Professor Atsuko Miyaji. She kindly accepted me as a working adult student, and gave me the opportunity to study on *statistical cryptanalysis of stream ciphers* as my research topic. I appreciate her invaluable support and guidance through the hard moments of graduate school.

I also would like to express my gratitude to the members of my examination committee, Professor Tetsuya Takine, Professor Noboru Babaguchi, Professor Kyo Inoue, Professor Seiichi Sampei, Professor Takashi Washio, Professor Akihiro Maruta, Professor Kazunori Komatani, and Associate Professor Akinori Kawachi, for reviewing my dissertation and giving me valuable feedbacks. A very special thanks goes to Professor Serge Vaudenay from École Polytechnique Fédérale de Lausanne in Switzerland, who is a member of my examination committee. He also took time to review my dissertation from his busy schedule and give me valuable feedbacks from a remote location.

I would like to thank Professor Yasuhiro Nakamura and Associate Professor Munetoshi Iwakiri, who are staff members of Software Engineering Laboratory in National Defense Academy (NDA). When I was a researcher at their laboratory in 2012, they taught me basic things required for a cryptographic researcher such as knowledge on information security including cryptography, programming techniques, how to read and write academic papers, and how to approach from finding problems to solving them.

I would like to thank Associate Professor Kazumasa Omote, Associate Professor Yuichi Futa, Associate Professor Jiageng Chen, Associate Professor Chunhua Su, and Assistant Professor Satoru Tanaka, who were staff members of Miyaji Laboratory when I was enrolled in Japan Advanced Institute of Science and Technology, for giving me helpful comments in our discussions.

I would like to thank Associate Professor Hidema Tanaka from NDA. If he had not strongly recommended me to pursue my PhD, this dissertation might not have existed.

I am thankful to my superiors, colleagues, and subordinates in my workshop at Japan Air Self-Defense Force, Ministry of Defense, Japan. Thanks to their support and encouragement, I was able to pursue my PhD as a working adult student.

Finally, I am thankful to my family for their longtime support through my life. Especially, I deeply appreciate my wife Sayaka for understanding my dream and encouraging me every day.

Contents

List of Figures

List of Tables

List of Symbols

K	secret key: $\{K[0], K[1], \ldots, K[\ell-1]\}$
ℓ	key size (typically, $\ell = 16$ bytes)
r	the number of rounds
S	internal state: $\{S[0], S[1], \ldots, S[N-1]\}$
N	the number of arrays in S (typically, $N = 2^8$)
S_r^K	S of the KSA in the r-th round: $\{S_r^K[0], S_r^K[1], \ldots, S_r^K[N-1]\}$
S_r	S of the PRGA in the r-th round: $\{S_r[0], S_r[1], \ldots, S_r[N-1]\}$
i, j_r^K	indices of S_r^K
i_r, j_r	indices of S_r
Z_r	the r-th keystream byte
t_r	index of Z_r
P_r	the r-th plaintext byte
C_r	the r-th ciphertext byte
$\gg$	bitwise right shift operator
$\|$	bitwise OR operator
&	bitwise AND operator

Chapter 1

Introduction

1.1 Motivation

Recently, with the development of the advanced information and communications society, the use of mobile information and communication devices, e.g., smartphones and tablet computers, has been widely spreading, and the public wireless LAN service area has also been widely expanding. Thanks to this society, anyone can easily communicate a large amount of data via the Internet at any time or place.

However, we must continuously deal with various problems related to the use of the Internet. One of the problems is that threats of cyber-attacks by malicious third parties, called *adversaries*, are increasing. Actually, we have many opportunities to deal with confidential information in communications via the Internet, e.g., internet shopping, internet banking, and electronic voting, and therefore need to take measures to ensure information security in order to protect our confidential information from adversaries. One of the measures to ensure information security includes *cryptography*.

1.1.1 Cryptography

For the formal definition of cryptography, we refer to the *Handbook of Applied Cryptography* by Menezes et al. in [MOV96, Definition 1.1] as follows:

> *Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.*

Cryptography is roughly divided into *symmetric key cryptography* and *asymmetric key cryptography*. Symmetric key cryptography uses the same secret key for encryption and decryption. It has a disadvantage that the same secret key must be pre-shared securely with the communication partner, but it has an advantage that the encryption/decryption processing can be performed at a high speed by using only simple logical and arithmetic operations.

On the contrary, asymmetric key cryptography uses different keys (a secret key and a public key) for encryption and decryption. It has an advantage that the different keys need not be pre-shared with the communication partner, but it has a disadvantage that the encryption/decryption processing is performed at a lower speed than that in symmetric key cryptography.

This dissertation will focus on symmetric key cryptography in keeping with the background that it is required to increase communication speeds owing to the large scale of the advanced information and communications society.

1.1.2 Symmetric Key Cryptography

Symmetric key cryptography is further divided into *block ciphers* and *stream ciphers* for ensuring confidentiality of information. A block cipher divides a plaintext/ciphertext into fixed-length blocks, and encrypts/decrypts one block at a time using the same secret key according to the modes of operation, e.g., electronic codebook (ECB) mode, cipher-block chaining (CBC) mode, cipher feedback (CFB) mode, and output feedback (OFB) mode (refer to [MOV96] for details). Representative block ciphers include DES [oS77], AES [DR99], Camellia [AIK+01], MISTY [Mat97], and SIMON/SPECK [BTCS+15].

A stream cipher generates an arbitrary-length pseudorandom number sequence called a *keystream* using the secret key, and encrypts/decrypts one bit or one byte at a time by XORing the plaintext/ciphertext and the keystream. Representative stream ciphers include RC4 [Ano94], HC-128 [Wu08], Rabbit [BVZ08], Salsa20/12, [Ber08b], ChaCha20 [Ber08a, Ber08c], SOSEMANUK [BBC+08], Grain v1 [HJMM08], MICKEY [BD08], and Trivium [Can08].

Stream ciphers have an advantage that the encryption/decryption processing can be performed at a higher speed than that in block ciphers. Therefore, this dissertation will focus on stream ciphers and particularly on RC4, which is one of the representative stream ciphers, and is still widely used today. Our motivation in this dissertation is to contribute to security evaluations of all stream ciphers through cryptanalysis of RC4.

1.1.3 RC4 Stream Cipher

RC4 stream cipher, designed by Ronald L. Rivest in 1987, is widely used in various security protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS), Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access Temporal Key Integrity Protocol (WPA-TKIP).

SSL/TLS adopts RC4 as a standard stream cipher for confidentiality of information, and provides secure communications via the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery [DA98, DR06, DR08, FKK11]. SSL was developed by Netscape Corporation in the middle of 1990s [FKK11]. After that, the TLS working group of the Internet Engineering Task Force (IETF) released TLS 1.0 as RFC 2246 in 1999 [DA98] and TLS 1.1 as RFC 4346 in 2006 [DR06]. Then, the current version TLS 1.2 was published as RFC 5246 in 2008 [DR08].

WEP and WPA-TKIP adopt RC4 for confidentiality of information, and provide secure communications via Wi-Fi networks between clients and access points. In 1999, WEP was

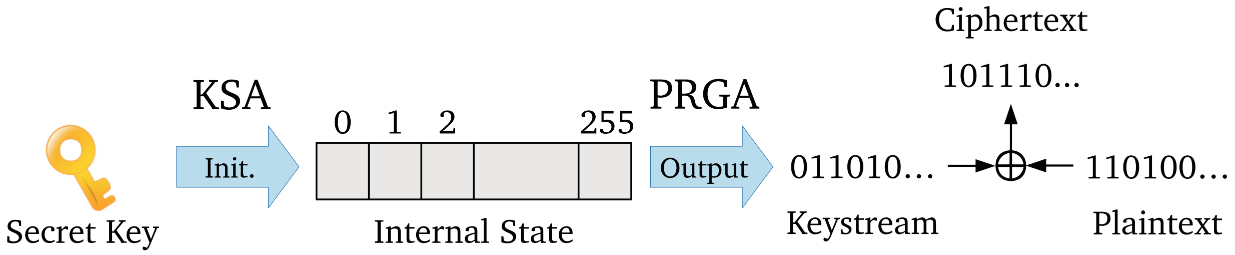

Figure 1.1: Encryption process by the RC4 stream cipher.

developed to achieve a equivalent level of confidentiality to wired local area network (LAN) medium that does not use cryptographic schemes [Soc04]. A practical attack against WEP, however, was proposed by Fluhrer et al. in 2001 [FMS01], and WEP is considered to be broken today. In order to prevent the existing attack by Fluhrer et al. [FMS01], WEP had been superseded by WPA in 2003 [Soc04]. WPA improves secret key setting in WEP, and adopts TKIP as a countermeasure against the existing attack (refer to Sections 2.3 and 2.4 for details).

RC4 consists of two algorithms: a *Key Scheduling Algorithm* (KSA) and a *Pseudo Random Generation Algorithm* (PRGA). The KSA generates a secret initial state to become an input of the PRGA from a secret key, and then the PRGA outputs one byte of the keystream at a time. After that, the keystream is XORed with a plaintext/ciphertext to obtain a ciphertext/plaintext (see Figure 1.1).

After the disclosure of RC4 algorithms in 1994 [Ano94], RC4 has been intensively analyzed over the past two decades, owing to its popularity and simplicity. There are mainly two approaches to the cryptanalysis of RC4. One is to demonstrate the existence of a certain event with *statistical weakness* known as a *bias* or a *correlation* involving the secret key bytes, the internal state variables, or the keystream bytes. Now, we refer to an event with significantly higher or lower probability than the probability of random association as a *positive bias* or a *negative bias*, respectively. The other approach is to recover a plaintext (a *plaintext recovery attack*), an RC4 key (a *key recovery attack*), and an internal state (a *state recovery attack*) by using various biases or correlations. In addition, many cryptanalyses on the security protocols have been reported, such as plaintext recovery attacks on SSL/TLS and WPA-TKIP, and key recovery attacks on WEP (refer to Chapter 3 for details).

Owing to the influence of the above cryptanalyses, the usage of RC4 cipher suites was prohibited in all SSL/TLS versions in 2015 [Pop15], and was also recommended in neither WEP nor WPA-TKIP. Actually, the IETF adopts ChaCha20 cipher suites from the current version TLS 1.2 [DR08, LCM$^+$16] as the TLS standard stream cipher, and abolishes RC4 cipher suites from the next version TLS 1.3 [DR18]. Currently, however, approximately 15.1% of all web browsers/servers for SSL/TLS continue to support RC4 cipher suites as of February 2019 [SSL], and downgrade attacks in Wi-Fi networks remain as real threats [VP16, VSP17].

In summary, many people may continue to use RC4 in the security protocols, and we therefore need to pay attention to RC4 from now on.

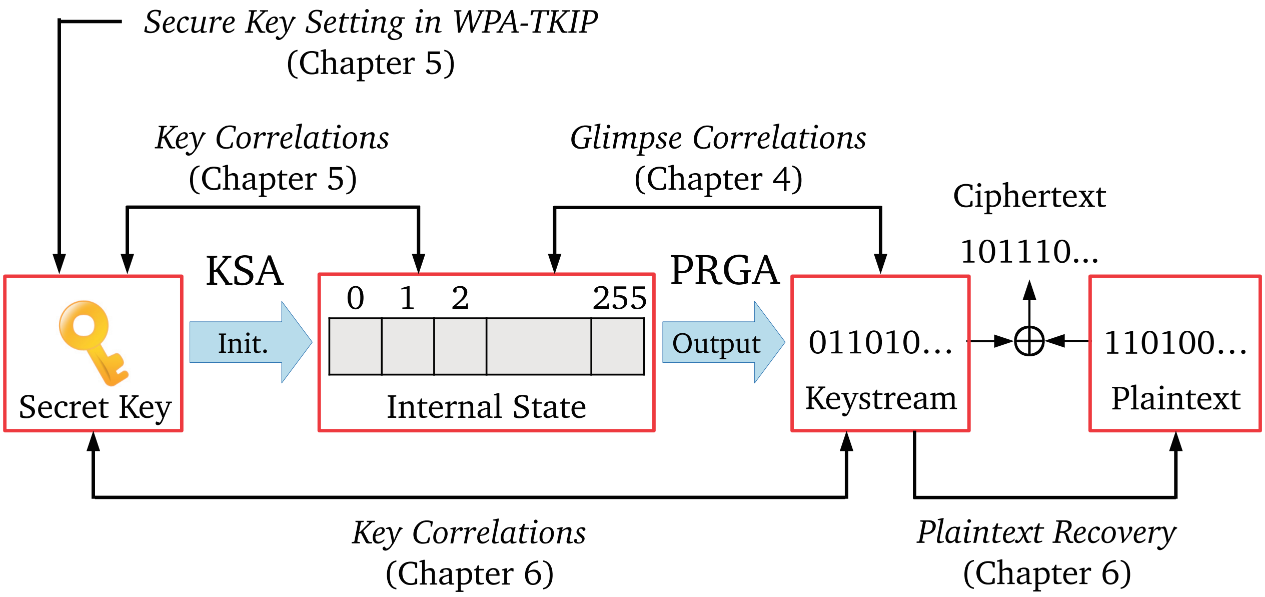

Figure 1.2: Visualization of our contributions.

1.2 Contributions

This dissertation deals with *a study on statistical cryptanalysis of stream ciphers*, and focuses particularly on RC4. Our cryptanalysis will be further extended to security evaluations of RC4-like stream ciphers, e.g., RC4+ [MP08a], RC4A [PP04], VMPC [Zol04], NGG [NGG05], GGHN [GGHN05], and Spritz [RS14], and other stream ciphers [Wu08, BVZ08, Ber08b, Ber08a, Ber08c, BBC$^+$08, HJMM08, BD08, Can08]. Our contributions can be summarized as the following three chapters (see Figure 1.2).

Chapter 4: Refined Glimpse Correlations

Publications included in this chapter are a journal paper and an international conference paper as follows:

- Ryoma Ito and Atsuko Miyaji. New Integrated Long-Term Glimpse of RC4. In Kyung-Hyune Rhee and Jeong Hyun Yi, editors, *Information Security Application - WISA 2014*, volume 8909 of *Lecture Notes in Computer Science*, pages 137–149. Springer Berlin Heidelberg, 2015. (**Ref.** [IM14a])
- Ryoma Ito and Atsuko Miyaji. Refined Glimpse Correlations of RC4. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(1):3–13, January 2016. (**Ref.** [IM16a])

This chapter investigates two types of existing *Glimpse Correlations*: the *Glimpse Theorem* and the *Long-term Glimpse*. In [Jen96], Jenkins discovered correlations between a keystream byte and an internal state variable, which are known as the Glimpse Theorem. In [MG13], Maitra and Sen Gupta proved the Glimpse Theorem completely, and presented other correlations between two consecutive keystream bytes and an internal state variable, which are known as the Long-term Glimpse. The existing Glimpse Correlations provide only cases with positive biases, and hold generally on any round. In this chapter, we refine the existing Glimpse Correlations from the following two approaches: One is to find new positive or negative biases on all values in addition to a known value. The other is to provide precise biases on specific rounds. As a result, we discover six cases with several new biases, and prove these cases theoretically. In the first approach, combining our new biases with the existing ones, the Long-term Glimpse is integrated with positive biases. In the second approach, we successfully find that two correlations on specific rounds become an impossible condition, whose probability is 0.

Chapter 5: Key Correlations of the Internal State Variables

Publications included in this chapter are two journal papers and two international conference papers as follows:

- Ryoma Ito and Atsuko Miyaji. New Linear Correlations Related to State Information of RC4 PRGA Using IV in WPA. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 557–576. Springer Berlin Heidelberg, 2015. (**Ref.** [IM15c])
- Ryoma Ito and Atsuko Miyaji. How TKIP Induces Biases of Internal States of RC4. In Emest Foo and Douglas Stebila, editors, *Information Security and Privacy - ACISP 2015*, volume 9144 of *Lecture Notes in Computer Science*, pages 329–342. Springer International Publishing, 2015. (**Ref.** [IM15a])
- Ryoma Ito and Atsuko Miyaji. Refined RC4 Key Correlations of Internal States in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(6):1132–1144, June 2016. (**Ref.** [IM16b])
- Ryoma Ito and Atsuko Miyaji. Refined Construction of RC4 Key Setting in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E100-A(1):138–148, January 2017. (**Ref.** [IM17])

This chapter discusses the weaknesses in WPA-TKIP. One of the remarkable features in WPA-TKIP is that the first three bytes of the RC4 key are derived from public parameters, and an existing work using this feature was reported by Sen Gupta et al. in [GMM$^+$14]. They focused on correlations between the known RC4 key bytes in WPA-TKIP and the keystream bytes, which are referred to as *key correlations of the keystream bytes*, and improved an existing plaintext recovery attack by Isobe et al. in [IOWM13] using their discovered key correlations. No study, however, has focused on such correlations including the unknown internal state variables in WPA-TKIP. We then investigate new correlations between the unknown internal state variables and the first three bytes of the RC4 key in both generic RC4 and WPA-TKIP, which are referred to as *key correlations of the internal state variables*, and provide theoretical proofs of 22 key correlations we discovered. Our theoretical proofs make clear how TKIP induces biases in the internal state of generic RC4. Ideally, WPA-TKIP should be constructed in such a way that it can retain the original security level of generic RC4. We then discuss secure RC4 key setting in WPA-TKIP in such a way that it can retain the security level of generic RC4. If the RC4 key setting in WPA-TKIP is refined, it can be difficult to induce key correlations of the keystream bytes or the internal state variables. As a result, we present that the number of key correlations induced by our refined RC4 key setting can be reduced by approximately 70% in comparison with that in the original setting in WPA-TKIP. Our cryptanalysis would also be useful to investigate a generic construction of a secret key setting including the public parameters in such a way that it can retain the security level of the original encryption.

Chapter 6: Iterated RC4 Key Correlations of the Keystream Bytes

Publications included in this chapter are an international conference paper and a domestic conference paper as follows:

- Ryoma Ito and Atsuko Miyaji. New Iterated RC4 Key Correlations. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy - ACISP 2018*, volume 10946 of *Lecture Notes in Computer Science*, pages 154–171. Springer International Publishing, 2018. (**Ref.** [IM18a])

- Ryoma Ito and Atsuko Miyaji. Plaintext Recovery Attacks against WPA-TKIP Using Iterated RC4 Key Correlations. In *IEICE Japan Technical Report - ISEC 2018*, ISEC 2018–48, pages 379–386, 2018–7. (**Ref.** [IM18c])

This chapter investigates key correlations of the keystream bytes, and then discusses significant improvements for plaintext recovery on WPA-TKIP from the existing attacks. We discuss new correlations between the RC4 key pair and a keystream byte in each round, where the RC4 key pairs in the correlations are *iterated* every specific rounds. Such correlations are referred to as the *iterated RC4 key correlations*. We further discuss how to apply key correlations of the keystream bytes to the plaintext recovery attack from the following three approaches. The first is to extend an existing attack by Isobe et al. in [IOWM13] in the same way as an existing attack by Sen Gupta et al. in [GMM$^+$14]. In this approach, we achieve significant improvement for recovering eight bytes of a plaintext on WPA-TKIP using our iterated RC4 key correlations from the existing attack in [IOWM13]. The second is to improve an existing attack by AlFardan et al. in [ABP$^+$13] using key correlations of the keystream bytes. In this approach, we achieve significant improvement for recovering five bytes of a plaintext on WPA-TKIP from existing attacks in [IOWM13, ABP$^+$13, PPS14]. The last is to optimize the plaintext recovery of the first 257 bytes on WPA-TKIP by combining ours and the existing attacks. In this approach, we achieve to recover the first 257 bytes of a plaintext on WPA-TKIP from approximately 2^{30} ciphertexts with a success probability of approximately 90.8%, whose probability is approximately 6.0% higher than a success probability of an existing attack by Paterson et al. in [PPS14]. Our result implies that WPA-TKIP further lowers the security level of generic RC4.

1.3 Organization of This Dissertation

The remainder of this dissertation is organized as follows:

- **Chapter 2** describes the outline of stream cipher, the description of RC4, the secret key setting in WEP and WPA-TKIP, and statistical methods as *preliminaries* for our cryptanalysis and discussions.

- **Chapter 3** describes some useful theorems, lemmas, and attack procedures in the *previous works*, which are used in our cryptanalysis and discussions.

- **Chapter 4** presents new results on the *Refined Glimpse Correlations*. We first show our experimental observations of the Glimpse Correlations, and then demonstrate theoretical proofs of the new results. We finally show our experimental evaluations to confirm the accuracy of our proofs.

- **Chapter 5** presents new results on *key correlations of the internal state variables*. We first show our experimental observations of the key correlations, and then demonstrate theoretical proofs of the new results. Next, we show our experimental evaluations to confirm the accuracy of our proofs, and finally discuss secure RC4 key setting in WPA-TKIP.

- **Chapter 6** presents new results on *iterated RC4 key correlations of the keystream bytes*. We first show our experimental observations of the iterated RC4 key correlations, and then demonstrate theoretical proofs of the new results. Next, we show our experimental evaluations to confirm the accuracy of our proofs, and finally discuss improvements for plaintext recovery on WPA-TKIP.

- **Chapter 7** concludes this dissertation by summarizing our results and future works.

Chapter 2

Preliminaries

2.1 Stream Cipher

A stream cipher is a function that outputs an arbitrary-length keystream from a secret key and an initialization vector (IV) as inputs, and provides confidentiality of information. Generally, the XOR operation is used for encryption/decryption by stream ciphers, and thus a ciphertext/plaintext is derived by XORing a plaintext/ciphertext and a keystream. For the formal definition of a stream cipher, we refer to the doctoral dissertation of Isobe in [Iso13] as follows:

Definition 2.1 ([Iso13, Definition 6])**.** *A* **stream cipher** *is a function such that a mapping* $S : \{0,1\}^k \times \{0,1\}^c = \{0,1\}^\ell$*, where* k *is a key size,* c *is an IV size, and* ℓ *is a keystream size.*

2.1.1 Security Level

Because the stream cipher works as a *pseudorandom generator*, its security level must satisfy the following definition of the pseudorandom generator (refer to [KL07] for details):

Definition 2.2 ([KL07, Definition 3.15])**.** *Let* $\ell(\cdot)$ *be a polynomial and let* G *be a deterministic polynomial-time algorithm such that upon any input* $s \in \{0,1\}^n$*, algorithm* G *outputs a string of length* $\ell(n)$*. We say that* G *is a* **pseudorandom generator** *if the following two conditions hold:*

1. *Expansion: For every* n*, it holds that* $\ell(n) > n$*.*

2. *Pseudorandomness: For all probabilistic polynomial-time distinguishers* D*, there exists a negligible function* `negl` *such that:*

$$|\Pr[D(r) = 1] - \Pr[D(G(s)) = 1]| \leq \mathtt{negl}(n), \tag{2.1}$$

where r *is chosen uniformly at random from* $\{0,1\}^{\ell(n)}$*, the seed* s *is chosen uniformly at random from* $\{0,1\}^n$*, and the probabilities are taken over the random coin used by* D *and the choice of* r *and* s*.*

2.1.2 Attack Scenarios

We describe the following attack scenarios of stream ciphers (refer to [KL07, MOV96] for details):

Ciphertext-only Attack: An adversary obtains only a ciphertext, and tries to determine the corresponding plaintext.

Known Plaintext Attack: An adversary obtains one or more pairs of plaintexts/ciphertexts encrypted under the same secret keys, and tries to determine the corresponding plaintext from another obtained ciphertext.

Chosen Plaintext Attack: An adversary has the ability to obtain the corresponding ciphertext(s) of arbitrary plaintext(s), and tries to determine the corresponding plaintext from an obtained ciphertext.

Chosen Ciphertext Attack: An adversary has the ability to obtain the corresponding plaintext(s) of arbitrary ciphertext(s), and tries to determine the corresponding plaintext from another ciphertext obtained without using the ability.

Note that an adversary has the ability to obtain the corresponding keystream by XORing a pair of plaintext and ciphertext, except under the scenario of the ciphertext-only attack.

2.1.3 Goals of Attack

We describe the following goals of attack on stream ciphers:

Distinguishing Attack: An adversary distinguishes a keystream from a true random number sequence. The aim of the attack is to confirm whether the stream cipher satisfies the pseudorandomness described in Definition 2.2.

Predicting Attack: An adversary predicts an unknown keystream bit/byte by using the knowledge of known keystream bits/bytes under the scenario of the known plaintext attack. The aim of the attack is to confirm whether the stream cipher satisfies the pseudorandomness described in Definition 2.2.

Key Recovery Attack: An adversary derives a secret key from a keystream under the scenario of the known plaintext attack. If the secret key can be obtained with less than the computational complexity of an exhaustive key search, then the stream cipher is regarded as insecure.

State Recovery Attack: An adversary derives an internal state from a keystream under the scenario of the known plaintext attack. This is equivalent to the key recovery attack essentially. Once the internal state is recovered at any stage of the keystream generation, the adversary can obtain the entire subsequent keystream.

2.2 Description of RC4

RC4 consists of the KSA and the PRGA. Both the KSA and the PRGA have two 8-bit indices $\{i, j\}$ and a secret internal state S, which is a permutation of all possible N bytes $\{0, 1, 2, \ldots, N-1\}$ (typically, $N = 2^8$). The KSA generates the initial state $S_0(= S_N^K)$, which becomes an input of the PRGA from a secret key K of ℓ bytes. Once the initial state S_0 is generated from the KSA, the PRGA outputs a keystream byte $\{Z_1, Z_2, \ldots, Z_r\}$ in each round, where r is the number of rounds. After that, the keystream byte Z_r is XORed with a plaintext byte P_r to generate a ciphertext byte C_r. Figure 2.1 shows the encryption/decryption process by RC4 stream cipher.

We describe the KSA and the PRGA as Algorithms 1 and 2. $\{S_i^K, i, j_i^K\}$ and $\{S_r, i_r, j_r\}$ are $\{S, i, j\}$ in the i-th and the r-th round of the KSA and the PRGA, respectively. The Swap function takes two 8-bit input variables, mutually exchanges the values of the variables, and outputs the exchanged variables. t_r is an 8-bit index of a keystream byte as $S_r[i_r] + S_r[j_r]$. All additions are arithmetic addition modulo N. We use these notations throughout the remainder of this dissertation.

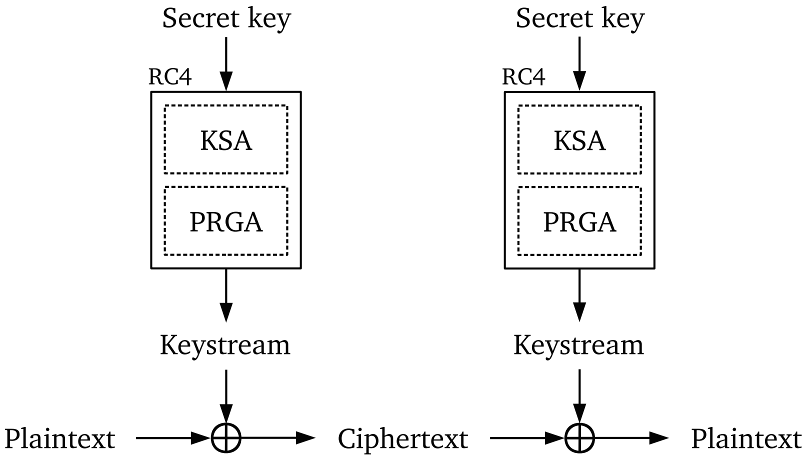

Figure 2.1: Encryption/decryption process by RC4 stream cipher.

Algorithm 1 KSA

```
Input: ℓ-byte key $K$
Output: initial state $S_0 \leftarrow S_N^K$
for $i = 0$ to $N-1$ do
    $S_0^K[i] \leftarrow i$
end for
$j_0^K \leftarrow 0$
for $i = 0$ to $N-1$ do
    $j_{i+1}^K \leftarrow j_i^K + S_i^K[i] + K[i \bmod \ell]$
    Swap($S_i^K[i], S_i^K[j_{i+1}^K]$)
    $S_{i+1}^K \leftarrow S_i^K$
end for
```

Algorithm 2 PRGA

```
Input: initial state $S_0$
Output: keystream bytes $\{Z_1, Z_2, \ldots, Z_r\}$
$r \leftarrow 0$, $i_0 \leftarrow 0$, $j_0 \leftarrow 0$
loop
    $r \leftarrow r + 1$, $i_r \leftarrow i_{r-1} + 1$
    $j_r \leftarrow j_{r-1} + S_{r-1}[i_r]$
    Swap($S_{r-1}[i_r], S_{r-1}[j_r]$)
    $S_r \leftarrow S_{r-1}$
    $t_r \leftarrow S_r[i_r] + S_r[j_r]$
    $Z_r \leftarrow S_r[t_r]$
end loop
```

2.3 Secret Key Setting in WEP

WEP adopts RC4 stream cipher for confidentiality of information, and uses a 64-bit or 128-bit per-packet key K which concatenates a 24-bit (3-byte) IV and a 40-bit or 104-bit (5-byte or 13-byte) WEP key. For example, the per-packet key setting with the 104-bit WEP key is as follows:

$$K = K[0]||K[1]||K[2]||K[3]||\ldots||K[15] = \mathrm{IV}[0]||\mathrm{IV}[1]||\mathrm{IV}[2]||K'[0]||\ldots||K'[12],$$

where IV$[i]$ is the $i+1$-th byte of the IV, and $K'[j]$ is the $j+1$-th byte of the WEP key. The IV is automatically generated for each packet by a transmitter-side system. The reason why the IV is used is that the packets may be lost owing to transmission/reception errors in the wireless networks. The WEP key is secretly pre-shared between all users and the access point, and is not frequently updated.

WEP also adopts Cyclic Redundancy Check 32 (CRC32) for the integrity of information, and generates an Integrity Check Value (ICV) from the plaintext data. Figure 2.2 shows the WEP encapsulation process [Soc04]. The transmitters generate the per-packet key, which becomes an input of RC4, and encrypt each packet by XORing the plaintext data appending the ICV and the keystream generated from RC4. Then, the transmitters append the corresponding IV to the ciphertext data, and transmit the result to the receivers. After the receivers receive the packet, they generate the corresponding per-packet key from the IV appended to the packet, and decrypt by XORing the ciphertext data and the keystream generated from RC4. The receivers can check the integrity of the information by computing the ICV of the decrypted data using CRC32 and by verifying whether it matches the ICV included in the packet.

Note that the IV appended to the packet remains in plaintext. Therefore, anyone can easily obtain the IVs by intercepting the packets on wireless networks.

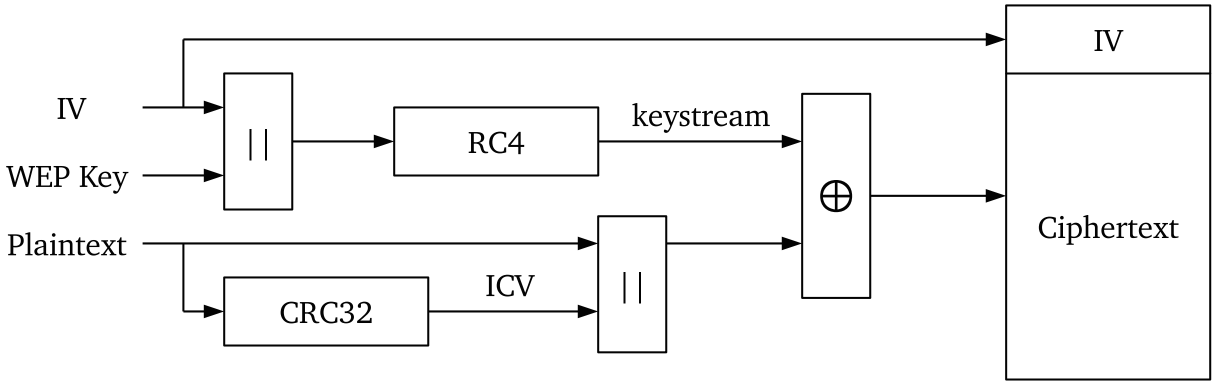

Figure 2.2: WEP encapsulation process.

2.4 Secret Key Setting in WPA-TKIP

WPA-TKIP adopts RC4 stream cipher for confidentiality of information, and improves a 16-byte RC4 key setting in WEP. It includes a *temporal key hash function* [HWF02], a MICHAEL algorithm [FM02], and a key management scheme based on IEEE 802.1X [Soc04]. Figure 2.3 shows the TKIP encapsulation process [Soc04].

The key management scheme generates a 16-byte *Temporal Key* (TK) after the IEEE 802.1X authentication. After that, the temporal key hash function outputs a 16-byte per-packet RC4 key ($K = \texttt{RC4KEY}$) from the TK, a 6-byte *Transmitter Address* (TA), and a 48-bit IV, which is often called the *TKIP sequence counter* (TSC). The temporal key hash function consists of two phases: The first phase (Phase 1) mixes the TK with the TA and the most significant 32-bit IV (IV32). The output of Phase 1 is cached, and it can be reused to process subsequent packets associated with the same TK and the same TA. The second phase (Phase 2) mixes the output of Phase 1 with the TK and the least significant 16-bit IV (IV16). The 48-bit IV value must be different for each packet encrypted under the same TK and the same TA.

We describe Phase 1 and Phase 2 as Algorithms 3 and 4, respectively. P1K and PPK are treated as arrays of 16-bit words. TK, TA, and RC4KEY are treated as arrays of 8-bit words. The S function is a bijective nonlinear S-box defined by a table lookup in [HWF02]; it takes a 16-bit input and outputs a 16-bit value. The Mk16 function takes two 8-bit inputs, and outputs a 16-bit word such that $\texttt{Mk16}(\texttt{X}, \texttt{Y}) = 256 * \texttt{X} + \texttt{Y}$, which is equivalent to $\texttt{Mk16}(\texttt{X}, \texttt{Y}) = \texttt{X} \mid\mid \texttt{Y}$. The Hi16 and Lo16 functions take a 32-bit input, and output the most and the least significant 16 bits, respectively. The Hi8 and Lo8 functions are similar to the Hi16 and Lo16 functions, but the input size is 16 bits and the output size is 8 bits. Both RotR1 and $\ggg$ denote a cyclic right-shift by one.

TKIP uses the MICHAEL algorithm to generate a *Message Integrity Code* (MIC) for the integrity of information [FM02]. The algorithm takes a MIC key, the TA, the receiver address (RA), and the message as inputs, and outputs the plaintext data concatenated with a MIC-tag.

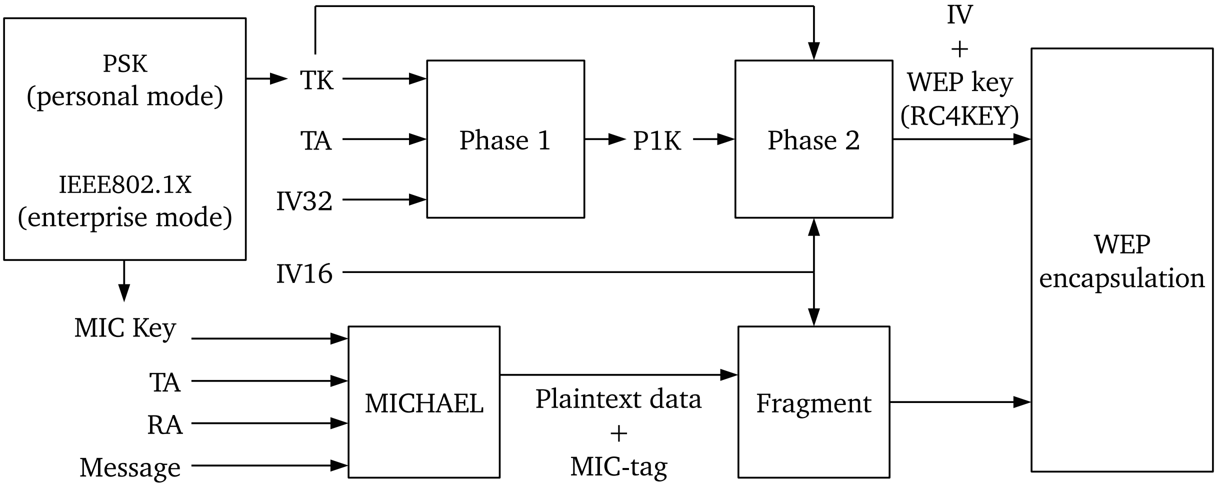

Figure 2.3: TKIP encapsulation process.

Algorithm 3 Phase 1 of the temporal key hash function

```
Input: $\texttt{TK}, \texttt{TA}, \texttt{IV32}$
Output: $\texttt{P1K}$
Phase1_STEP1 :
  $\texttt{P1K}[0] = \texttt{Lo16}(\texttt{IV32})$
  $\texttt{P1K}[1] = \texttt{Hi16}(\texttt{IV32})$
  $\texttt{P1K}[2] = \texttt{Mk16}(\texttt{TA}[1], \texttt{TA}[0])$
  $\texttt{P1K}[3] = \texttt{Mk16}(\texttt{TA}[3], \texttt{TA}[2])$
  $\texttt{P1K}[4] = \texttt{Mk16}(\texttt{TA}[5], \texttt{TA}[4])$
Phase1_STEP2 :
  for $\texttt{i} = 0$ to 7 do
    $\texttt{j} = 2 * (\texttt{i} \ \& \ 1)$
    $\texttt{P1K}[0] = \texttt{P1K}[0] + \texttt{S}[\texttt{P1K}[4] \oplus \texttt{Mk16}(\texttt{TK}[\ 1 + \texttt{j}], \texttt{TK}[\ 0 + \texttt{j}])]$
    $\texttt{P1K}[1] = \texttt{P1K}[1] + \texttt{S}[\texttt{P1K}[0] \oplus \texttt{Mk16}(\texttt{TK}[\ 5 + \texttt{j}], \texttt{TK}[\ 4 + \texttt{j}])]$
    $\texttt{P1K}[2] = \texttt{P1K}[2] + \texttt{S}[\texttt{P1K}[1] \oplus \texttt{Mk16}(\texttt{TK}[\ 6 + \texttt{j}], \texttt{TK}[\ 8 + \texttt{j}])]$
    $\texttt{P1K}[3] = \texttt{P1K}[3] + \texttt{S}[\texttt{P1K}[2] \oplus \texttt{Mk16}(\texttt{TK}[13 + \texttt{j}], \texttt{TK}[12 + \texttt{j}])]$
    $\texttt{P1K}[4] = \texttt{P1K}[4] + \texttt{S}[\texttt{P1K}[3] \oplus \texttt{Mk16}(\texttt{TK}[\ 1 + \texttt{j}], \texttt{TK}[\ 0 + \texttt{j}])] + \texttt{i}$
  end for
```

This output is fragmented before inputting it in the WEP encapsulation process for encrypting the plaintext data and computing the ICV (see Section 2.3). The receivers can verify the MIC-tag after decryption of the received ciphartext data, ICV checking, and defragmentation of the decrypted plaintext data, and can discard any received data with invalid MIC.

One of the remarkable features of TKIP is that the first three bytes of the RC4 key $\{K[0], K[1], K[2]\}$ are derived from the IV16 (see PHASE2_STEP3 in Algorithm 4) as follows:

$$K[0] = (\texttt{IV16} \gg 8) \ \& \ \texttt{0xFF}, \tag{2.2}$$

$$K[1] = ((\texttt{IV16} \gg 8) \mid \texttt{0x20}) \ \& \ \texttt{0x7F}, \tag{2.3}$$

$$K[2] = \texttt{IV16} \ \& \ \texttt{0xFF}. \tag{2.4}$$

Note that the first three bytes of the RC4 key $\{K[0], K[1], K[2]\}$ in WPA-TKIP are known because the IV can be obtained by observing packets.

Algorithm 4 Phase 2 of the temporal key hash function

```
Input: PiK, TK, IV16
Output: RC4KEY
Phase2_STEP1 :
  PPK[0] = P1K[0]
  PPK[1] = P1K[1]
  PPK[2] = P1K[2]
  PPK[3] = P1K[3]
  PPK[4] = P1K[4]
  PPK[5] = P1K[4] + IV16
Phase2_STEP2 :
  PPK[0] = PPK[0] + S[PPK[5] $\oplus$ Mk16(TK[ 1], TK[ 0])]
  PPK[1] = PPK[1] + S[PPK[0] $\oplus$ Mk16(TK[ 3], TK[ 2])]
  PPK[2] = PPK[2] + S[PPK[1] $\oplus$ Mk16(TK[ 5], TK[ 4])]
  PPK[3] = PPK[3] + S[PPK[2] $\oplus$ Mk16(TK[ 7], TK[ 6])]
  PPK[4] = PPK[4] + S[PPK[3] $\oplus$ Mk16(TK[ 9], TK[ 8])]
  PPK[5] = PPK[5] + S[PPK[4] $\oplus$ Mk16(TK[11], TK[10])]
  PPK[0] = PPK[0] + RotR1(PPK[5] $\oplus$ Mk16(TK[13], TK[12]))
  PPK[1] = PPK[1] + RotR1(PPK[0] $\oplus$ Mk16(TK[15], TK[14]))
  PPK[2] = PPK[2] + RotR1(PPK[1])
  PPK[3] = PPK[3] + RotR1(PPK[2])
  PPK[4] = PPK[4] + RotR1(PPK[3])
  PPK[5] = PPK[5] + RotR1(PPK[4])
Phase2_STEP3 :
  RC4KEY[0] = Hi8(IV16)
  RC4KEY[1] = (Hi8(IV16) | 0x20) & 0x7F
  RC4KEY[2] = Lo8(IV16)
  RC4KEY[3] = Lo8((PPK[5] $\oplus$ Mk16(TK[1], TK[0])) $\ggg$ 1)
  for i = 0 to 0 do
    RC4KEY[4 + (2 * i)] = Lo8(PPK[i])
    RC4KEY[5 + (2 * i)] = Hi8(PPK[i])
  end for
```

2.5 Statistical Cryptanalysis of RC4 Stream Cipher

2.5.1 Probability Distributions

We describe the formal definition of probability distributions which are used in our statistical cryptanalysis of RC4 stream cipher (refer to [DS12] for details).

Definition 2.3 ([DS12, Definition 5.2.1])**.** *A random variable X has the* **bernoulli distribution** *with parameter p $(0 \leq p \leq 1)$ if X can take only the values 0 and 1 and the probabilities are*

$$\Pr(X = 1) = p \quad \textit{and} \quad \Pr(X = 0) = 1 - p. \tag{2.5}$$

The probability function of X can be given by

$$f(x \mid p) = \begin{cases} p^x(1-p)^{1-x} & \textit{for } x = 0, 1, \\ 0 & \textit{otherwise.} \end{cases} \tag{2.6}$$

Definition 2.4 ([DS12, Definition 5.6.1])**.** *A random variable X has the* **normal distribution** *with mean μ and variance σ^2 $(-\infty < \mu < \infty$ and $\sigma > 0)$ if X has a continuous distribution with the following probability density function:*

$$f(x \mid \mu, \sigma^2) = \frac{1}{(2\pi)^{1/2}\sigma} \exp\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2\right] \textit{ for } -\infty < x < \infty. \tag{2.7}$$

Definition 2.5 ([DS12, Definition 5.6.2])**.** *The normal distribution with mean 0 and variance 1 is called the* **standard normal distribution***. The probability density function of the standard normal distribution is usually denoted by the symbol ϕ, and the cumulative distribution function is denoted by the symbol Φ. Thus,*

$$\phi(x) = f(x \mid 0, 1) = \frac{1}{(2\pi)^{1/2}} \exp\left(-\frac{1}{2}x^2\right) \textit{ for } -\infty < x < \infty. \tag{2.8}$$

and

$$\Phi(x) = \int_{-\infty}^{x} \phi(u)du \textit{ for } -\infty < x < \infty. \tag{2.9}$$

Definition 2.6 ([DS12, Definition 5.9.1])**.** *A discrete random vector $\boldsymbol{X} = (X_1, \ldots, X_k)$ whose probability function is given by the following equation has the* **multinomial distribution** *with parameters n and $\boldsymbol{p} = (p_1, \ldots, p_k)$:*

$$\begin{aligned} f(\boldsymbol{x} \mid n, \boldsymbol{p}) &= \Pr(\boldsymbol{X} = \boldsymbol{x}) = \Pr(X_1 = x_1, \ldots, X_k = x_k) \\ &= \begin{cases} \dfrac{n!}{x_1!x_2!\cdots x_k!} p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k} & \textit{if } x_1 + x_2 + \cdots + x_k = n, \\ 0 & \textit{otherwise.} \end{cases} \end{aligned} \tag{2.10}$$

2.5.2 Confidence Interval for Population Mean

We would like to investigate the occurrence probability of certain events in RC4 stream cipher by experiments using all secret keys. Such probability can be regarded as the *population mean*. However, it is impossible to investigate population mean accurately from the perspective of time complexity because secret key space is too large (typically, RC4 has secret key space of size 2^{128}). Therefore, we estimate confidence interval for population mean from *sample mean*, which is defined as Definition 2.7.

Definition 2.7 ([DS12, Definition 5.6.2])**.** *Let $X_1, \ldots, X_n$ be random variables. The average of these n random variables, $\frac{1}{n}\sum_{i=1}^{n} X_i$, is called their* **sample mean** *and is commonly denoted $\overline{X}_n$.*

Before showing the definition of confidence interval for population mean, we describe the *central limit theorem* as Theorem 2.1.

Theorem 2.1 ([DS12, Theorem 6.3.1])**. (Central Limit Theorem)** *If the random variables $X_1, \ldots, X_n$ form a random sample of size n from a given distribution with mean μ and variance σ^2 $(0 < \sigma^2 < \infty)$, then for each fixed number x,*

$$\lim_{n\to\infty} \Pr\left[\frac{\overline{X}_n - \mu}{\sigma/n^{1/2}} \leq x\right] = \Phi(x), \tag{2.11}$$

where Φ denotes the cumulative distribution function of the standard normal distribution.

The central limit theorem shows that if a large amount of random sample is taken from any distribution with mean μ and variance σ^2, then the distribution of the random variable $\frac{\overline{X}_n-\mu}{\sigma/n^{1/2}}$ will be approximately the standard normal distribution (see Definition 2.5). From the theorem, we can derive α% confidence interval for population mean from the table of the standard normal distribution function, where α is the confidence coefficient. In this dissertation, we use 95% confidence interval for population mean μ, which is defined as Definition 2.8.

Definition 2.8 ([Dev11, Definition in Chapter 7])**.** *If, after observing $X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n$, we compute the observed sample mean $\overline{x}_n$ and then the resulting fixed interval is called a* **95% confidence interval for population mean** *μ. This confidence interval can be expressed as*

$$\overline{x}_n - 1.96 \cdot \frac{\sigma}{\sqrt{n}} < \mu < \overline{x}_n + 1.96 \cdot \frac{\sigma}{\sqrt{n}} \text{ with 95\% confidence.} \tag{2.12}$$

A concise expression for the interval is $\overline{x}_n \pm 1.96 \cdot \sigma/\sqrt{n}$, where $-$ gives the left endpoint (lower limit) and $+$ gives the right endpoint (upper limit).

We consider whether the certain event occurs or not. Let $X = 0$ if the event does not occur, and let $X = 1$ if the event occurs. Then, the random variable X has the bernoulli distribution with parameter $p = \Pr(X = 1)$ (see Definition 2.3).

Now, we describe the *law of large numbers* as Theorem 2.2.

Theorem 2.2 ([DS12, Theorem 6.2.4])**. (Law of Large Numbers)** *Suppose that $X_1, \ldots, X_n$ form a random sample from a distribution for which the mean is μ and for which the variance is finite. Let $\overline{X}_n$ denote the sample mean. Then*

$$\overline{X}_n \xrightarrow{p} \mu. \tag{2.13}$$

From the theorem, if a large amount of random sample is taken from the bernoulli distribution, the parameter p converges to the observed sample mean $\overline{x}_n$, and therefore its standard deviation $\sigma = \sqrt{p(1-p)}$ converges to $\sqrt{\overline{x}_n(1-\overline{x}_n)}$ (refer to [DS12] for details).

In summary, we use the following equations instead of Equation (2.12) to estimate 95% confidence interval for population mean μ in our statistical cryptanalysis of RC4 stream cipher:

$$\overline{x}_n - 1.96 \cdot \frac{\sqrt{\overline{x}_n(1-\overline{x}_n)}}{\sqrt{n}} < \mu < \overline{x}_n + 1.96 \cdot \frac{\sqrt{\overline{x}_n(1-\overline{x}_n)}}{\sqrt{n}}. \tag{2.14}$$

Hereinafter, the lower and upper limit in 95% confidence interval for population mean μ are denoted by μ_{lower} and μ_{upper}, respectively.

2.5.3 Experiments for Statistical Cryptanalysis

Experimental Environments

The followings are our experimental environments in Chapters 4–6:

- Intel® Core™ i3-3230M CPU with 2.60 GHz, 4.0 GB memory, C language, and gcc 4.6.3 compiler.
- Intel® Core™ i3-3220M CPU with 3.30 GHz, 4.0 GB memory, C language, and gcc 4.8.2 compiler.
- Intel® Core™ i5-3320M CPU with 2.60 GHz, 8.0 GB memory, C language, and gcc 4.8.2 compiler.
- Intel® Xeon® E5-1680 v3 CPU with 3.20 GHz, 32.0 GB memory, C language, and gcc 5.4.0 compiler.

Experimental Evaluations: Percentage of Relative Error

In order to check the accuracy of our theoretical values, we use the percentage of the relative error ϵ defined as Definition 2.9.

Definition 2.9. *The percentage of the relative error is determined by using the following formula:*

$$\epsilon = \frac{|\mathit{experimental\ value} - \mathit{theoretical\ value}|}{\mathit{experimental\ value}} \times 100(\%).$$

The experimental value is treated as the sample mean. Then, we estimate the lower and upper limit in 95% confidence interval for population mean μ_{lower} and μ_{upper} from the experimental value. Next, we compute the percentage of the relative error ϵ_{lower} and ϵ_{upper} from μ_{lower} and μ_{upper} as the experimental value, respectively. Finally, we evaluate the accuracy of our theoretical value using the maximum of the percentage of the relative error $\epsilon_{max} = \max(\epsilon_{lower}, \epsilon_{upper})$.

Chapter 3

Previous Works

We consider two approaches to the cryptanalysis of RC4. One is to demonstrate the existence of a certain event with statistical weakness, known as a *bias* or a *correlation*, involving the RC4 key bytes, internal state variables, or keystream bytes (a *distinguishing attack*). Now, we refer to an event with significantly higher or lower probability than the probability of random association $\frac{1}{N}$ as a *positive bias* or *negative bias*, respectively. The other approach is to attack RC4 itself using biases or correlations in order to recover the plaintext bytes (a *plaintext recovery attack*), the RC4 key bytes (a *key recovery attack*), or the internal state variables (a *state recovery attack*). In addition, many cryptanalyses on security protocols have been reported, such as distinguishing attacks on WPA-TKIP, plaintext recovery attacks on SSL/TLS and WPA-TKIP, and key recovery attacks on WEP.

This chapter describes some useful theorems, lemmas, and attack procedures, which are used later in our cryptanalysis and discussions. Almost all theorems and lemmas in this chapter use the symbol of approximate equation "$\approx$", which should be mathematically confirmed. In fact, those proofs seem to be neither complete, theoretical, nor precise. Ideally, we should check all approximations in practice because some approximations may be correct and others may be incorrect. Now, we should note this facts and list the previous results.

3.1 Distinguishing Attacks: Biases and Correlations

A distinguishing attack is to distinguish a keystream byte from a true random number sequence, and aims to confirm the pseudorandomness of an output generated from stream ciphers. This section describes the previous works on distinguishing attacks with respect to the following aspects:

Section 3.1.1: Short-term Biases in the Keystream Bytes in [MS01, Mir02, GMPS14, Man01, SGPM15, IOWM13, GMM+14]

Section 3.1.2: Long-term Biases in the Keystream Bytes in [FM00, Man05]

Section 3.1.3: Glimpse Correlations in [Jen96, MG13]

Section 3.1.4: Key Correlations of the Internal State Variables in [Roo95, PM07, MP08b]

Section 3.1.5: Key Correlations of the Keystream Bytes in [SVV10, Sar14, GMM+14]

Although many other attacks have been reported, e.g., in [BMPdM18, DS18, GMPS11, JBIO16, MPG11, MPS+13, PM09, Sar15, SV17, VP15], we will not describe these attacks in this section because these are out of our cryptanalysis and discussions in this dissertation.

3.1.1 Short-term Biases in the Keystream Bytes

In [MS01], Mantin and Shamir presented that the second keystream byte Z_2 is biased toward 0 as Theorem 3.1.

Theorem 3.1 ([MS01, Theorem 1])**.** *Assume that the initial state S_0 is randomly chosen from a set of all possible permutations of $\{0, \ldots, N-1\}$. Then, the probability that the second keystream byte Z_2 is biased toward 0 is approximately $\frac{2}{N}$.*

Mantin and Shamir further presented the number of samples to distinguish two distributions with a constant probability of success as Theorem 3.2.

Theorem 3.2 ([MS01, Theorem 2])**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be two distributions, and assume that the event e occurs in $\mathcal{X}$ with probability p and $\mathcal{Y}$ with probability $p \cdot (1+q)$. Then, for small p and q, $\mathcal{O}(\frac{1}{p \cdot q^2})$ samples suffice to distinguish $\mathcal{X}$ from $\mathcal{Y}$ with a constant probability of success.*

Let $\mathcal{X}$ be a distribution of the second byte of a true random number sequence, and let $\mathcal{Y}$ be a distribution of the second byte of the keystream Z_2 generated from RC4. Then, the number of samples to distinguish $\mathcal{X}$ from $\mathcal{Y}$ is $\mathcal{O}(N)$ because $p = \frac{1}{N}$ and $q = 1$.

In [Mir02], Mironov experimentally presented a bias in a distribution of the first byte of the keystream Z_1. Subsequently, Sen Gupta et al. provided a theoretical value of the bias in [GMPS14] as Theorem 3.3. The proof of Theorem 3.3 uses Lemma 3.1, presented by Mantin in [Man01].

Lemma 3.1 ([Man01, Theorem 6.2.1])**.** *In the initial state of the PRGA, for $0 \leq u \leq N-1$ and $0 \leq v \leq N-1$, we have*

$$\Pr(S_0[u] = v) = \begin{cases} \frac{1}{N}\left(\left(1 - \frac{1}{N}\right)^{v} + \left(1 - \left(1 - \frac{1}{N}\right)^{v}\right)\left(1 - \frac{1}{N}\right)^{N-u-1}\right) & \text{when } v \leq u, \\ \frac{1}{N}\left(\left(1 - \frac{1}{N}\right)^{N-u-1} + \left(1 - \frac{1}{N}\right)^{v}\right) & \text{when } v > u. \end{cases}$$

Theorem 3.3 ([GMPS14, Theorem 13])**.** *The probability distribution of the first keystream byte* *is given as*

$$\Pr(Z_1 = v) = Q_v + \sum_{X \in \mathcal{L}_v} \sum_{Y \in \mathcal{T}_{v,X}} \Pr(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X+Y] = v),$$

$$\text{with } Q_v = \begin{cases} \Pr(S_0[1] = 1 \wedge S_0[2] = 0) & \text{when } v = 0, \\ \Pr(S_0[1] = 0 \wedge S_0[0] = 1) & \text{when } v = 1, \\ \Pr(S_0[1] = 1 \wedge S_0[2] = v) + \Pr(S_0[1] = v \wedge S_0[v] = 0) & \\ \quad + \Pr(S_0[1] = 1 - v \wedge S_0[1-v] = v) & \text{otherwise,} \end{cases}$$

where $v \in \{0, \ldots, N-1\}$, $\mathcal{L}_v = \{0, \ldots, N-1\} \backslash \{1, v\}$, *and* $\mathcal{T}_{v,X} = \{0, \ldots, N-1\} \backslash \{0, X, 1-X, v\}$.

In [MPG11], Maitra et al. presented that the 3rd to the 255th bytes of the keystream $\{Z_3, Z_4, \ldots, Z_{255}\}$ are biased toward 0. Subsequently, Sen Gupta et al. provided a complete proof of the biases in [GMPS14] as Theorem 3.4. The proof of Theorem 3.4 uses Lemmas 3.2 and 3.3, presented by Sen Gupta et al. in [GMPS14].

Lemma 3.2 ([GMPS14, Lemma 1]). *After the first round of the PRGA, for* $0 \leq u \leq N-1$ *and* $0 \leq v \leq N-1$*, the probability distribution of the internal state* S_1 *is given as*

$$\Pr(S_1[u] = v) = \begin{cases} \Pr(S_0[1] = 1) + \sum_{X \neq 1} \Pr(S_0[1] = X \wedge S_0[X] = 1), & u = 1, v = 1; \\ \sum_{X \neq 1, v} \Pr(S_0[1] = X \wedge S_0[X] = v), & u = 1, v \neq 1; \\ \Pr(S_0[1] = u) + \sum_{X \neq u} \Pr(S_0[1] = X \wedge S_0[u] = u), & u \neq 1, v = u; \\ \sum_{X \neq u, v} \Pr(S_0[1] = X \wedge S_0[u] = v), & u \neq 1, v \neq u. \end{cases}$$

Lemma 3.3 ([GMPS14, Theorem 1]). *After the* $u-1$*-th round of the PRGA, for* $3 \leq u \leq N-1$ *and* $0 \leq v \leq N-1$*, we have*

$$\Pr(S_{u-1}[u] = v) \approx \Pr(S_1[u] = v)\left(1 - \frac{1}{N}\right)^{u-2} + \sum_{t=2}^{u-1} \sum_{w=0}^{u-t} \frac{\Pr(S_1[t] = v)}{w! \cdot N} \left(\frac{u-t-1}{N}\right)^w \left(1 - \frac{1}{N}\right)^{u-3-w}.$$

Theorem 3.4 ([GMPS14, Theorem 14]). *For* $3 \leq r \leq 255$*, the probability that the* r*-th keystream byte* Z_r *is biased toward* 0 *is given as*

$$\Pr(Z_r = 0) \approx \frac{1}{N} + \frac{c_r}{N^2},$$

$$\text{where } c_r = \begin{cases} \dfrac{N}{N-1} \cdot (N \cdot \Pr(S_{r-1}[r] = r) - 1) - \dfrac{N-2}{N-1} & \text{for } r = 3, \\ \dfrac{N}{N-1} \cdot (N \cdot \Pr(S_{r-1}[r] = r) - 1) & \text{otherwise.} \end{cases}$$

In [SGPM15], Sarkar et al. presented that the 256th and the 257th bytes of the keystream $\{Z_{256}, Z_{257}\}$ are biased toward 0, and provided complete proofs as Theorems 3.5 and 3.6, respectively.

Theorem 3.5 ([SGPM15, Theorem 5])**.** *When $N = 256$, the probability that the N-th keystream byte Z_N is biased toward* 0 *is given as*

$$\Pr(Z_N = 0) \approx \frac{1}{N} - \frac{0.37}{N}.$$

Theorem 3.6 ([SGPM15, Theorem 6])**.** *When $N = 256$, the probability that the $N+1$-th keystream byte Z_{N+1} is biased toward* 0 *is given as*

$$\Pr(Z_{N+1} = 0) \approx \frac{1}{N} + \frac{0.36}{N}.$$

In [IOWM13], Isobe et al. presented four biases in the first 255 bytes of the keystream. They first proved a conditional bias, by which Z_1 is biased toward 0 when $Z_2 = 0$ as Theorem 3.7. Subsequently, they proved that Z_3 is biased toward 131 as Theorem 3.8, Z_r are biased toward r for $3 \leq r \leq N-1$ as Theorem 3.9, and extended keylength-dependent biases by which Z_r are biased toward $-r$ when $r = x \cdot \ell$ $(x = 1, 2, \ldots, 7)$ as Theorem 3.10, where ℓ is the key size. They further provided a set of the strongest short-term biases in the first 257 bytes of the keystream $\{Z_1, Z_2, \ldots, Z_{257}\}$ as listed in Table 3.1.

Theorem 3.7 ([IOWM13, Theorem 6])**.** $\Pr(Z_1 = 0 \mid Z_2 = 0)$ *is given as*

$$\Pr(Z_1 = 0 \mid Z_2 = 0) \approx \frac{1}{2} \cdot \left(\Pr(S_0[1] = 1 + (1 - \Pr(S_0[1] = 1)) \cdot \frac{1}{N} \right) + \frac{1}{2} \cdot \frac{1}{N}.$$

Theorem 3.8 ([IOWM13, Theorem 7])**.** $\Pr(Z_3 = 131)$ *is given as*

$$\Pr(Z_3 = 131) \approx \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128) + (1 - \Pr(S_0[1] = 131) \cdot \Pr(S_0[2] = 128)) \cdot \frac{1}{N}.$$

Theorem 3.9 ([IOWM13, Theorem 8])**.** *For $3 \leq r \leq N-1$,* $\Pr(Z_r = r)$ *is given as*

$$\begin{aligned}\Pr(Z_r = r) \approx\, & p_{r-1,0} \cdot \frac{1}{N} + p_{r-1,r} \cdot \frac{1}{N} \cdot \frac{N-2}{N} \\ & + \left(1 - p_{r-1,0} \cdot \frac{1}{N} - p_{r-1,r} \cdot \frac{1}{N} - (1 - p_{r-1,0}) \cdot \frac{1}{N} \cdot 2 \right) \cdot \frac{1}{N},\end{aligned}$$

where $p_{r-1,0} = \Pr(S_{r-1}[r] = 0)$ *and* $p_{r-1,r} = \Pr(S_{r-1}[r] = r)$*.*

Theorem 3.10 ([IOWM13, Theorem 9])**.** *When $r = x \cdot \ell$ $(x = 1, 2, \ldots, 7)$,* $\Pr(Z_r = -r)$ *is given as*

$$\Pr(Z_r = -r) \approx \frac{1}{N^2} + \left(1 - \frac{1}{N^2} \right) \cdot \gamma_r + (1 - \delta_r) \cdot \frac{1}{N},$$

where $\gamma_r = \frac{1}{N^2} \cdot \left(1 - \frac{r+1}{N}\right)^y \cdot \sum_{y=r+1}^{N-1} \left(1 - \frac{1}{N}\right) \cdot \left(1 - \frac{2}{N}\right)^{y-r} \cdot \left(1 - \frac{3}{N}\right)^{N-y+2r-4}$, $\delta_r = \Pr(S_{r-1}[r] = 0)$.

In [GMM+14], Sen Gupta et al. presented that a distribution of $K[0] + K[1]$ has biases from a relation between $K[0]$ and $K[1]$ in WPA-TKIP as Theorem 3.11 and Table 3.2.

Table 3.1: Set of the strongest short-term biases in the first 257 bytes of the keystream.

r	Strongest known bias of Z_r	Theoretical Value	Reference
1	$Z_1 = 0 \mid Z_2 = 0$	$2^{-8} \cdot (1 + 2^{-1.009})$	[IOWM13]
2	$Z_2 = 0$	$2^{-8} \cdot (1 + 2^{0})$	[MS01]
3	$Z_3 = 131$	$2^{-8} \cdot (1 + 2^{-8.089})$	[IOWM13]
4	$Z_4 = 0$	$2^{-8} \cdot (1 + 2^{-7.581})$	[GMPS14]
5–15	$Z_r = r$	max: $2^{-8} \cdot (1 + 2^{-7.627})$ min: $2^{-8} \cdot (1 + 2^{-7.737})$	[IOWM13]
16	$Z_{16} = 240$	$2^{-8} \cdot (1 + 2^{-4.671})$	[GMPS11]
17–31	$Z_r = r$	max: $2^{-8} \cdot (1 + 2^{-7.759})$ min: $2^{-8} \cdot (1 + 2^{-7.912})$	[IOWM13]
32	$Z_{32} = 224$	$2^{-8} \cdot (1 + 2^{-5.176})$	[IOWM13]
33–47	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-7.897})$ min: $2^{-8} \cdot (1 + 2^{-8.050})$	[GMPS14]
48	$Z_{48} = 208$	$2^{-8} \cdot (1 + 2^{-5.651})$	[IOWM13]
49–63	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-8.072})$ min: $2^{-8} \cdot (1 + 2^{-8.224})$	[GMPS14]
64	$Z_{64} = 192$	$2^{-8} \cdot (1 + 2^{-6.085})$	[IOWM13]
65–79	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-8.246})$ min: $2^{-8} \cdot (1 + 2^{-8.398})$	[GMPS14]
80	$Z_{80} = 176$	$2^{-8} \cdot (1 + 2^{-6.574})$	[IOWM13]
81–95	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-8.420})$ min: $2^{-8} \cdot (1 + 2^{-8.571})$	[GMPS14]
96	$Z_{96} = 160$	$2^{-8} \cdot (1 + 2^{-6.970})$	[IOWM13]
97–111	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-8.592})$ min: $2^{-8} \cdot (1 + 2^{-8.741})$	[GMPS14]
112	$Z_{112} = 144$	$2^{-8} \cdot (1 + 2^{-7.300})$	[IOWM13]
113–255	$Z_r = 0$	max: $2^{-8} \cdot (1 + 2^{-8.763})$ min: $2^{-8} \cdot (1 + 2^{-10.052})$	[GMPS14]
256	$Z_{256} = 0$	$2^{-8} \cdot (1 - 2^{-9.434})$	[SGPM15]
257	$Z_{257} = 0$	$2^{-8} \cdot (1 + 2^{-9.474})$	[SGPM15]

Theorem 3.11 ([GMM⁺14, Theorem 1])**.** *For $0 \leq v \leq N-1$, a distribution of $K[0]+K[1]=v$ in WPA-TKIP is given by*

$$\begin{aligned}
&\Pr(K[0]+K[1]=v) = 0 && \textit{when } v \textit{ is odd,}\\
&\Pr(K[0]+K[1]=v) = 0 && \textit{when } v \textit{ is even and } v \in [0,31] \cup [128,159],\\
&\Pr(K[0]+K[1]=v) = \frac{2}{N} && \textit{when } v \textit{ is even and } v \in [32,63] \cup [96,127] \cup [160,191] \cup [224,255],\\
&\Pr(K[0]+K[1]=v) = \frac{4}{N} && \textit{when } v \textit{ is even and } v \in [64,95] \cup [192,223].
\end{aligned}$$

Sen Gupta et al. further presented new biases in WPA-TKIP by using the distribution of $K[0]+K[1]$ in Theorem 3.11. They first proved a bias in a distribution of the initial round of the internal state variables $S_0[1]$ as Lemma 3.4. Subsequently, they showed experimentally that Theorems 3.3 and 3.4 for WPA-TKIP, which present the distribution of Z_1 and the biases

Table 3.2: Probability distribution of $K[0]+K[1]$ in WPA-TKIP.

$K[0]$	$K[1]$ (depends on $K[0]$)		$K[0]+K[1]$ (only even)	
Range	Value	Range	Value	Range
0–31	$K[0]+32$	32–63	$2K[0]+32$	32–95
32–63	$K[0]$	32–63	$2K[0]$	64–127
64–95	$K[0]+32$	96–127	$2K[0]+32$	160–223
96–127	$K[0]$	96–127	$2K[0]$	192–255
128–159	$K[0]-96$	32–63	$2K[0]-96$	160–223
160–191	$K[0]-128$	32–63	$2K[0]-128$	192–255
192–223	$K[0]-96$	96–127	$2K[0]-96$	32–95
224–255	$K[0]-128$	96–127	$2K[0]-128$	64–127

$K[0]+K[1]$	Prob.
(only even)	(0 if odd)
0–31	0
32–63	2/256
64–95	4/256
96–127	2/256
128–159	0
160–191	2/256
192–223	4/256
224–255	2/256

of $Z_r = 0$ for $3 \le r \le 255$, are demonstrated by using Lemma 3.4. In addition, they provided a precise proof of Theorem 3.9 as Theorem 3.12, which presents the biases of $Z_r = r$ for $3 \le r \le 255$ in both generic RC4 and WPA-TKIP.

Lemma 3.4 ([GMM+14, Theorem 2]). *In WPA-TKIP, the probability distribution of* $(S_0[1] = v)$ *for* $v = 0, 1, \ldots, N-1$ *is given as*

$$\begin{aligned}\Pr(S_0[1] = v) \approx\ & \alpha \cdot \Pr(K[0]+K[1] = v-1) \\ & + (1-\alpha)\cdot(1 - \Pr(K[0]+K[1] = v-1)) \cdot \Pr(S_0[1] = v)_{\mathrm{RC4}} \\ & + \frac{(1-\alpha)}{N-1} \cdot \sum_{x \neq v} \Pr(K[0]+K[1] = x-1) \cdot \Pr(S_0[1] = x)_{\mathrm{RC4}},\end{aligned}$$

where $\alpha = 1/N + (1-1/N)^{N+2}$, *and both* $\Pr(S_0[1] = v)_{\mathrm{RC4}}$ *and* $\Pr(S_0[1] = x)_{\mathrm{RC4}}$ *are given by Lemma 3.1.*

Theorem 3.12 ([GMM+14, Theorem 3]). *For* $3 \le r \le N-1$, *the probability that* $Z_r = r$ *is given as*

$$\Pr(Z_r = r) \approx \frac{1}{N} + \Pr(S_0[1] = r) \cdot \frac{1}{N}\left(1 - \frac{1}{N}\right)\left(1 - \frac{r-2}{N}\right)\left(1 - \frac{2}{N}\right)^{r-3}.$$

3.1.2 Long-term Biases in the Keystream Bytes

In [FM00], Fluhrer and McGrew presented long-term biases of two consecutive keystream bytes with the condition of index $i = r \bmod N$, which are called the *Fluhrer–McGrew digraph biases*. They consist of 12 positive or negative digraphs as listed in Table 3.3.

In [Man05], Mantin presented a different type of digraph bias in the keystream. Assuming A and B are two consecutive keystream bytes, the digraph AB tends to repeat with short (G-byte) gaps S in the keystream, e.g., $ABAB$, $ABCAB$, and $ABCDAB$, where the gap S is given as nothing, C, and CD, respectively. This is why it is called the *Digraph Repetition Bias* or the *ABSAB Bias*. The ABSAB Bias is described as the following equation:

$$Z_r \parallel Z_{r+1} = Z_{r+2+G} \parallel Z_{r+3+G} \text{ for } G \ge 0, \tag{3.1}$$

Table 3.3: Fluhrer–McGrew digraph biases with the condition of index $i = r \bmod N$.

Condition of index i	Digraph (Z_r, Z_{r+1})	Probability
$i = 1$	$(0, 0)$	$N^{-2} \cdot (1 + 2 \cdot N^{-1})$
$i \neq 1, N-1$	$(0, 0)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 0, 1$	$(0, 1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq N-2$	$(i+1, N-1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 1, N-2$	$(N-1, i+1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq 0, N-3, N-2, N-1$	$(N-1, i+2)$	$N^{-2} \cdot (1 + N^{-1})$
$i = N-2$	$(N-1, 0)$	$N^{-2} \cdot (1 + N^{-1})$
$i = N-1$	$(N-1, 1)$	$N^{-2} \cdot (1 + N^{-1})$
$i = 0, 1$	$(N-1, 2)$	$N^{-2} \cdot (1 + N^{-1})$
$i = 2$	$(N/2+1, N/2+1)$	$N^{-2} \cdot (1 + N^{-1})$
$i \neq N-2$	$(N-1, N-1)$	$N^{-2} \cdot (1 - N^{-1})$
$i \neq 0, N-1$	$(0, i+1)$	$N^{-2} \cdot (1 - N^{-1})$

where $\|$ is the symbol of concatenate operation. The probability of the ABSAB Bias is given as Theorem 3.13.

Theorem 3.13 ([Man05, Theorem 1]). *For small values of G, the probability of the keystream pattern ABSAB where S is a G-word string is* $(1 + e^{(-4-8G)/N}/N) \cdot 1/N^2$.

Mantin further estimated discrimination of two distributions in a set of independent events as Theorem 3.14, and the number of samples to distinguish such distributions with a constant probability of success as Theorem 3.15.

Theorem 3.14 ([Man05, Lemma 3]). *Let $\mathcal{X}$ and $\mathcal{Y}$ be two distributions, and assume that independent events $\{E_i : 1 \leq i \leq k\}$ occur in $\mathcal{X}$ with probabilities $p_{\mathcal{X}}(E_i) = p_i$ and $\mathcal{Y}$ with probabilities $p_{\mathcal{Y}}(E_i) = (1 + b_i)p_i$. Then, discrimination of the distributions is $\sum_i p_i b_i^2$.*

Theorem 3.15 ([Man05, Lemma 4]). *The number of samples to distinguish two distributions that have discrimination D with success probability $1 - \alpha$ (for both directions) is* $(1/D) \cdot (1 - 2\alpha) \cdot \log_2\left(\frac{1-\alpha}{\alpha}\right)$.

3.1.3 Glimpse Correlations

In [Jen96], Jenkins experimentally presented two types of correlations between a keystream byte Z_r and an internal state variable $S_r[i_r]$ or $S_r[j_r]$. The first correlation holds when $S_r[i_r] + S_r[j_r] = j_r$, and then the r-th byte of the keystream becomes

$$Z_r = S_r[S_r[i_r] + S_r[j_r]] = S_r[j_r] = j_r - S_r[i_r]. \tag{3.2}$$

The second correlation holds when $S_r[i_r] + S_r[j_r] = i_r$, and then the r-th byte of the keystream becomes

$$Z_r = S_r[S_r[i_r] + S_r[j_r]] = S_r[i_r] = i_r - S_r[j_r]. \tag{3.3}$$

These correlations are known as the *Glimpse Theorem* or the *Jenkins' Correlation*. Maitra and Sen Gupta provided a proof of the Glimpse Theorem, and we introduce their proof.

Theorem 3.16 ([MG13, Theorem 1])**.** *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(Z_r = j_r - S_r[i_r]) = \Pr(Z_r = i_r - S_r[j_r]) \approx \frac{2}{N}.$$

Proof. To provided this result, one needs to use the paths $i_r = S_r[i_r] + S_r[j_r]$ and $j_r = S_r[i_r] + S_r[j_r]$, respectively. Note that

$$\begin{aligned} i_r = S_r[i_r] + S_r[j_r] \quad &\Rightarrow \quad Z_r = S_r[i_r] = i_r - S_r[j_r], \quad \text{and} \\ j_r = S_r[i_r] + S_r[j_r] \quad &\Rightarrow \quad Z_r = S_r[j_r] = j_r - S_r[i_r]. \end{aligned}$$

Thus, one may evaluate $\Pr(S_r[j_r] = i_r - Z_r)$ as

$$\begin{aligned} &\Pr(Z_r = i_r - S_r[j_r] \mid i_r = S_r[i_r] + S_r[j_r]) \cdot \Pr(i_r = S_r[i_r] + S_r[j_r]) \\ &\quad + \Pr(Z_r = i_r - S_r[j_r] \mid i_r \neq S_r[i_r] + S_r[j_r]) \cdot \Pr(i_r \neq S_r[i_r] + S_r[j_r]) \\ &\quad \approx 1 \cdot \frac{1}{N} + \frac{1}{N} \cdot \left(1 - \frac{1}{N}\right) \approx \frac{2}{N}, \end{aligned}$$

where it is assumed that the desired event $(S_r[j_r] = i_r - Z_r)$ occurs with the probability of random association $\frac{1}{N}$ if $i_r \neq S_r[i_r] + S_r[j_r]$. One may prove the bias in $(S_r[i_r] = j_r - Z_r)$ similarly. □

In [MG13], Maitra and Sen Gupta further presented two types of correlations between two consecutive keystream bytes $\{Z_r, Z_{r+1}\}$ and an internal state variable $S_r[r+1]$ as Theorems 3.17 and 3.18, and we introduce their proofs. These correlations are known as the *Long-term Glimpse*. The Glimpse Theorem and the Long-term Glimpse are collectively referred to as the *Glimpse Correlations*.

Theorem 3.17 ([MG13, Theorem 2])**.** *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(S_r[r+1] = N - 1 \mid Z_{r+1} = Z_r) \approx \frac{2}{N}.$$

Proof. We first prove $\Pr(Z_{r+1} = Z_r \mid S_r[r+1] = N-1) \approx \frac{2}{N}$, and then apply Bayes' theorem to obtain the probability of the target event. The condition $(S_r[r+1] = N-1)$ and the path $(j_r = r+1)$ results in $j_{r+1} = j_r + S_r[r+1] = r + 1 + N - 1 = r$, which eventually gives

$$\begin{aligned} t_{r+1} &= S_{r+1}[i_{r+1}] + S_{r+1}[j_{r+1}] \\ &= S_r[j_{r+1}] + S_r[i_{r+1}] \\ &= S_r[r] + S_r[r+1] \\ &= S_r[i_r] + S_r[j_r] = t_r. \end{aligned}$$

Thus, $Z_{r+1} = S_{r+1}[t_{r+1}] = S_{r+1}[t_r]$ is equal to $Z_r = S_r[t_r]$ in almost all cases, except when t_r equals either i_{r+1} or j_{r+1}, the only two locations that get swapped in transition from S_r to S_{r+1}.

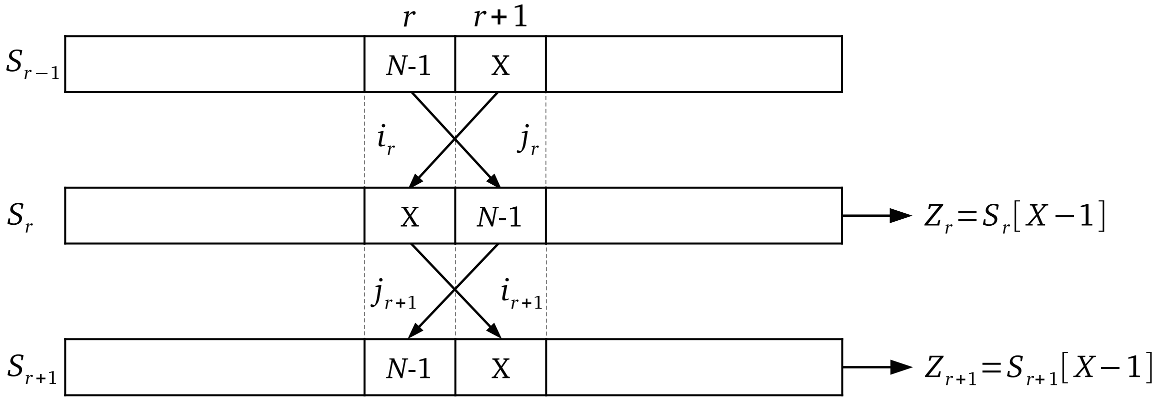

Figure 3.1: The scenario for $(Z_{r+1} = Z_r \mid S_r[r+1] = N-1 \wedge j_r = r+1)$

Thus,

$$\Pr(Z_{r+1} = Z_r \mid S_r[r+1] = N-1 \wedge j_r = r+1) \approx 1.$$

This scenario is as illustrated in Figure 3.1

We now evaluate $\Pr(Z_{r+1} = Z_r \mid S - r[r+1] = N-1)$ as

$$\begin{aligned} &\Pr(Z_{r+1} = Z_r \mid S_r[r+1] = N-1 \wedge j_r = r+1) \cdot \Pr(j_r = r+1) \\ &\quad + \Pr(Z_{r+1} = Z_r \mid S_r[r+1] = N-1 \wedge j_r \neq r+1) \cdot \Pr(j_r \neq r+1) \\ &\quad \approx 1 \cdot \frac{1}{N} + \frac{1}{N} \cdot \left(1 - \frac{1}{N}\right) \approx \frac{2}{N}. \end{aligned}$$

Applying Bayes' theorem to the above result, we obtain

$$\begin{aligned} &\Pr(S_r[r+1] = N-1 \mid Z_{r+1} = Z_r) \cdot \Pr(Z_{r+1} = Z_r) \\ &\quad = \Pr(Z_{r+1} = Z_r \mid S_r[r+1] = N-1) \cdot \Pr(S_r[r+1] = N-1) \\ &\quad \approx \frac{2}{N} \cdot \frac{1}{N}. \end{aligned}$$

Assuming pseudorandomness of the keystream bytes, we obtain $\Pr(Z_{r+1} = Z_r) \approx \frac{1}{N}$ (experimentally verified over a billion trials). Therefore, we obtain $\Pr(S_r[r+1] = N-1 \mid Z_{r+1} = Z_r) \approx \frac{2}{N}$. □

Before introducing the proof of Theorem 3.18, we introduce a simple corollary of the Glimpse Theorem as Corollary 3.1 and its proof by Maitra and Sen Gupta.

Corollary 3.1 ([MG13, Corollary 1]). *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(S_r[r+1] = N-1 \mid Z_{r+1} = r+2) \approx \frac{2}{N}.$$

Proof. In a state transition between rounds r and $r+1$ of the PRGA, we have $i_{r+1} = r+1$, and $S_{r+1}[j_{r+1}] = S_r[i_{r+1}] = S_r[r+1]$, due to the swap operation in the r-th round. Thus, by the Glimpse Theorem (Theorem 3.16), we have

$$\Pr(S_r[r+1] = r+1-Z_{r+1}) \approx \frac{2}{N}.$$

When $Z_{r+1} = r+2$, we obtain the probability of the target event. □

Theorem 3.18 ([MG13, Theorem 3]). *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(S_r[r+1] = N-1 \mid Z_{r+1} = Z_r \wedge Z_{r+1} = r+2) \approx \frac{3}{N}.$$

Proof. We define the main events as follows:

$$A := (S_r[r+1] = N-1), \quad B := (Z_{r+1} = Z_r), \quad C := (Z_{r+1} = r+2).$$

The target event seems a simple combination of Theorem 3.17 and Corollary 3.1. However, it is not actually the case. $\Pr(A \mid B \wedge C)$ is difficult to compute because the events B and C are not independent. To avoid this problem, we further define a new event $B' := (Z_r = r+2)$. Then, $\Pr(A \mid B \wedge C) = \Pr(A \mid B' \wedge C)$ because the events $(B \wedge C)$ and $(B' \wedge C)$ are the same, and therefore we will compute the target probability easily. Note here that

$$\Pr(A \mid B' \wedge C) = \frac{\Pr(A \wedge B' \wedge C)}{\Pr(B' \wedge C)} = \frac{\Pr(C \mid B' \wedge A) \cdot \Pr(B' \mid A) \cdot \Pr(A)}{\Pr(B' \wedge C)}.$$

Now, we first compute $\Pr(C \mid B' \wedge A)$. Note that the event A implies $Z_{r+1} = S_{r+1}[S_{r+1}[r+1] + S_r[r+1]] = S_{r+1}[S_{r+1}[r+1] - 1]$, and the event B' implies $Z_r = S_r[t_r] = r+2$. We then consider the following two paths: $S_{r+1}[r+1] = r+2$ (Path 1) and $S_{r+1}[r+1] = t_r + 1$ (Path 2).

Path 1: We have $Z_{r+1} = S_{r+1}[(r+2)-1] = S_{r+1}[r+1] = r+2$ with probability 1.

Path 2: We have $Z_{r+1} = S_{r+1}[(t_r+1)-1] = S_{r+1}[t_r] = S_r[t_r] = r+2$ with probability approximately 1, except when t_r is equal to either i_{r+1} or j_{r+1}.

In almost all other cases, we assume that the event C occurs with probability of random association $\frac{1}{N}$. Therefore, we compute $\Pr(C \mid B' \wedge A)$ as

$$\begin{aligned}
&\Pr(C \mid B' \wedge A \wedge (S_{r+1}[r+1] = r+2)) \cdot \Pr(S_{r+1}[r+1] = r+2)) \\
&\quad + \Pr(C \mid B' \wedge A \wedge (S_{r+1}[r+1] = t_r+1)) \cdot \Pr(S_{r+1}[r+1] = t_r+1)) \\
&\quad + \sum_{X \neq r+2, t_r+1} \Pr(C \mid B' \wedge A \wedge (S_{r+1}[r+1] = X)) \cdot \Pr(S_{r+1}[r+1] = X)) \\
&\quad \approx 1 \cdot \frac{1}{N} + 1 \cdot \frac{1}{N} + \left(1 - \frac{2}{N}\right) \cdot \frac{1}{N} \approx \frac{3}{N}.
\end{aligned}$$

Next, we assume that the event $(B' \mid A)$ occurs with probability of random association $\frac{1}{N}$ because no study has been reported on correlations between $S_r[r+1]$ and Z_r in the literature, and we further assume $\Pr(A) \approx \frac{1}{N}$ according to pseudorandomness of stream ciphers. Thus,

$$\Pr(A \wedge B' \wedge C) = \Pr(C \mid B' \wedge A) \cdot \Pr(B' \mid A) \cdot \Pr(A) \approx \frac{3}{N} \cdot \frac{1}{N} \cdot \frac{1}{N}.$$

Finally, We assume that $\Pr(B' \wedge C) = \Pr(B') \cdot \Pr(C) \approx \frac{1}{N} \cdot \frac{1}{N}$, and therefore we obtain the probability of the target event as $\Pr(A \mid B \wedge C) = \Pr(A \mid B' \wedge C) \approx \frac{3}{N}$. □

3.1.4 Key Correlations of the Internal State Variables

In [Roo95], Roos experimentally presented significant correlations between the initial state variables S_0 and the RC4 key bytes K as Equation (3.4), and provided the experimental results as listed in Table 3.4. Such correlations are called the *Roos Biases*.

$$S_0[i] = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x] \quad \text{for } 0 \leq i \leq 47. \tag{3.4}$$

In [PM07], Paul and Maitra provided a complete proof of the Roos Biases as Theorem 3.19. The proof of Theorem 3.19 uses Lemmas 3.5 and 3.6. They further provided the theoretical result of the Roos Biases as listed in Table 3.5.

Lemma 3.5 ([PM07, Lemma 1]). *Assume that the index j_r^K takes its values from $\{0, 1, \ldots, N-1\}$ uniformly at random at each round of the KSA. Then,*

$$\Pr(j_{i+1}^K = \sum_{x=0}^{i} S_0^K[x] + \sum_{x=0}^{i} K[x]) \approx \left(1 - \frac{1}{N}\right)^{1+\frac{i(i+1)}{2}} + \frac{1}{N}.$$

Table 3.4: Experimental observations of the Roos Biases.

i	$\Pr(S_0[i] = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x])$							
0–7	0.370	0.368	0.362	0.358	0.349	0.340	0.330	0.322
8–15	0.309	0.298	0.285	0.275	0.260	0.245	0.229	0.216
16–23	0.203	0.189	0.173	0.161	0.147	0.135	0.124	0.112
24–31	0.101	0.090	0.082	0.074	0.064	0.057	0.051	0.044
32–39	0.039	0.035	0.030	0.026	0.023	0.020	0.017	0.014
40–47	0.013	0.012	0.010	0.009	0.008	0.007	0.006	0.006

Table 3.5: Theoretical probabilities of the Roos Biases.

i	$\Pr(S_N^K[i] = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x])$							
0–7	0.371	0.368	0.364	0.358	0.351	0.343	0.334	0.324
8–15	0.313	0.301	0.288	0.275	0.262	0.248	0.234	0.220
16–23	0.206	0.192	0.179	0.165	0.153	0.140	0.129	0.117
24–31	0.107	0.097	0.087	0.079	0.071	0.063	0.056	0.050
32–39	0.045	0.039	0.035	0.031	0.027	0.024	0.021	0.019
40–47	0.016	0.015	0.013	0.011	0.010	0.009	0.008	0.008

Corollary 3.2 ([PM07, Corollary 1]). *If the initial permutation is the identity permutation, i.e., $S_0^K[i] = i$ for $0 \leq i \leq N-1$, then*

$$\Pr(j_{i+1}^K = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]) \approx \left(1 - \frac{1}{N}\right)^{1+\frac{i(i+1)}{2}} + \frac{1}{N}.$$

Lemma 3.6 ([PM07, Lemma 2]). *Assume that the index j_r^K takes its values from $\{0, 1, \ldots, N-1\}$ uniformly at random at each round of the KSA. Then,*

$$\Pr(S_N^K[i] = S_0^K[j_{i+1}^K]) \approx \left(1 - \frac{i}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{N-1}.$$

Theorem 3.19 ([PM07, Theorem 1]). *Assume that the index j_r^K takes its values from $\{0, 1, \ldots, N-1\}$ uniformly at random at each round of the KSA. Then,*

$$\Pr\left(S_N^K[i] = S_0\left[\sum_{x=0}^{i} S_0^K[x] + \sum_{x=0}^{i} K[x]\right]\right) \approx \left(1 - \frac{i}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{[\frac{i(i+1)}{2}+N]} + \frac{1}{N}.$$

Corollary 3.3 ([PM07, Corollary 2]). *The probability that the initial permutation S_0 is biased toward the secret key is given by*

$$\Pr(S_0[i] = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]) \approx \left(1 - \frac{i}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{[\frac{i(i+1)}{2}+N]} + \frac{1}{N}.$$

In [MP08b], Maitra and Paul extended the Roos Biases as Equation (3.5), and provided a theoretical proof of the biases as Theorem 3.20. The extended Roos Biases are called the *Nested Roos Biases*. The proof of Theorem 3.20 uses Lemmas 3.7 and 3.8.

$$S_0[S_0[i]] = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]. \tag{3.5}$$

Lemma 3.7 ([MP08b, Lemma 5]). *Let $f_i = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]$ for $0 \leq i \leq 31$, we have*

$$\Pr((S_{i+1}^K[S_{i+1}^K[i]] = f_i) \wedge (S_{i+1}^K[i] \leq i)) \approx \left(\frac{1}{N} \cdot \left(1 - \frac{1}{N}\right)^{\frac{i(i+1)}{2}}\right) \cdot \left(i\left(1 - \frac{2}{N}\right)^{i-1} + \left(1 - \frac{1}{N}\right)^{i}\right).$$

Lemma 3.8 ([MP08b, Lemma 6]). *Let $f_i = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]$ and $p_r(i) = \Pr((S_r^K[S_r^K[i]] = f_i) \wedge (S_r^K[i] \leq r-1))$ for $0 \leq i \leq 31$ and $y + 2 \leq r \leq N$, we have*

$$p_r(i) = \left(1 - \frac{2}{N}\right) p_{r-1}(i) + \frac{1}{N} \cdot \left(1 - \frac{y}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{\frac{i(i+1)}{2}+2r-3}.$$

Theorem 3.20 ([MP08b, Theorem 2]). *Let* $f_i = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]$*, for* $0 \le r \le 31$*, we have*

$$\Pr(S_0[S_0[i]] = f_i) \approx \frac{i}{N}\cdot\left(1-\frac{1}{N}\right)^{\frac{i(i+1)}{2}+2(N-2)} + \frac{1}{N}\cdot\left(1-\frac{1}{N}\right)^{\frac{i(i+1)}{2}-i+2(N-1)} + \left(1-\frac{i+1}{N}\right)\cdot\left(1-\frac{i}{N}\right)\cdot\left(1-\frac{1}{N}\right)^{\frac{i(i+1)}{2}+2N-3}.$$

3.1.5 Key Correlations of the Keystream Bytes

In [SVV10], Sepehrdad et al. investigated key correlations of the keystream bytes Z_r by using a linear form

$$(a_0 \cdot K[0] + \cdots + a_{\ell-1} \cdot K[\ell-1] + a_\ell \cdot Z_1 + \cdots + a_{2\ell-1} \cdot Z_\ell) \bmod N = b, \tag{3.6}$$

where $a_i \in \{-1, 0, 1\}$ for $0 \le i \le 2\ell-1$. The number of equations is approximately $N \cdot 3^{2\ell} = 2^{58.7}$ for $N = 256$ and $\ell = 16$, which is too large for an exhaustive search. Then, they reduced the RC4 key size to $\ell = 5$ bytes, and obtained approximately $2^{23.8}$ equations for an exhaustive search. They showed 18 key correlations of the keystream bytes (including the existing ones) with the RC4 key length of 5 bytes as listed in Table 3.6, which have been experimentally confirmed with the RC4 key length of 16 bytes.

In [Sar14], Sarkar theoretically proved the key correlations of the keystream bytes $\{Z_1, Z_3, Z_4\}$ reported in [SVV10] as Theorem 3.21, Proposition 3.1, and Proposition 3.2. We introduce their proofs.

Table 3.6: Experimentally observed key correlations of the keystream bytes.

Key Correlations	Probability	Reference
$Z_1 + K[0] + K[1] = 0$	$1.35779/N$	[Kle08]
$Z_1 - K[0] = 0$	$1.11784/N$	[MP08b]
$Z_2 = 0$	$2.01825/N$	[MS01]
$Z_2 + K[0] + K[1] + K[2] = -1$	$1.36095/N$	[Kle08]
$Z_1 - K[0] - K[1] = 1$	$1.04237/N$	[SVV10]
$Z_1 - K[0] + K[1] = -1$	$1.04969/N$	[SVV10]
$Z_3 + K[0] + K[1] + K[2] + K[3] = -3$	$1.35362/N$	[Kle08]
$Z_3 - K[0] + K[3] = -3$	$1.04620/N$	[SVV10]
$Z_1 - K[0] - K[1] - K[2] = 3$	$1.33474/N$	[Roo95]
$Z_2 - K[0] - K[1] - K[2] = 3$	$0.64300/N$	[SVV10]
$Z_3 - K[0] - K[1] - K[2] = 3$	$1.13555/N$	[MP08b]
$Z_2 + K[1] + K[2] = -3$	$1.36897/N$	[SVV10]
$Z_2 - K[1] - K[2] = 3$	$1.36733/N$	[SVV10]
$Z_1 - K[2] = 3$	$1.14193/N$	[SVV10]
$Z_1 + K[0] + K[1] - K[2] = 3$	$1.14116/N$	[SVV10]
$Z_4 - K[0] + K[4] = -4$	$1.04463/N$	[SVV10]
$Z_4 + K[0] + K[1] + K[2] + K[3] + K[4] = -6$	$1.35275/N$	[Kle08]
$Z_4 - K[0] - K[1] - K[2] - K[3] = 10$	$1.11432/N$	[MP08b]

Theorem 3.21 ([Sar14, Theorem 4]). *For any arbitrary secret key K, a key correlation of the keystream byte Z_1 is given by*

$$\Pr(Z_1 = K[0] - K[1] - 1) \approx \alpha_1 + \frac{1}{N}(1 - \alpha_1),$$

where $\alpha_1 = \frac{1}{N^2} \cdot (1 - \frac{2}{N}) \cdot (1 - \frac{1}{N})^{N-2} \sum_{x=2}^{N-1} (1 - \frac{1}{N})^x \cdot (1 - \frac{1}{N})^{x-2} \cdot (1 - \frac{2}{N})^{N-x-1}$.

Proof. The major path for the target event is considered as follows:

- We assume that $K[0] \neq 0, 1$ and $K[1] = N - 1$. This occurs with probability $\frac{1}{N}\left(1 - \frac{2}{N}\right)$.
- After the second round of the KSA, $S_2^K[1] = 0$ since $j_2^K = K[0] + K[1] + 1 = K[0] - (K[1] + 1) = K[0]$.
- From the third to the final round of the KSA, none of j^K values equal to 1. This occurs with probability approximately $(1 - \frac{1}{N})^{N-2}$.
- For $x \in [2, N-1]$, we assume that $S_x^K[x] = x$. This occurs with probability approximately $(1 - \frac{1}{N})^x$.
- From the third to the x-th round of the KSA, the j^K values do not touch the indices 0. This occurs with probability approximately $(1 - \frac{1}{N})^{x-2}$.
- In the $x+1$-th round of the KSA, j_{x+1}^K becomes 0 with probability $\frac{1}{N}$ when $i = x$. Due to the swap operation, $S_{x+1}^K[0] = x$.
- For the remaining $N - x - 1$ rounds of the KSA, none of j^K values should touch the indices $\{0, x\}$. This occurs with probability approximately $(1 - \frac{2}{N})^{N-x-1}$.
- Finally, after the KSA, we have $S_0[0] = x$, $S_0[1] = 0$, and $S_0[x] = K[0]$.

If all the individual events hold, Z_1 is always equal to $K[0] - K[1] - 1 = K[0]$ as $K[1] = N - 1$. We assume that all the individual events in the above path to be mutually independent, we obtain the probability of all events hold is $\alpha_1 = \frac{1}{N^2} \cdot (1 - \frac{2}{N}) \cdot (1 - \frac{1}{N})^{N-2} \sum_{x=2}^{N-1} (1 - \frac{1}{N})^x \cdot (1 - \frac{1}{N})^{x-2} \cdot (1 - \frac{2}{N})^{N-x-1} = 0.000194$ when $N = 256$. Experimentally we have $\alpha_1 = 0.000185(\pm 6\%)$, which supports this result.

For the complimentary path, we assume that Z_1 is equal to $K[0] - K[1] - 1$ with probability $\frac{1}{N} = 0.003906$ of random association. Our experiments show that this probability is $0.003845(\pm 1\%)$ for the complimentary path, which supports our assumption.

Adding the contribution from both paths, we obtain $\Pr(Z_1 = K[0] - K[1] - 1) = \alpha_1 + \frac{1}{N}(1 - \alpha_1) = \frac{1.05}{N} = 0.004101$, when $N = 256$. □

Proposition 3.1 ([Sar14, Theorem 8]). *For any arbitrary secret key K, a key correlation of the keystream byte Z_3 is given by*

$$\Pr(Z_3 = K[0] - K[3] - 3) \approx \alpha_3 + \frac{1}{N}(1 - \alpha_3),$$

where $\alpha_3 = \frac{N^3-11N^2+42N-55}{N^4} \cdot (1-\frac{1}{N})^{N-4} \cdot \frac{N^2-3N+2}{N^2}) \cdot \frac{1}{N}\sum_{x=4}^{N-1}(1-\frac{1}{N})^x \cdot (1-\frac{1}{N})^{x-4} \cdot (1-\frac{2}{N})^{N-x-1}$.

Proof. The major path for the target event is considered as follows:

- We assume that $K[0] \notin \{1,2,3\}$, $3+K[0]+K[1]+K[2] \notin \{0,1,3\}$, $K[2] \neq N-2$, $3+K[1]+K[2] = 0$, $1+K[0]+K[1] \notin \{2,3\}$, $K[1] \neq N-1$, and $-K[1]-K[2]-K[3] = 6$. This occurs with probability $\frac{N^3-11N^2+42N-55}{N^4}$.
- Due to above conditions, after the third round of the KSA, $S_3^K[2] = 3+K[0]+K[1]+K[2]$ and $S_3^K[3] = 3$, and then $j_4^K = 6+K[0]+K[1]+K[2]+K[3] = K[0]$ because $-K[1]-K[2]-K[3] = 6$. Hence, we have $S_4^K[3] = 0$.
- From the fifth to the final round of the KSA, none of j^K values equal to 3. This occurs with probability approximately $(1-\frac{1}{N})^4$.
- For $x \in [4, N-1]$, we assume that $S_x^K[x] = x$. This occurs with probability approximately $(1-\frac{1}{N})^x$.
- From the fifth to the x-th round of the KSA, j^K values do not touch the indices 2. This occurs with probability approximately $(1-\frac{1}{N})^{x-4}$.
- In the $x+1$-th round of the KSA, j_{x+1}^K becomes 2 with probability $\frac{1}{N}$ when $i = x$. Due to the swap operation, $S_{x+1}^K[2] = x$.
- For the remaining $N-x-1$ rounds of the KSA, none of j^K values should touch the indices $\{2, x\}$. This occurs with probability approximately $(1-\frac{2}{N})^{N-x-1}$.
- After the KSA, we have $S_0[2] = x$, $S_0[3] = 0$, and $S_0[x] = 3+K[0]+K[1]+K[2] = -3+K[0]-K[3]$.
- Let $S_0[1] + S0[2] \neq 3$ and $S_0[1] \notin \{2,3\}$. This occurs with probability approximately $\frac{N^2-3N+2}{N^2}$.

If all the individual events hold, Z_3 is always equal to $K[0]-K[3]-3$.

We assume that all the individual events in the above path to be mutually independent, we obtain the probability of all events as $\alpha_3 = \frac{N^3-11N^2+42N-55}{N^4} \cdot (1-\frac{1}{N})^{N-4} \cdot \frac{N^2-3N+2}{N^2}) \cdot \frac{1}{N}\sum_{x=4}^{N-1}(1-\frac{1}{N})^x \cdot (1-\frac{1}{N})^{x-4} \cdot (1-\frac{2}{N})^{N-x-1} = 0.000187$ when $N = 256$. Experimentally we have $\alpha_3 = 0.000185(\pm 6\%)$, which supports this result.

For the complimentary path, we assume that Z_3 is equal to $K[0]-K[3]-3$ with probability $\frac{1}{M} = 0.003906$ of random association. Our experiments show that this probability is $0.003904(\pm 1\%)$ for the complimentary path.

Adding the contribution from both paths, we obtain $\Pr(Z_3 = K[0]-K[3]-3) = \alpha_3 + \frac{1}{N}(1-\alpha_3) = \frac{1.05}{N} = 0.004101$, when $N = 256$. □

Proposition 3.2 ([Sar14, Theorem 9]). *For any arbitrary secret key K, a key correlation of the keystream byte Z_4 is given by*

$$\Pr(Z_4 = K[0] - K[4] - 4) \approx \alpha_4 + \frac{1}{N}(1 - \alpha_4),$$

where $\alpha_4 = \frac{N^4-18N^3+124N^2-385N+452}{N^5} \cdot (1-\frac{1}{N})^{N-5} \cdot \frac{N^3-8N^2+21N-18}{N^3} \cdot \frac{1}{N}\sum_{x=5}^{N-1}(1-\frac{1}{N})^{x} \cdot (1-\frac{1}{N})^{x-5} \cdot (1-\frac{2}{N})^{N-x-1}$.

Proof. The major path for the target event is considered as follows:

- We assume that $K[0] \notin \{1,2,3,4\}$, $-4+K[0]-K[4] \notin \{0,1,2\}$, $1+K[0]+K[1] \notin \{2,3,4\}$, $3+K[0]+K[1]+K[2] \notin \{3,4\}$, $6+K[0]+K[1]+K[2]+K[3] \neq 4$, $K[1] \neq N-1$, $K[2]+K[3] \neq N-5$, $K[3] \neq N-3$, $K[1]+K[2] \neq N-3$, $K[1]+K[2]+K[3] \neq N-6$, and $-K[1]-K[2]-K[3]-K[4] = 10$. This occurs with probability $\frac{N^4-18N^3+124N^2-385N+452}{N^5}$.
- Due to above conditions, after fourth round of the KSA, $S_4^K[3] = 6+K[0]+K[1]+K[2]+K[3]$ and $S_4^K[4] = 4$, and then $j_5^K = K[0]$ because $-K[1]-K[2]-K[3]-K[4] = 10$. Hence, we have $S_5^K[4] = 0$.
- From the sixth to the final round of the KSA, none of j^K values equal to 4. This occurs with probability approximately $(1-\frac{1}{N})^{N-5}$.
- For $x \in [5, N-1]$, we assume that $S_x^K[x] = x$. This occurs with probability approximately $(1-\frac{1}{N})^{x}$.
- From the sixth to the x-th round of the KSA, j^K values do not touch the indices 3. This occurs with probability approximately $(1-\frac{1}{N})^{x-5}$.
- In the $x+1$-th round of the KSA, j_{x+1}^K becomes 3 with probability $\frac{1}{N}$ when $i = x$, Due to the swap operation, $S_{x+1}^K[3] = x$.
- For the remaining $N-x-1$ rounds of the KSA, none of j^K values should touch the indices $\{3, x\}$. This occurs with probability approximately $(1-\frac{2}{N})^{N-x-1}$.
- After the KSA, we have $S_N^K[3] = x$, $S_N^K[4] = 0$, and $S_N^K[x] = 6+K[0]+K[1]+K[2]+K[3] = K[0]-K[4]-4$.
- $S_0[1]+S0[2] \neq 3$, $S_0[1]+S0[2] \neq 4$, $S_0[1]+S_0[2]+S_0[3] \neq 4$, $S_0[1] \notin \{2,3,4\}$, $S_0[1]+S_0[2] \neq x$, and $S_0[1]+S_0[2]+S_0[3] \neq x$. This occurs with probability approximately $\frac{N^3-8N^2+21N-18}{N^3}$.

If all the individual events hold, Z_4 is always equal to $K[0]-K[4]-4$.

We assume that all individual events in the above path to be mutually independent, we obtain the probability of all events as $\alpha_4 = \frac{N^4-18N^3+124N^2-385N+452}{N^5} \cdot (1-\frac{1}{N})^{N-5} \cdot \frac{N^3-8N^2+21N-18}{N^3} \cdot \frac{1}{N}\sum_{x=5}^{N-1}(1-\frac{1}{N})^{x} \cdot (1-\frac{1}{N})^{x-5} \cdot (1-\frac{2}{N})^{N-x-1} = 0.000179$ when $N = 256$. Experimentally we have $\alpha_4 = 0.000178(\pm 7\%)$, which supports this result.

Table 3.7: Experimentally observed key correlations of the keystream bytes in both generic RC4 and WPA-TKIP.

Key Correlations	RC4	WPA-TKIP
$Z_1 = -K[0] - K[1]$	0.005264	0.005338
$Z_1 = K[0]$	0.004325	0.004179
$Z_1 = K[0] + K[1] + K[2] + 3$	0.005220	0.004633
$Z_1 = K[0] + K[1] + 1$	0.004025	0.003760
$Z_1 = K[0] - K[1] - 1$	0.004083	0.003905
$Z_1 = K[2] + 3$	0.004428	0.003902
$Z_1 = -K[0] - K[1] + K[2] + 3$	0.004424	0.003903
$Z_2 = -K[0] - K[1] - K[2] - 1$	0.005298	0.005303
$Z_2 = -K[1] - K[2] - 3$	0.005303	0.005314
$Z_2 = K[1] + K[2] + 3$	0.005304	0.005315
$Z_2 = K[0] + K[1] + K[2] + 3$	0.002507	0.002503
$Z_3 = K[0] + K[1] + K[2] + 3$	0.004401	0.004405
$Z_{256} = -K[0]$	0.004427	0.004429
$Z_{256} = -K[1]$	0.003907	0.004036
$Z_{257} = -K[0] - K[1]$	0.004096	0.004094

For the complimentary path, we assume that Z_4 is equal to $K[0] - K[4] - 4$ with probability $\frac{1}{N} = 0.003906$ of random association. Our experiments show that this probability is $0.003902(\pm 1\%)$ for the complimentary path.

Thus, $\Pr(Z4 = K[0] - K[4] - 4) = \alpha_4 + \frac{1}{N}(1 - \alpha_4) = \frac{1.04}{N} = 0.004062$, when $N = 256$. We obtain experimentally $\Pr(Z_4 = K[0] - K[4] - 4) = 0.004077 = \frac{1.04}{N}$. □

In [GMM+14], Sen Gupta et al. investigated significant correlations between the keystream bytes Z_r and the known RC4 key bytes $\{K[0], K[1], K[2]\}$ in WPA-TKIP by using a linear form

$$Z_r = a \cdot K[0] + b \cdot K[1] + c \cdot K[2] + d \tag{3.7}$$

for $a, b, c \in \{0, \pm 1\}$ and $d \in \{0, \pm 1, \pm 2, \pm 3\}$ for $r \geq 1$. They experimentally observed the most significant key correlations of the keystream bytes (including the existing ones), as listed in Table 3.7. Actually, these key correlations can be updated to the set of the strongest short-term biases for the keystream bytes (see Table 3.1).

3.2 Plaintext Recovery Attacks

A plaintext recovery attack aims to recover a plaintext under the scenario of the ciphertext-only attack in the *broadcast setting*, where the same plaintext is encrypted with different randomly chosen keys. This section describes the previous works on plaintext recovery attacks in the broadcast setting with respect to the following aspects:

Section 3.2.1: Plaintext Recovery Attacks on Generic RC4 in [MS01, IOWM13, ABP+13]

Section 3.2.2: Plaintext Recovery Attacks on WPA-TKIP in [GMM+14, PPS14]

Although many other attacks have been reported, e.g., in [GPdM15, IOWM14, MPG11, OIWM13, OIWM15, PS18, VP15, WIOM17], we will not describe these attacks in this section because these are out of our cryptanalysis and discussions in this dissertation.

3.2.1 Plaintext Recovery Attacks on Generic RC4

The Mantin-Shamir (MS) attack

In [MS01], Mantin and Shamir first presented the plaintext recovery attack in the broadcast setting, and demonstrated how to recover the second byte of a plaintext in the broadcast setting as Theorem 3.22.

Theorem 3.22 ([MS01, Theorem 3])**.** *Let P be a plaintext and $C^{(1)}, \ldots, C^{(k)}$ be k ciphertexts obtained by the RC4 encryptions of P with different randomly chosen keys. Then, if $k = \Omega(N)$, the second byte of the plaintext P_2 can be reliably extracted from $C^{(1)}, \ldots, C^{(k)}$.*

If $Z_2^{(i)} = 0$, then P_2 has the same value as $C_2^{(i)}$ because P_2 is XORed with $Z_2^{(i)}$ to output $C_2^{(i)}$ in the RC4 encryptions. From Theorem 3.1, the event $(Z_2 = 0)$ occurs with relatively high probability in comparison with the other events. Thus, we can recover P_2 by exploiting the most frequent value in the distribution of $C_2^{(1)}, \ldots, C_2^{(k)}$. From Theorem 3.2, the number of samples for recovering P_2 requires more than $\mathcal{O}(N)$ ciphertexts encrypted with randomly chosen keys.

The Isobe-Ohigashi-Watanabe-Morii (IOWM) attack

In [IOWM13], Isobe et al. demonstrated a practical plaintext recovery attack by using their provided set of the strongest short-term biases (see Table 3.1), given by the following four steps:

Step 1. Randomly generate a target plaintext P.

Step 2. Obtain 2^x ciphertexts C by encrypting P with different randomly chosen keys.

Step 3. Exploit the most/least frequent value in the distribution of C_r.

Step 4. Recover P_r by using the set of the strongest short-term biases of the keystream bytes.

According to their experimental results, the first 257 bytes of the plaintext can be recovered with probability more than 80% by using 2^{32} ciphertexts in the broadcast setting.

The AlFardan-Bernstein-Paterson-Poettering-Schuldt (ABPPS) attack

In [ABP+13], AlFardan et al. proposed a plaintext recovery algorithm that considers all possible short-term biases at the same time, given by the following four steps:

Step 1. Estimate the accurate distributions of the keystream bytes Z_r in the first 257 rounds:

$$p_{r,k} := \Pr(Z_r = k) \text{ for } k = \text{0x00, ..., 0xFF},$$

where the probability is taken from randomly chosen keys.

Algorithm 5 Short-term bias attack in [ABP+13]

```
Input: $\{C_j\}_{1\leq j\leq S}$: $S$ ciphertexts by encrypting the same plaintext $P$,
    $r$: the number of rounds,
    $p_{r,k}$: the accurate distribution of the keystream $Z_r$ at round $r$.
Output: $P_r^*$: estimate for plaintext byte $P_r$.
$N_{0x00} \leftarrow 0, \ldots, N_{0xFF} \leftarrow 0$
for $j$ from 1 to $S$ do
    $N_{C_{j,r}} \leftarrow N_{C_{j,r}} + 1$
end for
for $\mu$ from 0x00 to 0xFF do
    for $k$ from 0x00 to 0xFF do
        $N_k^{(\mu)} \leftarrow N_{k\oplus\mu}$
    end for
    $\lambda_\mu \leftarrow \sum_{k=0x00}^{0xFF} N_k^{(\mu)} \log p_{r,k}$
end for
$P_r^* \leftarrow \arg\max_{\mu\in\{0xFF,\ldots,0xFF\}} \lambda_\mu$
```

Step 2. Assuming that we obtain S ciphertexts $\{C_1, \ldots, C_S\}$ for the attack in the broadcast setting. Let $C_{j,r}$ be the r-th round of ciphertext C_j. For any candidate plaintext byte μ in each round, the vector $(N_{0x00}^{(\mu)}, ..., N_{0xFF}^{(\mu)})$ with

$$N_k^{(\mu)} = |\{j \mid C_{j,r} = k \oplus \mu\}_{1\leq j\leq S}| \text{ for } k = 0x00, ..., 0xFF$$

represents the induced distribution of the keystream bytes Z_r obtained from $\{C_{j,r}\}_{1\leq j\leq S}$ and μ.

Step 3. Calculate the probability λ_μ that the candidate plaintext byte μ is correctly encrypted into the ciphertext bytes $\{C_{j,r}\}_{1\leq j\leq S}$ as

$$\lambda_\mu = \frac{S!}{N_{0x00}^{(\mu)}! \cdots N_{0xFF}^{(\mu)}!} \prod_{k\in\{0x00,\ \ldots,\ 0xFF\}} p_{r,k}^{N_k^{(\mu)}},$$

where λ_μ follows the multinomial distribution with parameter S and $(p_{r,0x00}, \ldots, p_{r,0xFF})$ (see Definition 2.6).

Step 4. Determine the maximum-likelihood plaintext byte value P_r^* by calculating λ_μ for all $0x00 \leq \mu \leq 0xFF$ and then distinguishing μ such that λ_μ is the maximum value.

The details of the ABPPS attack are described as Algorithm 5.

3.2.2 Plaintext Recovery Attacks on WPA-TKIP

The Sen Gupta-Maitra-Meier-Paul-Sarkar (SMMPS) attack

In [GMM+14], Sen Gupta et al. presented that their exploited key correlations of the keystream bytes (see Table 3.7) can improve the plaintext recovery attack on WPA-TKIP in the same way

Table 3.8: Experimental results for recovering four bytes of a plaintext on WPA-TKIP. The probability of success in each case is approximately 100%.

Round	Key correlations	# of ciphertexts
1	$Z_1 = -K[0] - K[1]$ $Z_1 = K[0] + K[1] + K[2] + 3$	$5 \cdot 2^{13} \approx 2^{15.322}$
3	$Z_3 = K[0] + K[1] + K[2] + 3$	2^{19}
256	$Z_{256} = -K[0]$	2^{19}
257	$Z_{257} = -K[0] - K[1]$	2^{21}

as the IOWM attack in [IOWM13] when the key correlations induce higher biases than certain events used in the IOWM attack.

Table 3.8 shows their experimental results for the plaintext recovery attack on WPA-TKIP. Their results show significant improvement for recovering four bytes of a plaintext $\{P_1, P_3, P_{256}, P_{257}\}$, where the IOWM attack requires approximately 2^{30} ciphertexts encrypted by randomly chosen keys to achieve the same probability of success.

The Paterson-Poettering-Schuldt (PPS) attack

In [PPS14], Paterson et al. extended the ABPPS attack in [ABP+13] by using all the IV pairs in WPA-TKIP. Let the least and the most significant 8-bit $\mathtt{IV16}$ be denoted by $\mathtt{IV}_0$ and $\mathtt{IV}_1$, respectively, and $\overline{\mathtt{IV}} = (\mathtt{IV}_0, \mathtt{IV}_1)$. Their extended attack algorithm consists of the following five steps:

Step 1. Estimate accurate distributions of the keystream bytes Z_r in the first 257 rounds on a per $(\mathtt{IV}_0, \mathtt{IV}_1)$ pair basis:

$$p_{\overline{\mathtt{IV}},r,k} := \Pr(Z_r = k) \text{ for } \overline{\mathtt{IV}} = (\text{0x00}, \text{0x00}), \ldots, (\text{0xFF}, \text{0xFF}) \text{ and } k = \text{0x00, ..., 0xFF},$$

where the probability is taken from randomly chosen keys.

Step 2. Assuming that we obtain S ciphertexts $\{C_1, \ldots, C_S\}$ for the attack in the broadcast setting. Let $T = S/2^{16}$, let $\mathcal{S}_{\overline{\mathtt{IV}}}$ be the bin of ciphertexts associated with a particular $\overline{\mathtt{IV}} = (\mathtt{IV}_0, \mathtt{IV}_1)$ pair and have members $C_{\overline{\mathtt{IV}},j}$ for $j = 1, \ldots, T$, and let $C_{\overline{\mathtt{IV}},j,r}$ be the r-th round of $C_{\overline{\mathtt{IV}},j}$. For any candidate plaintext byte μ in each round, the vector $(N^{(\mu)}_{\overline{\mathtt{IV}},\text{0x00}}, \ldots, N^{(\mu)}_{\overline{\mathtt{IV}},\text{0xFF}})$ with

$$N^{(\mu)}_{\overline{\mathtt{IV}},k} = |\{j \mid C_{\overline{\mathtt{IV}},j,r} = k \oplus \mu\}_{1 \le j \le T}| \text{ for } k = \text{0x00}, ..., \text{0xFF}$$

represents the induced distribution of the keystream bytes Z_r obtained from $\{C_{\overline{\mathtt{IV}},j,r}\}_{1 \le j \le T}$ and μ.

Step 3. Calculate the probability $\lambda_{\overline{\mathtt{IV}},\mu}$ that the candidate plaintext byte μ is encrypted into the ciphertext bytes $\{C_{\overline{\mathtt{IV}},j,r}\}_{1 \le j \le T}$ as

$$\lambda_{\overline{\mathtt{IV}},\mu} = \frac{T!}{N^{(\mu)}_{\overline{\mathtt{IV}},\text{0x00}}! \cdots N^{(\mu)}_{\overline{\mathtt{IV}},\text{0xFF}}!} \prod_{k \in \{\text{0x00}, \ldots, \text{0xFF}\}} p_{\overline{\mathtt{IV}},r,k}^{N^{(\mu)}_{\overline{\mathtt{IV}},k}},$$

Algorithm 6 Short-term bias attack in [PPS14]

```
Input: $\{C_{\overline{\mathtt{IV}},j}\}_{1 \le j \le T}$: $S = 2^{16} \cdot T$ ciphertexts by encrypting the same plaintext $P$,
    $r$: the number of rounds,
    $p_{\overline{\mathtt{IV}},r,k}$: the accurate keystream distribution of the keystream $Z_r$ at round $r$.
Output: $P_r^*$: estimate for plaintext byte $P_r$.
$N_{(\text{0x00, 0x00}),\ \text{0x00}} \leftarrow 0, \dots, N_{(\text{0xFF, 0xFF}),\ \text{0xFF}} \leftarrow 0$
for $\overline{\mathtt{IV}}$ from (0x00, 0x00) to (0xFF, 0xFF) do
    for $j$ from 1 to $T$ do
        $k \leftarrow C_{\overline{\mathtt{IV}},j,r}$
        $N_{\overline{\mathtt{IV}},k} \leftarrow N_{\overline{\mathtt{IV}},k} + 1$
    end for
end for
for $\overline{\mathtt{IV}}$ from (0x00, 0x00) to (0xFF, 0xFF) do
    $F_{\overline{\mathtt{IV}}} \leftarrow \sum_{\text{0x00} \le j \le \text{0xFF}} \log((N_{\overline{\mathtt{IV}},j})!)$
    for $\mu$ from 0x00 to 0xFF do
        for $k$ from 0x00 to 0xFF do
            $N^{(\mu)}_{\overline{\mathtt{IV}},k} \leftarrow N_{\overline{\mathtt{IV}},k \oplus \mu}$
        end for
        $\lambda_{\overline{\mathtt{IV}},\mu} \leftarrow -F_{\overline{\mathtt{IV}}} + \sum_{k=\text{0x00}}^{\text{0xFF}} N^{(\mu)}_{\overline{\mathtt{IV}},k} \log p_{\overline{\mathtt{IV}},r,k}$
    end for
end for
for $\mu$ from 0x00 to 0xFF do
    $\lambda_\mu \leftarrow \sum_{(\text{0x00, 0x00}) \le \overline{\mathtt{IV}} \le (\text{0xFF, 0xFF})} \lambda_{\overline{\mathtt{IV}},\mu}$
end for
$P_r^* \leftarrow \arg\max_{\mu \in \{\text{0xFF},\dots,\text{0xFF}\}} \lambda_\mu$
```

where $\lambda_{\overline{\mathtt{IV}},\mu}$ follows the multinomial distribution with parameter T and $(p_{\overline{\mathtt{IV}},r,\text{0x00}}, \dots, p_{\overline{\mathtt{IV}},r,\text{0xFF}})$ (see Definition 2.6).

Step 4. Further calculate the probability λ_μ that the candidate plaintext byte μ is encrypted into the ciphertext bytes $\{C_{\overline{\mathtt{IV}},j,r}\}_{1 \le j \le T}$ across all bins $\mathcal{S}_{\overline{\mathtt{IV}}}$ as

$$\lambda_\mu = \prod_{(\text{0x00, 0x00}) \le \overline{\mathtt{IV}} \le (\text{0xFF, 0xFF})} \lambda_{\overline{\mathtt{IV}},\mu}.$$

Step 5. Determine the maximum-likelihood plaintext byte value P_r^* by calculating λ_μ for all $\text{0x00} \le \mu \le \text{0xFF}$ and then distinguishing μ such that λ_μ is the maximum value.

The details of the PPS attack are described as Algorithm 6.

3.3 Key Recovery Attacks

A key recovery attack is to recover a secret key from a keystream under the scenario of the known plaintext attack, and aims to confirm the difficulty in recovering a secret key in the ciphers. This section describes the previous works on the key recovery attacks with respect to the following aspects:

Section 3.3.1: Key Recovery Attack Using the Roos Biases in [PM07]

Section 3.3.2: Key Recovery Attack Using Key Correlations of the Keystream Bytes in [SVV10]

Section 3.3.3: Key Recovery Attack on WEP Using Weak IVs in [FMS01]

Section 3.3.4: Key Recovery Attack on WEP without Using Weak IVs in [Kle08]

Although many other attacks have been reported, e.g., in [PM09, SVV11, SSVV13, TWP08, TAO$^+$10, VV07], we will not describe these attacks in this section because these are out of our cryptanalysis and discussions in this dissertation.

3.3.1 Key Recovery Attack Using the Roos Biases

In [PM07], Paul and Maitra proposed an attack algorithm for recovering the RC4 key bytes from the knowledge of the internal state variables by using certain events with the Roos biases (see Theorem 3.19). If the internal state at any round of the KSA is known, then we can recover the RC4 key bytes by solving simultaneous equations based on the Roos biases in much less time than the exhaustive key search algorithm.

Before showing their attack algorithm, we introduce the following example (refer to [PM07] for details):

Example 3.1 ([PM07, Example 2]). *Assume that the RC4 key size is five bytes. Let* $f_i = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x]$. *We would consider all possible sets of five equations chosen from 16 equations of the form* $S[i] = f_i$ *for* $0 \leq i \leq 15$, *and then try to solve them. One such set would correspond to i = 0, 1, 2, 3, and 13. Let the values of the corresponding* $S[i]$ *be 246, 250, 47, 204, and 185, respectively. Then, we can form the following equations:*

$$K[0] = 246 \tag{3.8}$$

$$K[0] + K[1] + (1 \cdot 2)/2 = 250 \tag{3.9}$$

$$K[0] + K[1] + K[2] + (2 \cdot 3)/2 = 47 \tag{3.10}$$

$$K[0] + K[1] + K[2] + K[3] + (3 \cdot 4)/2 = 204 \tag{3.11}$$

$$K[0] + \cdots + K[13] + (13 \cdot 14)/2 = 185 \tag{3.12}$$

From the first four equations, we simply obtain $K[0] = 246$, $K[1] = 3$, $K[2] = 51$, *and* $K[3] = 154$. *Because the key size is five bytes,* $K[5] = K[0], \ldots, K[9] = K[4]$, $K[10] = K[0], \ldots, K[13] = K[3]$. *Let s be the sum of the key bytes* $K[0] + \cdots + K[4]$, *we can rewrite Equation (3.12) as*

$$2s + K[0] + K[1] + K[2] + K[3] + 91 = 185 \tag{3.13}$$

Subtracting Equation (3.11) from Equation (3.13) and solving for s, we obtain $s = 76$ *or* 204. *Taking the value* $s = 76$, *we obtain*

$$K[0] + K[1] + K[2] + K[3] + K[4] = 76 \tag{3.14}$$

Algorithm 7 key recovery attack in [PM07]

```
Input: $l$: the number of key bytes.
    $m$ ($\leq l$): the number of key bytes to be solve from equations.
    $n$ ($\geq m$): the number of equations to be tried.
    $S_r^K[x]$: the internal state bytes, $0 \leq x \leq r-1$ and round $r$ for $n \leq r \leq N$.
Output: The recovered key bytes $K[0], K[1], \ldots, K[l-1]$, if they are found.
    Otherwise, the algorithm halts after trying all the system of equations.
for each distinct tuple $\{x_1, x_2, \ldots, x_m\}$, $0 \leq x_q \leq n-1$, $1 \leq q \leq m$ do
    if the tuple belongs to $m$ equations then
        Arbitrarily select any $m$ variables presented in the system;
        Solve for the $m$ variables in terms of the remaining $l-m$ variables;
        for each possible assignment of the $l-m$ variables do
            Find values of the other $m$ key bytes;
            if the correct key bytes are found then
                return $K[0], K[1], \ldots, K[l-1]$;
            end if
        end for
    end if
end for
```

Subtracting Equation (3.11) from Equation (3.14), we obtain $K[4] = 134$*. On the contrary, Taking the value* $s = 204$ *does not give the correct key, as can be verified by running the KSA and observing the initial state* S_0*.*

We now present their attack algorithm for recovering the RC4 key bytes from the initial state obtained after the completion of the KSA as Algorithm 7.

Paul and Maitra theoretically analyzed the key recovery attacks from the knowledge of the internal state. They demonstrated the attack with an optimized success probability of $2^{-2.43}$ and a time complexity of $2^{75.5}$. However, they also demonstrated the attack with an optimized time complexity of $2^{32.2}$ and a success probability of $2^{-10.7}$.

3.3.2 Key Recovery Attack Using Key Correlations of the Keystream Bytes

In [SVV10], Sepehrdad et al. experimentally observed key correlations of the keystream bytes, and summarized a list including the previous and their new key correlations as listed in Table 3.9. They further applied a list of useful key correlations of the keystream bytes in Table 3.9 to a theoretical key recovery attack on generic RC4. The success probability that all of the RC4 key bytes are recovered is

$$p \approx \prod_{i=0}^{l-1}\left(1 - \prod_{j=1}^{n_i}(1 - p_{i,j})\right), \tag{3.15}$$

where i is an index of a key byte, n_i is the number of equations in the i-th index to be tried, and $p_{i,j}$ is the probability of the j-th equation in the i-th index for the target key byte. In addition, let $m = \prod_{i=0}^{l-1} n_i$ be the number of combinations of key correlations to solve the simultaneous

Table 3.9: Useful key correlations of the keystream bytes for a theoretical key recovery attack on generic RC4 for $\ell = 16$. Let $\overline{K}[i] = K[0] + \cdots + K[i]$.

Equation	Probability	Reference
$Z_1 = \overline{K}[0]$	$1.10873/N$	[MP08b]
$Z_1 = -\overline{K}[1]$	$1.36467/N$	[VV07]
$Z_1 = \overline{K}[1] + 1$	$1.04237/N$	[SVV10]
$Z_2 = \overline{K}[2] + 3$	$0.64300/N$	[SVV10]
$Z_2 = -\overline{K}[2] - 1$	$1.36036/N$	[VV07]
$Z_3 = \overline{K}[2] + 3$	$1.12742/N$	[MP08b]
$\vdots$	$\vdots$	$\vdots$
$Z_{14} = -\overline{K}[14] + 165$	$1.22758/N$	[VV07]
$Z_{15} = \overline{K}[14] + 105$	$1.06444/N$	[MP08b]
$Z_{15} = -\overline{K}[15] + 151$	$1.06444/N$	[VV07]
$Z_{16} = \overline{K}[15] + 120$	$1.07519/N$	[MP08b]
$Z_{16} = \overline{K}[15] + \overline{K}[0] + 152$	$1.01838/N$	[SVV10]
$Z_{16} = -\overline{K}[15] - \overline{K}[0] + 104$	$1.01242/N$	[SVV10]
$Z_{16} = -\overline{K}[15] - \overline{K}[0] + 136$	$1.19880/N$	[VV07]
$Z_{17} = \overline{K}[15] + \overline{K}[0] + 120$	$1.07519/N$	[MP08b]
$\vdots$	$\vdots$	$\vdots$
$Z_{30} = -\overline{K}[15] - \overline{K}[14] + 77$	$1.04582/N$	[VV07]
$Z_{31} = \overline{K}[15] + \overline{K}[14] + 209$	$1.02118/N$	[MP08b]
$Z_{31} = -2\overline{K}[15] + 77$	$1.03963/N$	[VV07]
$Z_{32} = 2\overline{K}[15] + 240$	$1.03833/N$	[MP08b]
$Z_{32} = 2\overline{K}[15] + \overline{K}[0] + 48$	$1.00900/N$	[SVV10]
$Z_{32} = -2\overline{K}[15] - \overline{K}[0] + 208$	$1.00620/N$	[MP08b]
$Z_{32} = -2\overline{K}[15] - \overline{K}[0] + 240$	$1.03403/N$	[VV07]
$\vdots$	$\vdots$	$\vdots$
$Z_{46} = -2\overline{K}[15] - \overline{K}[14] + 57$	$1.00900/N$	[SVV10]
$Z_{47} = -3\overline{K}[15] + 199$	$1.00620/N$	[MP08b]

equations. Then, the time complexity of the attack is given by

$$c \approx \mathcal{O}(m^2) \tag{3.16}$$

because the time complexity of simultaneous linear equations with m unknowns is computed in a triangular form.

As a result, Sepehrdad et al. theoretically analyzed the key recovery attack from useful key correlations of the first 48-byte keystream bytes. They demonstrated the attack with an optimized success probability of $2^{-87.90}$ and a time complexity of $2^{38.09}$. However, they also demonstrated the attack with an optimized time complexity of 1 and a success probability of $2^{-122.06}$.

3.3.3 Key Recovery Attack on WEP Using Weak IVs

In [FMS01], Fluhrer et al. proposed a key recovery attack on WEP using the property of certain specific IV values, called *weak IVs*. In their attack, called the *FMS attack*, a byte of the RC4 key $K[A+3]$ can be derived when the first three bytes of the IV value are IV[0] $= A+3$, IV[1] $= 255$, and IV[2] $= X$, respectively. They regarded such IVs as weak IVs.

We introduce the FMS attack to derive $K[3]$ as the following example (refer to [FMS01, VV07] for details):

Example 3.2. *In order to derive $K[3]$, we collect a large number of encrypted packets with IV[0] $= 3$, IV[1] $= 255$, and IV[2] $= X$. When the above IV values are used, an internal state in the first four rounds of the KSA is transited as Figure 3.2. Assume that the values of $S_4^K[0]$, $S_4^K[1]$, and $S_4^K[3]$ are never swapped during the subsequent $N-4$ rounds of the KSA, whose probability is $\left(1-\frac{3}{N}\right)^{N-4} \approx 5.127(\%)$. When the above assumptions are used, an internal state in the first two rounds of the PRGA is also transited as Figure 3.3, and the third byte of the RC4 key $K[3]$ is given by*

$$\begin{aligned} S_3^K[X+6+K[3]] &= Z_1 \\ X+6+K[3] &= S_3^K[Z_1]^{-1} \\ K[3] &= S_3^K[Z_1]^{-1} - (X+6), \end{aligned} \tag{3.17}$$

where $S_r^K[x]^{-1}$ is the index of the value x in the internal state variable S_r^K. We can now easily recover the third byte of the RC4 key $K[3]$ from Equation (3.17) because the first byte of the keystream Z_1 can be recovered: $Z_1 = C_1 \oplus P_1 = C_1 \oplus$ `0xAA` where C_1 is the first byte of the ciphertext and $P_1 =$ `0xAA` is the first constant byte of the plaintext, which is the LLC header.

We can recover the remaining WEP key bytes $\{K[4], K[5], \ldots, K[15]\}$ in the same way as

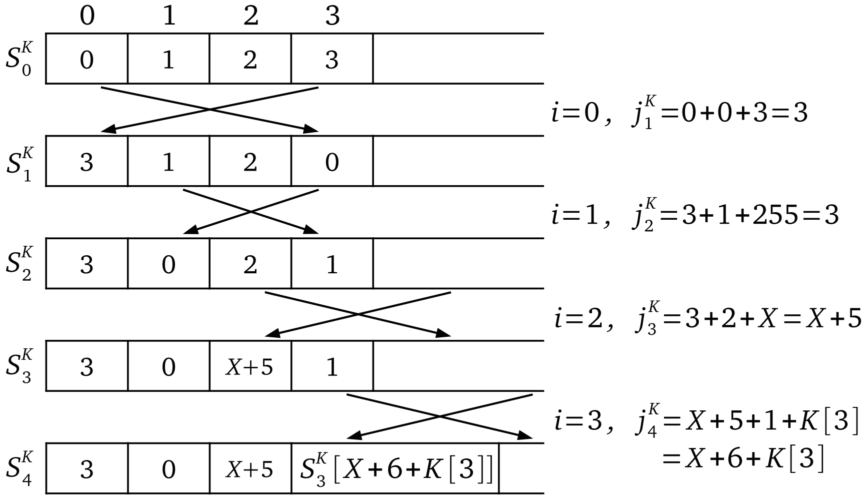

Figure 3.2: State transition diagram in the first four rounds of the KSA (Example 3.2).

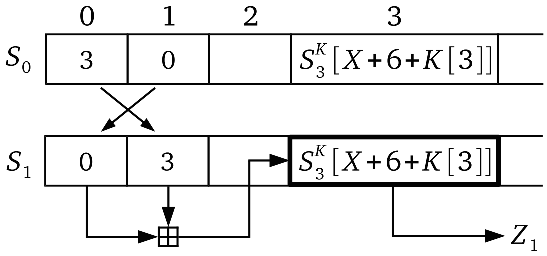

Figure 3.3: State transition diagram in the first two rounds of the PRGA (Example 3.2).

in Example 3.2. Now, we can generalize the FMS attack as the following function f_{FMS}:

$$\begin{aligned} K[x] = f_{FMS}(K[0], \dots, K[x-1], Z_1) &= S_x^K[Z_1]^{-1} - S_x^K[x] - j_x^K \\ &= S_x^K[Z_1]^{-1} - \sum_{j=1}^{x} S_j^K[j] - \sum_{i=0}^{x-1} K[i], \end{aligned} \tag{3.18}$$

which holds with the success probability

$$P_{FMS}(x) = \left(1 - \frac{3}{N}\right)^{N-x-1} \tag{3.19}$$

for recovering the RC4 key byte $K[x]$. As a result, Fluhrer et al. presented that all the WEP key bytes can be recovered with high probability of success by observing approximately 4,000,000–6,000,000 packets.

3.3.4 Key Recovery Attack on WEP without Using Weak IVs

In [Kle08], Klein improved the existing key recovery attack on WEP with the *Klein attack*, which does not need any weak IVs. Klein first presented a practical application of the Glimpse Theorem as the following theorem:

Theorem 3.23 ([Kle08, Theorem 1]). *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(Z_r + S_r[j_r] = c) \approx \begin{cases} \dfrac{2}{N} & \textit{when } c = i_r, \\ \dfrac{N-2}{N(N-1)} & \textit{when } c \neq i_r. \end{cases} \tag{3.20}$$

Klein also presented a strong correlation with the following five steps:

Step 1. $S_r[j_r] = i_r - Z_r$ with probability approximately $\frac{2}{N}$ from Theorem 3.23.

Step 2. $S_{r-1}[i_r] = S_r[j_r]$ with probability 1 from 5th step of Algorithm 2.

Step 3. $S_{r+1}^K[r] = S_{r-1}[i_r]$ with probability approximately $\left(1 - \frac{1}{N}\right)^{N-2}$. This means that the value of $S_{r+1}^K[r]$ in the KSA is never swapped during $N-2$ rounds up to $S_{r-1}[i_r]$ in the PRGA.

Step 4. $S_r^K[j_{r+1}^K] = S_{r+1}^K[r]$ with probability 1 from 7th step of Algorithm 1.

Step 5. $j_{r+1}^K = j_r^K + S_r^K[r] + K[r]$ with probability 1 from 6th step of Algorithm 1.

By summarizing the above steps, we can generalize the Klein attack as the following function f_{Klein}:

$$K[r] = f_{Klein}(K[0], \dots, K[r-1], Z_r) = S_r^K[i_r - Z_r]^{-1} - j_r^K - S_r^K[r], \tag{3.21}$$

which holds with the success probability

$$P_{Klein} \approx \left(1 - \frac{1}{N}\right)^{N-2} \cdot \frac{2}{N} + \left(1 - \left(1 - \frac{1}{N}\right)^{N-2}\right) \cdot \frac{N-2}{N(N-1)} \approx \frac{1.36}{N} \tag{3.22}$$

for recovering an arbitrary RC4 key byte $K[r]$.

Note that a significant limitation of the Klein attack is that we must know the value of the r-th round of the keystream to recover the RC4 key byte $K[r]$.

3.4 State Recovery Attacks

A state recovery attack recovers an internal state from a keystream under the scenario of the known plaintext attack, and aims to confirm the difficulty in recovering an internal state in the ciphers. This section describes the previous work on the state recovery attack reported in [KMP+98]. Although many other attacks have been reported, e.g., in [DMPS11, GS16, MP08b, SOM03], we will not describe these attacks in this section because these are out of our cryptanalysis and discussions in this dissertation.

In [KMP+98], Knudsen et al. presented a basic recursive algorithm to recover the internal state. At every round r, we have the following four unknown internal state variables:

$$S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1} \quad \text{for } r \geq 0. \tag{3.23}$$

One can simply simulate the PRGA, and guess these unknown values in order to continue the simulation if necessary. The recursion steps backward when a contradiction is reached owing to previous wrong guesses. In addition, assuming that certain values are a priori known (guessed, given, or derived somehow), we can significantly reduce the complexity of the attack.

We now present the details of their algorithm to recover the internal state as Algorithm 8. In this algorithm, let a_t denote the number of variables in the initial state, which were assigned a value at round r. As a result, their complete state recovery attack on RC4 requires a complexity of approximately 2^{779}.

Algorithm 8 State recovery attack in [KMP+98]

```
Step 1. It is checked whether $S_{r-1}[i_r]$ has been assigned a value:
if it has, then
    proceed to step 2.
else if it has not, then
    assign, one by one, the $2^n - a_r$ remaining values to $S_{r-1}[i_r]$, increment and go to step 2.
end if
Step 2. It is checked whether $Z_r$ has a value which has been used in an assignment:
if it has, then
    we can calculate the expected value of $S_r[j_r]$ from 6-th step of Algorithm 2.
    if this does not lead to a contradiction, then
        proceed to round $r + 1$ and go to step 1.
    end if
else if it has not, then
    go to step 3.
end if
Step 3. It is checked whether $S_{r-1}[j_r]$ has already been assigned a value:
if it has not, then
    assign, one by one, the $2^n - a_r$ remaining values to $S_{r-1}[j_r]$ and update $a_r$. Subsequently,
    it can be checked whether the given values of $i_r$, $j_r$, and $Z_r$ lead to a contradiction.
    if they do not, then
        proceed to time $r + 1$ and go to step 1.
    end if
end if
```

Chapter 4

Refined Glimpse Correlations

In [Jen96], Jenkins found correlations between a keystream byte Z_r and an internal state variable $S_r[i_r]$ or $S_r[j_r]$, which are known as the *Glimpse Theorem*. These correlations induce biases with probability approximately $\frac{2}{N}$ (see Theorem 3.16). The Glimpse Theorem was often used for key recovery attacks on WEP [Kle08, TAO$^+$10, TWP08]. In [MG13], Maitra and Sen Gupta presented a complete proof of the Glimpse Theorem, and extended the Glimpse Theorem to the following two types of correlations between two consecutive keystream bytes $\{Z_r, Z_{r+1}\}$ and an internal state variable $S_r[r+1]$, which are known as the *Long-term Glimpse*: The first is that $S_r[r+1] = N-1$ occurs with probability approximately $\frac{2}{N}$ when $Z_{r+1} = Z_r$ (see Theorem 3.17). The second is the occurrence of its special case where $Z_{r+1} = r+2$ as well as $Z_{r+1} = Z_r$, and the probability of $S_r[r+1] = N-1$ is increased to approximately $\frac{3}{N}$ (see Theorem 3.18). Theorems 3.16–3.18 are collectively referred to as the *Glimpse Correlations*.

The Glimpse Correlations provide only cases with positive biases. However, there may exist a *dual case* of a positive bias, where a dual case means a negative bias in these cases. One of our motivations in this chapter is to find dual cases of the Glimpse Correlations. Furthermore, Theorems 3.16–3.18 deal with correlations in each round all together. There may be room for improvement on correlations in a specific round. The other motivation is to provide correlations in specific rounds, such as $r = 1, 2$, and more precisely.

This chapter investigates the existing Glimpse Correlations in more detail from the following two approaches: One is to find *dual cases* of the existing Glimpse Correlations, and the other is to provide precise biases on specific rounds $r = 1, 2, \ldots, 256$. As a result, we find the existence of several events with new biases, and prove the events theoretically. Our contributions in this chapter can be summarized as the following six theorems and one corollary:

- Theorem 4.1 presents a dual case of Theorem 3.17 when $Z_{r+1} = Z_r$.
- Theorem 4.2 is a special case of Theorem 4.1 when $Z_{r+1} = r + x$ for $x \in [0, N-1]$ as well as $Z_{r+1} = Z_r$.
- Theorem 4.3 presents a new positive bias on the Long-term Glimpse when $Z_{r+1} = r+1+x$ for $x \in [0, N-1]$ as well as $Z_{r+1} = Z_r$.
- Corollary 4.1 integrates the Long-term Glimpse with positive biases when $Z_{r+1} = Z_r$.

- Theorem 4.4 presents that $\Pr(S_1[2] = 0)$ is approximately $\frac{2}{N}$ when $r = 1$ in Theorem 4.1.
- Theorem 4.5 presents an impossible condition of Theorem 4.1 when $r = 2$.
- Theorem 4.6 presents an impossible condition of Theorem 3.16 when $r = 2$.

The remainder of this chapter is organized as follows: Section 4.1 discusses new Glimpse Correlations observed in our experiments. Section 4.2 presents the theoretical proofs of newly observed Glimpse Correlations. Section 4.3 demonstrates the experimental simulations in order to confirm the accuracy of the theoretical proofs. Section 4.4 concludes this chapter.

4.1 Experimental Observations

This section presents our experimental observations of new Glimpse Correlations. In the first part of our observations, we focus on a relation between positive and negative biases. The existing Glimpse Correlations provide cases with a positive bias. These cases may implicitly mean that there exist cases with a negative bias explicitly. We refer to such a case with a negative bias as a *dual case* of the positive bias. In order to observe dual cases of the existing Glimpse Correlations, we have performed experiments using 2^{16} randomly chosen keys of 16 bytes and 2^{16} keystream bytes for each key. Figure 4.1 shows the experimental distribution of the value of $S_r[r+1]$ when $Z_{r+1} = Z_r$. The horizontal and vertical lines represent the value of $S_r[r+1]$ and the probability induced the value of $S_r[r+1]$ when $Z_{r+1} = Z_r$, respectively. From the figure, we observe that there exists the dual case of Theorem 3.17 when $S_r[r+1] = 0$, which is shown in Theorem 4.1. Figure 4.2 shows the experimental distribution of the value of $S_r[r+1]$ when $Z_{r+1} = r+2$ as well as $Z_{r+1} = Z_r$. The horizontal and vertical lines are similar to those in Figure 4.1. From the figure, we observe that there exists the dual case of Theorem 3.18 when $S_r[r+1] = 0$, which is shown in Theorem 4.2. Furthermore, Figure 4.3 shows that our careful observation successfully finds new positive biases on $S_r[r+1]$. The horizontal and vertical lines represent the value of x and the probability induced $S_r[r+1] = N - x$ when $Z_{r+1} = r+1+x$ as well as $Z_{r+1} = Z_r$, respectively. Figure 4.3 indicates new biases on $S_r[r+1] = N - x$ when $Z_{r+1} = r+1+x$ as well as $Z_{r+1} = Z_r$ for $x \in [2, N-1]$, which are shown in Theorem 4.3.

In the second part of our observations, we focus on the Glimpse Correlations in specific rounds. The existing Glimpse Correlations hold generally in any round. As a result, the previous estimation on correlations may be rather rough. Therefore, by further examining correlations in each round in more detail, we find new precise biases in specific rounds. In the experiments for finding new precise biases in the first 256 rounds, 2^{32} randomly chosen keys of 16 bytes are executed. As a result, we find new precise biases on $r = 1$ and $r = 2$, which are shown in Theorems 4.4 and 4.5. Theorem 4.4 presents a positive bias that $S_1[2] = 0$ occurs with the probability of approximately $\frac{2}{N}$ when $Z_2 = Z_1$. The condition of Theorem 4.4 is included in that of Theorem 4.1, whereas Theorem 4.1 presents a negative case. Theorem 4.5 also examines a case of $r = 2$ in Theorem 4.1, and presents that $S_2[3] = 0$ never occurs. Finally, Theorem 4.6 presents that an event in Theorem 3.16 never occurs when $Z_2 = 1, 2,$ or 129 holds.

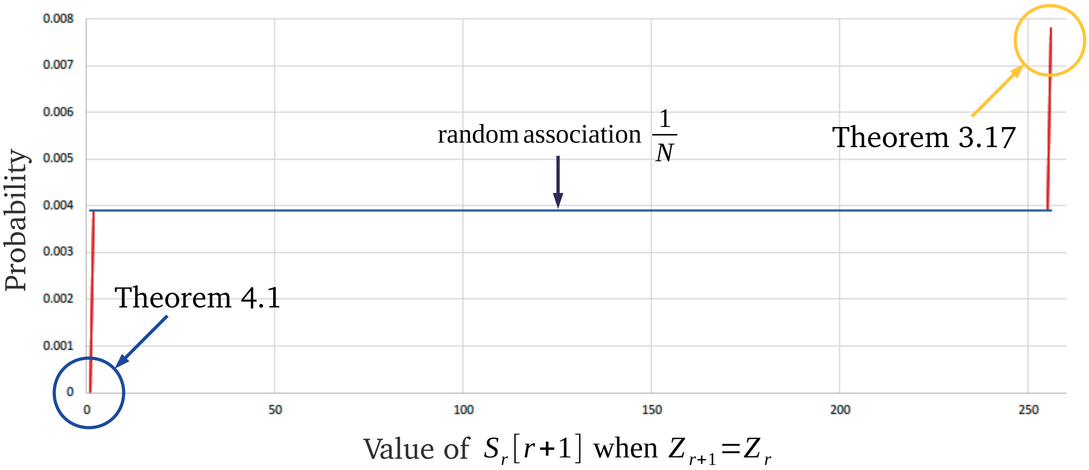

Figure 4.1: Bias in the value of $S_r[r + 1]$ when $Z_{r+1} = Z_r$.

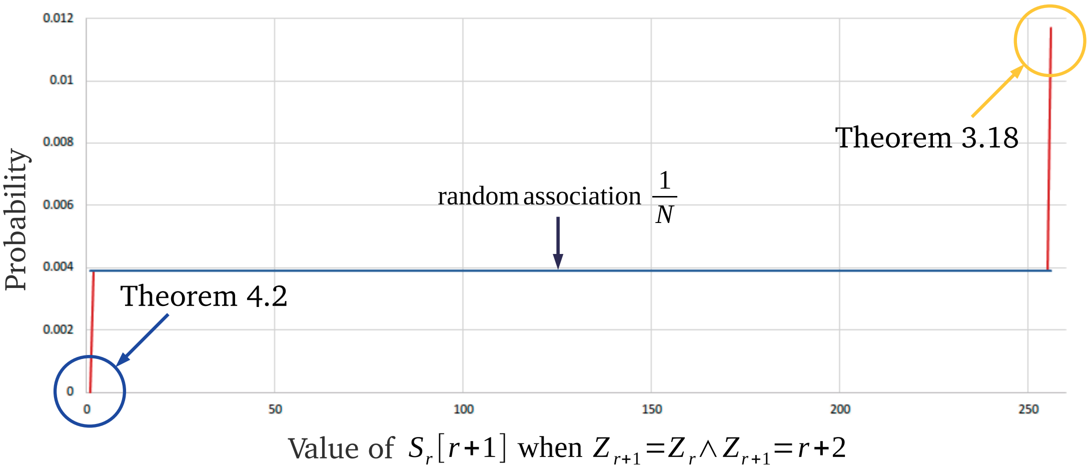

Figure 4.2: Bias in the value of $S_r[r + 1]$ when $Z_{r+1} = Z_r \wedge Z_{r+1} = r + 2$.

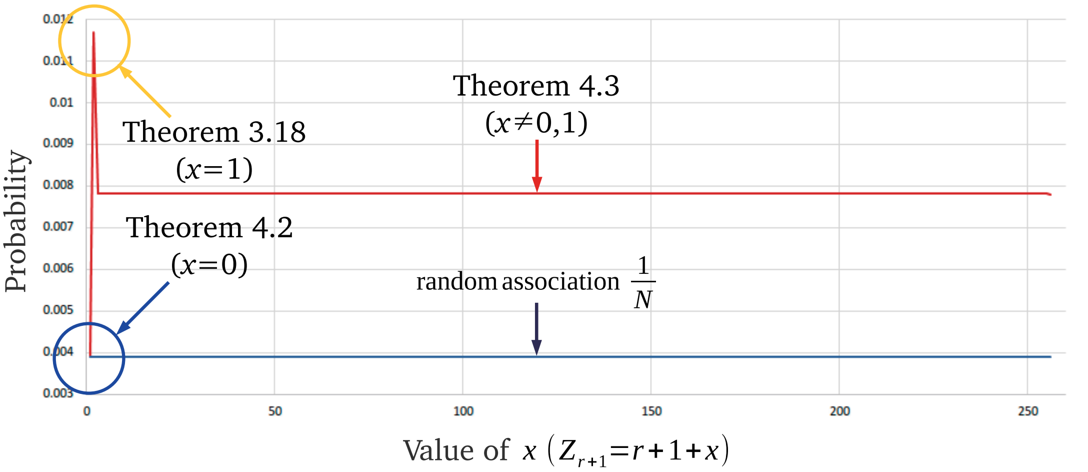

Figure 4.3: Bias in $S_r[r + 1] = N - x$ when $Z_{r+1} = Z_r \wedge Z_{r+1} = r + 1 + x$.

4.2 New Results

This section provides six theorems and their proofs. In our proofs, we often assume that the certain event occurs with probability approximately $\frac{1}{N}$, which is called the probability of *random association*. This is because it is difficult to demonstrate all events in the state transition of RC4, and it is a natural assumption based on the pseudorandomness of stream ciphers. The correctness of this assumption can be confirmed by experimental evaluations in Section 4.3. If this assumption is correct, the relative error between the experimental and theoretical value in each theorem will be small enough, and vice versa. Owing to this assumption, we often use the symbol of the approximate equation "≈" throughout this section.

4.2.1 Dual Cases of the Existing Long-term Glimpse

This subsection provides Theorems 4.1 and 4.2, which are dual cases of Theorems 3.17 and 3.18, and their proofs. Theorem 4.1 presents that an event $(S_r[r+1]=0)$ yields a negative bias when $Z_{r+1}=Z_r$. Theorem 4.2 is a special case of Theorem 4.1, and presents that an event $(S_r[r+1]=0)$ yields a negative bias when $Z_{r+1}=r+x$ $(x \in [0,N-1])$ as well as $Z_{r+1}=Z_r$. These are the revised versions of [IM16a, Theorems 2 and 3].

Theorem 4.1. *After the r-th round of the PRGA for $r \geq 1$, we have*

$$\Pr(S_r[r+1]=0 \mid Z_{r+1}=Z_r) \approx \begin{cases} \dfrac{2}{N^2} & \text{when } r = 0 \bmod N, \\ \dfrac{3}{N^2} - \dfrac{2}{N^3} & \text{when } r = 1 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{3}{N^3} & \text{when } r = N-3 \bmod N, \\ \dfrac{3}{N^2} + \dfrac{1}{N^3} & \text{when } r = N-2 \bmod N, \\ \dfrac{1}{N^2} + \dfrac{1}{N^3} & \text{when } r = N-1 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{2}{N^3} & \text{when } r \text{ is even and } r \neq 0, N-2 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{4}{N^3} & \text{when } r \text{ is odd and } r \neq 1, N-3, N-1 \bmod N. \end{cases}$$

Proof. We define the main events as follows:

$$A_r := (S_r[r+1]=0), \quad B_r := (Z_{r+1}=Z_r).$$

Note that

$$\Pr(A_r \mid B_r) = \frac{\Pr(A_r \wedge B_r)}{\Pr(B_r)} = \frac{\Pr(A_r)\Pr(B_r \mid A_r)}{\Pr(B_r)}.$$

Assuming that the events A_r and B_r occur with probability approximately $\frac{1}{N}$ (random association). We thus have $\Pr(A_r \mid B_r) \approx \Pr(B_r \mid A_r)$, and therefore

$$\begin{aligned}\Pr(A_r \mid B_r) &\approx \sum_{k=0}^{N-1} \Pr(B_r \wedge (j_r = k) \mid A_r) \\ &= \sum_{k=0}^{N-1} \Pr(j_r = k \mid A_r) \cdot \Pr(B_r \mid A_r \wedge (j_r = k)) \\ &\approx \frac{1}{N} \sum_{k=0}^{N-1} \Pr(B_r \mid A_r \wedge (j_r = k)),\end{aligned}$$

where assuming that an event $(j_r = k \mid A_r)$ occurs with probability approximately $\frac{1}{N}$ (random association).

Next, when the event A_r occurs, we have

$$j_{r+1} = j_r + S_r[i_{r+1}] = j_r + S_r[r+1] = j_r.$$

Then, we consider three paths: $j_r = r$ (Path 1), $j_r = r+1$ (Path 2), and $j_r = k \neq r, r+1$ (Path 3). Let $X = S_r[r] \neq 0$.

Path 1. Figure 4.4 shows a state transition diagram in Path 1. From the figure, the events A_r and $(j_r = r)$ imply

$$t_r = 2X, \quad t_{r+1} = X, \quad Z_r = S_r[2X], \quad Z_{r+1} = S_{r+1}[X].$$

Note that $X \neq 0 \Rightarrow 2X \neq X$, and then we have

$$\begin{aligned}\{B_r \mid A_r \wedge (j_r = r)\} &= \{S_r[2X] = S_{r+1}[X] \mid A_r \wedge (j_r = r)\} \\ &\Leftrightarrow \{(2X, X) = (r, r+1)\} \vee \{(2X, X) = (r+1, r)\}.\end{aligned}$$

When $(2X, X) = (r, r+1)$, we have $r = 2X = X + X = X + r + 1$, so that $X = N-1$ and $r = N-2$. Note here that an event $(X = N-1)$ occurs with probability $\frac{1}{N-1}$ only when $r = N-2$.

On the other hand, when $(2X, X) = (r+1, r)$, we have $r + 1 = 2X = X + X = X + r$, so that $X = 1$ and $r = 1$. Note here that an event $(X = 1)$ occurs with probability $\frac{1}{N-1}$ only when $r = 1$.

Therefore, we obtain

$$\begin{aligned}&\Pr(B_r \mid A_r \wedge (j_r = r)) \\ &\quad = \begin{cases} \Pr(X = 1 \mid A_r \wedge (j_r = r)) = \dfrac{1}{N-1} & \text{when } r = 1 \bmod N, \\ \Pr(X = N-1 \mid A_r \wedge (j_r = r)) = \dfrac{1}{N-1} & \text{when } r = N-2 \bmod N, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Path 2. Figure 4.5 shows a state transition diagram in Path 2. From the figure, the events A_r and $(j_r = r+1)$ imply

$$t_r = X, \quad t_{r+1} = 0, \quad Z_r = S_r[X], \quad Z_{r+1} = S_{r+1}[0].$$

In this case, $S_r[x] = S_{r+1}[x]$ for all $x = 0, 1, \ldots, N-1$, and then the event B_r implies $X = 0$, which contradicts $X \neq 0$. Therefore, we obtain

$$\Pr(B_r \mid A_r \wedge (j_r = r+1)) = 0.$$

Path 3. Figure 4.6 shows a state transition diagram in Path 3. Let $Y = S_r[j_r] \neq 0$ and $X \neq Y$. From the figure, the events A_r and $(j_r = k \neq r, r+1)$ imply

$$t_r = X+Y, \quad t_{r+1} = Y, \quad Z_r = S_r[X+Y], \quad Z_{r+1} = S_{r+1}[Y].$$

Note that $X \neq 0 \Rightarrow X+Y \neq Y$, and then we have

$$\begin{aligned}\{B_r \mid A_r \wedge (j_r = k)\} &= \{S_r[X+Y] = S_{r+1}[Y] \mid A_r \wedge (j_r = k)\}\\ &\Leftrightarrow \{(X,Y) = (r+1-k, k)\} \vee \{(X,Y) = (k-r-1, r+1)\},\end{aligned}$$

and vice versa if $X \neq 0$, $Y \neq 0$, and $X \neq Y$. Note that $(r+1-k, k) = (k-r-1, r+1)$ if and only if $k = r+1$, and thus we have $(r+1-k, k) \neq (k-r-1, r+1)$ if $k \neq r+1$. When $(X,Y) = (r+1-k, k)$, where $k \neq r, r+1$, we have $r+1-k \neq 0$, $k \neq 0$, and $r+1-k \neq k$, which are equivalent to $k \neq r+1$, $k \neq 0$, and $2k \neq r+1$. Note here that $2k \neq r+1$ holds if r is even, and then we have

$$\begin{cases} k \neq r, r+1 & \text{when } r = 0 \bmod N,\\ k \neq 0, r, r+1 & \text{when } r \text{ is even and } r \neq 0 \bmod N.\end{cases}$$

On the other hand, $2k \neq r+1$ implies $k \neq \frac{r+1}{2}, \frac{N+r+1}{2}$ if r is odd, so that $k \neq 0, r, r+1, \frac{r+1}{2}, \frac{N+r+1}{2}$ if r is odd. Note here that this constraint can be redundant as follows:

$$\begin{aligned}\{k = \frac{r+1}{2} = r\} &\Leftrightarrow \{(k=1) \wedge (r=1)\},\\ \{k = \frac{r+1}{2} = r+1\} &\Leftrightarrow \{(k = 0 = r+1) \wedge (r = N-1)\},\\ \{k = \frac{N+r+1}{2} = r\} &\Leftrightarrow \{(k = \frac{N+2}{2}) \wedge (r=1)\},\\ \{k = \frac{N+r+1}{2} = r+1\} &\Leftrightarrow \{(k = 0 = r+1) \wedge (r = N-1)\},\end{aligned}$$

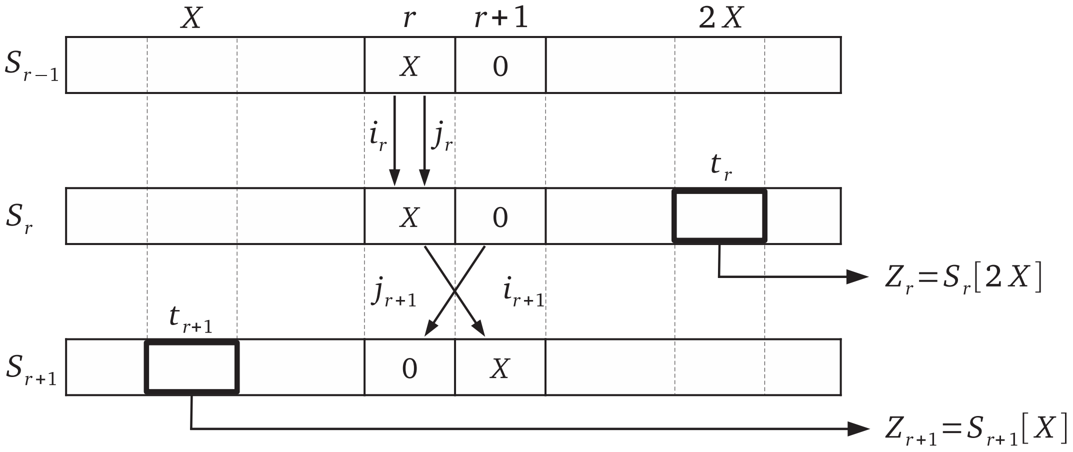

Figure 4.4: State transition diagram in Path 1 (Theorems 4.1 and 4.2).

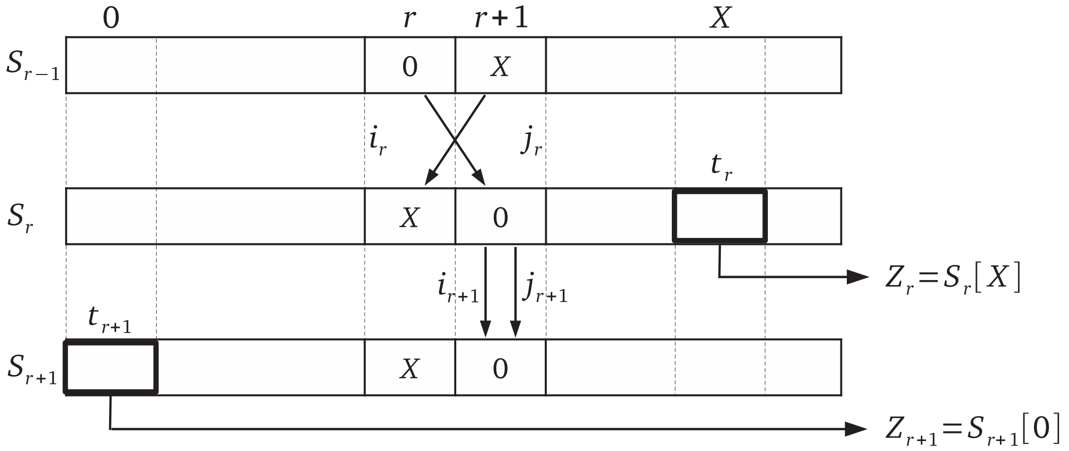

Figure 4.5: State transition diagram in Path 2 (Theorems 4.1 and 4.2).

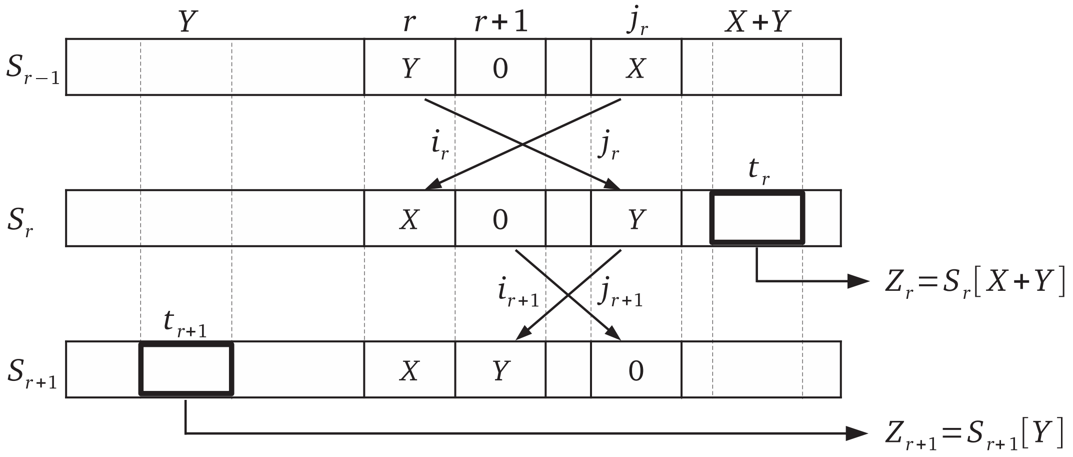

Figure 4.6: State transition diagram in Path 3 (Theorems 4.1 and 4.2).

and thus we have $(X, Y) = (r + 1 - k, k)$, where

$$\begin{cases} k \neq 0, r, r+1, \dfrac{N+2}{2} & \text{when } r = 1 \bmod N, \\ k \neq r, r+1 & \text{when } r = N-1 \bmod N, \\ k \neq 0, r, r+1, \dfrac{r+1}{2}, \dfrac{N+r+1}{2} & \text{when } r \text{ is odd and } r \neq 1, N-1 \bmod N. \end{cases}$$

Next, we consider $(X, Y) = (k - r - 1, r + 1)$, where $k \neq r, r+1$. Then, we have $k \neq r - 1$, $r \neq N - 1$, and $k \neq 2(r + 1)$, which imply $k \neq r - 1, r, r + 1, N - 1, 2(r + 1)$. Note here that $N - 1 \neq 2(r + 1)$ and this constraint can be redundant as follows:

$$\begin{aligned} \{k = r - 1 = N - 1\} &\Leftrightarrow \{r = 0\}, \\ \{k = r - 1 = 2(r + 1)\} &\Leftrightarrow \{(k = N - 4) \wedge (r = N - 3)\}, \\ \{k = r = 2(r + 1)\} &\Leftrightarrow \{(k = N - 2) \wedge (r = N - 2)\}, \\ \{k = r + 1 = N - 1\} &\Leftrightarrow \{r = N - 2\}, \\ \{k = r + 1 = 2(r + 1)\} &\Leftrightarrow \{(k = 0) \wedge (r = N - 1)\}, \end{aligned}$$

and thus we have $(X, Y) = (k - r - 1, r + 1)$, where

$$\begin{cases} k \neq r-1, r, r+1, 2(r+1) & \text{when } r = 0 \bmod N, \\ k \neq r-1, r, r+1, N-1 & \text{when } r = N-3 \bmod N, \\ k \neq r-1, r, r+1 & \text{when } r = N-2 \bmod N, \\ k \neq r-1, r, r+1, 2(r+1), N-1 & \text{when } r \neq 0, N-3, N-2, N-1 \bmod N, \end{cases}$$

and $(X, Y) = (k - r - 1, r + 1)$ is not feasible when $r = N - 1 \bmod N$.

In summary, the event B_r occurs under the events A_r and $(j_r = k \neq r, r + 1)$ if and only if we have the following seven cases:

(i) When $r = 0 \bmod N$:

$$\begin{cases} (X, Y) = (r + 1 - k, k), & \text{where } k \neq 0, 1, \\ (X, Y) = (k - r - 1, r + 1), & \text{where } k \neq 0, 1, 2, N - 1. \end{cases}$$

(ii) When $r = 1 \bmod N$:

$$\begin{cases} (X, Y) = (r + 1 - k, k), & \text{where } k \neq 0, 1, 2, \frac{N-2}{2}, \\ (X, Y) = (k - r - 1, r + 1), & \text{where } k \neq 0, 1, 2, 4, N - 1. \end{cases}$$

(iii) When $r = N - 3 \bmod N$:

$$\begin{cases} (X,Y) = (r+1-k, k), & \text{where } k \neq 0, N-3, N-2, \frac{N-2}{2}, N-1, \\ (X,Y) = (k-r-1, r+1), & \text{where } k \neq N-4, N-3, N-2, N-1. \end{cases}$$

(iv) When $r = N - 2 \bmod N$:

$$\begin{cases} (X,Y) = (r+1-k, k), & \text{where } k \neq 0, N-2, N-1, \\ (X,Y) = (k-r-1, r+1), & \text{where } k \neq N-3, N-2, N-1. \end{cases}$$

(v) When $r = N - 1 \bmod N$:

$$(X,Y) = (r+1-k, k), \text{ where } k \neq 0, N-1.$$

(vi) When r is even and $r \neq 0, N-2 \bmod N$:

$$\begin{cases} (X,Y) = (r+1-k, k), & \text{where } k \neq 0, r, r+1, \\ (X,Y) = (k-r-1, r+1), & \text{where } k \neq r-1, r, r+1, 2(r+1), N-1. \end{cases}$$

(vii) When r is odd and $r \neq 1, N-3, N-1 \bmod N$:

$$\begin{cases} (X,Y) = (r+1-k, k), & \text{where } k \neq 0, r, r+1, \frac{r+1}{2}, \frac{N+r+1}{2}, \\ (X,Y) = (k-r-1, r+1), & \text{where } k \neq r-1, r, r+1, 2(r+1), N-1. \end{cases}$$

As a result, we obtain

$$\sum_{\substack{k=0 \\ (k \neq r, r+1)}}^{N-1} \Pr(B_r \mid A_r \wedge (j_r = k))$$
$$= \begin{cases} \dfrac{2N-6}{(N-1)(N-2)} & \text{when } r = 0, N-2 \bmod N, \\ \dfrac{2N-9}{(N-1)(N-2)} & \text{when } r = 1, N-3 \bmod N, \\ \dfrac{1}{N-1} & \text{when } r = N-1 \bmod N, \\ \dfrac{2N-8}{(N-1)(N-2)} & \text{when } r \text{ is even and } r \neq 0, N-2 \bmod N, \\ \dfrac{2N-10}{(N-1)(N-2)} & \text{when } r \text{ is odd and } r \neq 1, N-3, N-1 \bmod N, \end{cases}$$

because $\Pr((X,Y) = (x,y) \mid A_r \wedge (j_r = k)) = \frac{1}{(N-1)(N-2)}$, for $x, y = 1, 2, \ldots, N-1$, and $x \neq y$.

In summary,

$$
\begin{aligned}
&\Pr(A_r \mid B_r)\\
&\quad= \frac{1}{N}\sum_{k=0}^{N-1} \Pr(B_r \mid A_r \wedge (j_r = k))\\
&\quad= \frac{1}{N}\Bigg[\Pr(B_r \mid A_r \wedge (j_r = r)) + \Pr(B_r \mid A_r \wedge (j_r = r+1)) + \sum_{\substack{k=0\\(k\neq r, r+1)}}^{N-1} \Pr(B_r \mid A_r \wedge (j_r = k))\Bigg]\\
&\quad= \begin{cases}
\dfrac{2N-6}{N(N-1)(N-2)} & \text{when } r = 0 \bmod N,\\
\dfrac{1}{N(N-1)} + \dfrac{2N-9}{N(N-1)(N-2)} & \text{when } r = 1 \bmod N,\\
\dfrac{2N-9}{N(N-1)(N-2)} & \text{when } r = N-3 \bmod N,\\
\dfrac{1}{N(N-1)} + \dfrac{2N-6}{N(N-1)(N-2)} & \text{when } r = N-2 \bmod N,\\
\dfrac{1}{N(N-1)} & \text{when } r = N-1 \bmod N,\\
\dfrac{2N-8}{N(N-1)(N-2)} & \text{when } r \text{ is even and } r \neq 0, N-2 \bmod N,\\
\dfrac{2N-10}{N(N-1)(N-2)} & \text{when } r \text{ is odd and } r \neq 1, N-3, N-1 \bmod N.
\end{cases}
\end{aligned}
$$

Note that

$$\frac{1}{N-1} = \frac{1}{N} + \frac{1}{N(N-1)}, \quad \frac{1}{N-2} = \frac{1}{N} + \frac{2}{N(N-2)}.$$

It then follows that

$$\frac{1}{N(N-1)} = \frac{1}{N^2} + \frac{1}{N^2(N-1)} = \frac{1}{N^2} + \frac{1}{N^3} + \frac{1}{N^3(N-1)} = \frac{1}{N^2} + \frac{1}{N^3} + o(\frac{1}{N^3}),$$

$$
\begin{aligned}
\frac{1}{N(N-1)(N-2)} &= \frac{1}{N^2(N-1)} + \frac{2}{N^2(N-1)(N-2)}\\
&= \frac{1}{N^3} + \frac{1}{N^3(N-1)} + \frac{2}{N^2(N-1)(N-2)} = \frac{1}{N^3} + o(\frac{1}{N^3}).
\end{aligned}
$$

In summary, we obtain

$$\Pr(A_r \mid B_r) \approx \begin{cases} \dfrac{2}{N^2} & \text{when } r = 0 \bmod N, \\ \dfrac{3}{N^2} - \dfrac{2}{N^3} & \text{when } r = 1 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{3}{N^3} & \text{when } r = N-3 \bmod N, \\ \dfrac{3}{N^2} + \dfrac{1}{N^3} & \text{when } r = N-2 \bmod N, \\ \dfrac{1}{N^2} + \dfrac{1}{N^3} & \text{when } r = N-1 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{2}{N^3} & \text{when } r \text{ is even and } r \neq 0, N-2 \bmod N, \\ \dfrac{2}{N^2} - \dfrac{4}{N^3} & \text{when } r \text{ is odd and } r \neq 1, N-3, N-1 \bmod N. \end{cases}$$

□

Remark 4.1. *The previous result of Theorem 4.1 was given as*

$$\Pr(S_r[r+1] = 0 \mid Z_{r+1} = Z_r) \approx \frac{2}{N^2}\left(1 - \frac{1}{N}\right).$$

For the purpose of comparison between the previous and revised result, the averaged result of Theorem 4.1 is given as

$$\frac{1}{N}\sum_{r=0 \bmod N}^{N-1} \Pr(S_r[r+1] = 0 \mid Z_{r+1} = Z_r) = \frac{2}{N^2} - \frac{1}{N^3} + o(\frac{1}{N^3}) \approx \frac{2}{N^2} - \frac{1}{N^3}.$$

After the revision, we improve the percentage of the relative error between the experimental and theoretical value from 0.379 % to 0.182 % (see Section 4.3). This is the result of strict analysis of the occurrence probability of the target event in each round. However, even if we apply the target events with either the previous or revised theoretical value to the existing attacks, no difference will be made in the efficiency of the attacks because either relative error is small enough.

Theorem 4.2 ([IM16a, Theorem 3])**.** *After the r-th round of the PRGA for $r \geq 1$ and $\forall x \in [0, N-1]$, we have*

$$\Pr(S_r[r+1] = 0 \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r + x)),$$

which is given as

$$\frac{1}{N}\sum_{r=0 \bmod N}^{N-1} \Pr(S_r[r+1]=0 \mid (Z_{r+1}=Z_r)\wedge(Z_{r+1}=r+x)) \approx \begin{cases} \dfrac{1}{N}+\dfrac{1}{N^3} & \textit{when } x=1,\\ \dfrac{2}{N^2} & \textit{when } x=N-1,\\ \dfrac{1}{N^2} & \textit{otherwise.} \end{cases}$$

Proof. We define the main events as follows:

$$A_r := (S_r[r+1]=0), \quad B_r := (Z_{r+1}=Z_r), \quad C_r := (Z_{r+1}=r+x).$$

$\Pr(A_r \mid B_r \wedge C_r)$ is difficult to compute because the events B_r and C_r are not independent. To avoid this problem, we further define a new event $B'_r := (Z_r = r+x)$. Then, $\Pr(A_r \mid B_r \wedge C_r) = \Pr(A_r \mid B'_r \wedge C_r)$ because the events $(B_r \wedge C_r)$ and $(B'_r \wedge C_r)$ are the same, and therefore we will compute the target probability easily. Note here that

$$\Pr(A_r \mid B'_r \wedge C_r) = \frac{\Pr(A_r \wedge B'_r \wedge C_r)}{\Pr(B'_r \wedge C_r)} = \frac{\Pr(C_r \mid B'_r \wedge A_r)\cdot \Pr(B'_r \mid A_r)\cdot \Pr(A_r)}{\Pr(B'_r \wedge C_r)}.$$

Assuming that the events A_r, B'_r, and C_r are mutually independent, and occur with probability approximately $\frac{1}{N}$ (random association), respectively. We thus have $\Pr(A_r \mid B'_r \wedge C_r) \approx \Pr(C_r \mid B'_r \wedge A_r)$, and therefore

$$\begin{aligned} \Pr(C_r \mid B'_r \wedge A_r) &= \sum_{k=0}^{N-1} \Pr(C_r \wedge (j_r = k) \mid B'_r \wedge A_r) \\ &= \sum_{k=0}^{N-1} \Pr(j_r = k \mid B'_r \wedge A_r)\cdot \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)) \\ &\approx \frac{1}{N}\sum_{k=0}^{N-1} \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)), \end{aligned}$$

where assuming that an event $(j_r = k \mid B'_r \wedge A_r)$ occurs with probability approximately $\frac{1}{N}$ (random association).

Next, when the event A_r occurs, we have

$$j_{r+1} = j_r + S_r[i_{r+1}] = j_r + S_r[r+1] = j_r.$$

Then, we consider three paths: $j_r = r$ (Path 1), $j_r = r+1$ (Path 2), and $j_r = k \neq r, r+1$ (Path 3). These paths are the same as in the proof of Theorem 4.1, and the proof itself is similar to that of Theorem 4.1. Let $X = S_r[r] \neq 0$.

Path 1. Figure 4.4 shows a state transition diagram in Path 1. From the figure, the events A_r,

B'_r, and $(j_r = r)$ imply

$$t_r = 2X, \quad t_{r+1} = X, \quad Z_r = S_r[2X] = r + x, \quad Z_{r+1} = S_{r+1}[X].$$

Note that $X \neq 0 \Rightarrow 2X \neq X$, and then we have

$$\begin{aligned}\{C_r \mid B'_r \wedge A_r \wedge (j_r = r)\} &= \{S_{r+1}[X] = r + x \mid B'_r \wedge A_r \wedge (j_r = r)\} \\ &\Leftrightarrow \{(2X, X) = (r, r+1)\} \vee \{(2X, X) = (r+1, r)\}.\end{aligned}$$

When $(2X, X) = (r, r+1)$, we have $r = 2X = X + X = X + r + 1$, so that $X = N - 1$ and $r = N - 2$. Note here that the event B'_r implies the event $(S_{r+1}[X] = N - 1)$ occurs with probability $\frac{1}{N-1}$ when $r = N - 2$ and $x = 1$.

On the other hand, when $(2X, X) = (r+1, r)$, we have $r + 1 = 2X = X + X = X + r$, so that $X = 1$ and $r = 1$. Note here that the event B'_r implies the event $(S_{r+1}[X] = 0)$ occurs with probability 1 when $r = 1$ and $x = N - 1$.

Therefore, we obtain

$$\begin{aligned}&\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r)) \\ &= \begin{cases} \Pr(S_{r+1}[X] = 0 \mid B'_r \wedge A_r \wedge (j_r = r)) = 1 & \text{when } r = 1 \bmod N \text{ and } x = N - 1, \\ \Pr(S_{r+1}[X] = N - 1 \mid B'_r \wedge A_r \wedge (j_r = r)) = \dfrac{1}{N-1} & \text{when } r = N - 2 \bmod N \text{ and } x = 1, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

Path 2. The event C_r never occurs in Path 2 as we discussed in the proof of Theorem 4.1. Therefore, we obtain

$$\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r + 1)) = 0.$$

Path 3. Figure 4.6 shows a state transition diagram in Path 3. Let $Y = S_r[j_r] \neq 0$ and $X \neq Y$. From the figure, the events A_r, B'_r, and $(j_r = k \neq r, r+1)$ imply

$$t_r = X + Y, \quad t_{r+1} = Y, \quad Z_r = S_r[X + Y] = r + x, \quad Z_{r+1} = S_{r+1}[Y].$$

Note that $X \neq 0 \Rightarrow X + Y \neq Y$, and then we have

$$\begin{aligned}\{C_r \mid B'_r \wedge A_r \wedge (j_r = k)\} &= \{S_{r+1}[Y] = r + x \mid B'_r \wedge A_r \wedge (j_r = k)\} \\ &\Leftrightarrow \{(X + Y, Y) = (r + 1, k)\} \vee \{(X + Y, Y) = (k, r + 1)\},\end{aligned}$$

and vice versa if $X \neq 0$, $Y \neq 0$, and $X \neq Y$.

When $(X + Y, Y) = (r + 1, k)$, we have $S_r[X + Y] = S_r[r + 1] = r + x = 0$ under the occurrence of the events A_r and B'_r. Note here that an event $(Y = k)$ occurs with probability $\frac{1}{N-2}$ when $r = N - x$ for all x.

On the other hand, when $(X+Y, Y) = (k, r+1)$, we have $S_r[X+Y] = S_r[k] = r+x = Y$ under the occurrence of the events A_r and B'_r. Note here that an event $(Y = r+1)$ occurs with probability $\frac{1}{N-2}$ when $x = 1$ for all r.

Therefore, we obtain

$$\begin{aligned}
&\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)) \\
&= \begin{cases} \Pr(S_{r+1}[Y] = 0 \mid B'_r \wedge A_r \wedge (j_r = k)) = \dfrac{1}{N-2} & \text{when } r = N - x \bmod N \text{ for all } x, \\ \Pr(S_{r+1}[Y] = r+1 \mid B'_r \wedge A_r \wedge (j_r = k)) = \dfrac{1}{N-2} & \text{when } x = 1 \text{ for all } r, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

In summary, we obtain

$$\begin{aligned}
\Pr(A_r \mid B_r \wedge C_r) &\approx \frac{1}{N} \sum_{k=0}^{N-1} \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)) \\
&= \frac{1}{N}\Bigg[\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r)) + \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r+1)) \\
&\quad + \sum_{\substack{k=0 \\ (k \neq r, r+1)}}^{N-1} \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k))\Bigg],
\end{aligned}$$

which is given as

$$\begin{aligned}
&\frac{1}{N} \sum_{r=0 \bmod N}^{N-1} \Pr(S_r[r+1] = 0 \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r+x)) \\
&\approx \begin{cases} \dfrac{1}{N} + \dfrac{1}{N^2(N-1)} \approx \dfrac{1}{N} + \dfrac{1}{N^3} & \text{when } x = 1, \\ \dfrac{2}{N^2} & \text{when } x = N-1, \\ \dfrac{1}{N^2} & \text{otherwise.} \end{cases}
\end{aligned}$$

□

Remark 4.2. *The previous result of Theorem 4.2 is as follows:*

$$\Pr(S_r[r+1] = 0 \mid Z_{r+1} = Z_r \wedge Z_{r+1} = r+x) \approx \begin{cases} \dfrac{1}{N}\left(1 - \dfrac{2}{N^2}\right) & \textit{when } x = 1, \\ \dfrac{2}{N^2}\left(1 - \dfrac{1}{N}\right) & \textit{when } x = N-1, \\ \dfrac{1}{N^2}\left(1 - \dfrac{2}{N}\right) & \textit{otherwise.} \end{cases}$$

After the revision, we improve the percentage of the relative error between the experimental and *theoretical value from 0.415 % to 0.410 % when $x = 1$, from 0.931 % to 0.541 % when $x = N-1$, and from 0.783 % to 0.004 % otherwise (see Section 4.3). This is the result of revision in the same way as the proof of Theorem 4.1. However, even if we apply the target events with either the previous or revised theoretical value to the existing attacks, no difference will be made in the efficiency of the attacks because either relative error is small enough.*

4.2.2 New Positive Bias and Integrated Long-term Glimpse

This subsection provides Theorem 4.3, which presents a new positive bias on $S_r[r+1]$, and its proof. This is the revised version of [IM16a, Theorem 4]. Then, we integrate our new results and the existing Long-term Glimpse as Corollary 4.1 by combining the results of Theorems 3.18, 4.2, and 4.3.

Theorem 4.3 ([IM16a, Theorem 4])**.** *After the r-th round of the PRGA for $r \geq 1$ and $\forall x \in [2, N-1]$, we have*

$$\Pr(S_r[r+1] = N - x \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r + 1 + x)),$$

which is given as

$$\frac{1}{N} \sum_{r=0 \bmod N}^{N-1} \Pr(S_r[r+1] = N - x \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r + 1 + x)) \approx \frac{2}{N}\left(1 - \frac{1}{N} + \frac{2}{N^2}\right).$$

Proof. We define the main events as follows.

$$\begin{aligned} A_r &:= (S_r[r+1] = N - x), \quad B_r := (Z_{r+1} = Z_r), \\ B'_r &:= (Z_r = r + 1 + x), \quad C_r := (Z_{r+1} = r + 1 + x). \end{aligned}$$

The proof itself is similar to that of Theorem 4.2. We thus have

$$\Pr(A_r \mid B_r \wedge C_r) \approx \frac{1}{N} \sum_{k=0}^{N-1} \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)).$$

Then, we consider three paths: $j_r = r$ (Path 1), $j_r = r + 1$ (Path 2), and $j_r \neq r, r+1$ (Path 3). Let $X = S_r[r]$, $W = S_r[j_{r+1}]$, and $X \neq W$.

Path 1. Figure 4.7 shows a state transition diagram in Path 1. From the figure, the events A_r, B'_r, and $(j_r = r)$ imply

$$t_r = 2X, \quad t_{r+1} = N - x - W, \quad Z_r = S_r[2X] = r + 1 + x, \quad Z_{r+1} = S_{r+1}[N - x + W].$$

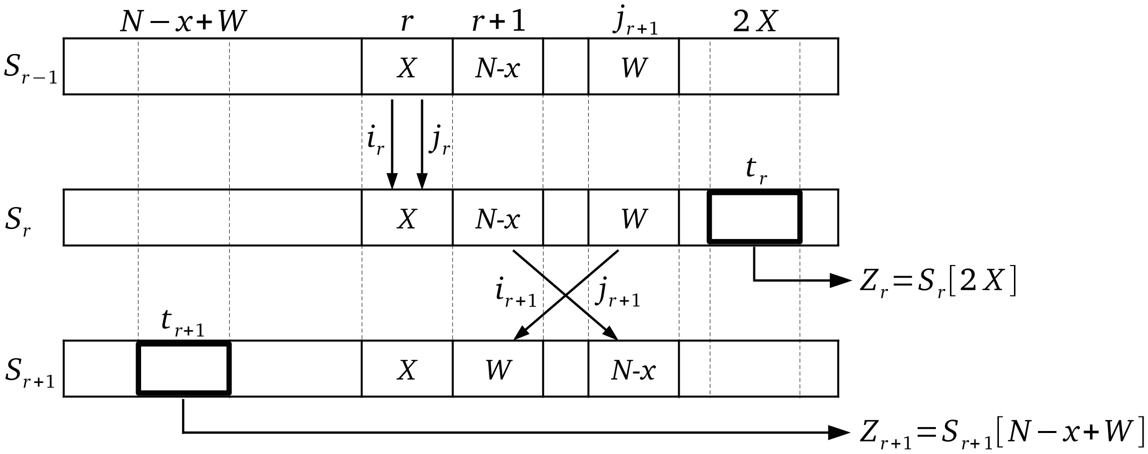

Figure 4.7: State transition diagram in Path 1 (Theorem 4.3).

Note that t_r and t_{r+1} are independent, and then we have

$$\begin{aligned}\{C_r \mid B'_r \wedge A_r \wedge (j_r = r) &= \{S_{r+1}[N - x + W] = r + 1 + x \mid B'_r \wedge A_r \wedge (j_r = r)\}\\ &\Leftrightarrow \{(t_r, t_{r+1}) = (r + 1, j_{r+1})\} \vee \{(t_r, t_{r+1}) = (j_{r+1}, t + 1)\} \vee \{t_r = t_{r+1}\}.\end{aligned}$$

(i) When $(t_r, t_{r+1}) = (r+1, j_{r+1})$, we have $S_r[t_r] = S_r[r+1] = r+1+x = N-x$ under the occurrence of the events A_r and B'_r, so that $S_{r+1}[t_{r+1}] = S_r[t_r] = r + 1 + x = N - x$. Note here that events $(t_r = r + 1) \wedge (t_{r+1} = j_{r+1})$ occur with probability $\frac{1}{(N-1)(N-2)}$ when $r = N - 2x - 1$ for all $x \in [2, N - 1]$.

(ii) When $(t_r, t_{r+1}) = (j_{r+1}, r + 1)$, we have $S_r[t_r] = S_r[j_{r+1}] = r + 1 + x = W$ under the occurrence of the events A_r and B'_r, so that $S_{r+1}[t_{r+1}] = S_r[t_r] = r + 1 + x = W$. Note here that events $(t_r = j_{r+1}) \wedge (t_{r+1} = r + 1)$ occur with probability $\frac{1}{N-2}$ for all r and $x \in [2, N - 1]$.

(iii) When $t_r = t_{r+1}$, we have $S_r[t_r] = S_{r+1}[t_{r+1}] = r + 1 + x$ except when $t_r = r + 1$ or j_{r+1}. Note here that an event $(t_r = t_{r+1})$ occurs with probability $\frac{1}{N}\left(1 - \frac{2}{N}\right)$ for all r and $x \in [2, N - 1]$.

Therefore, we obtain

$$\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r)) = \begin{cases} \dfrac{2}{N} - \dfrac{1}{N^2} + \dfrac{3}{N^3} + o(\dfrac{1}{N^3}) & \text{when } r = N - 2x - 1, \\ \dfrac{2}{N} - \dfrac{1}{N^2} + \dfrac{2}{N^3} + o(\dfrac{1}{N^3}) & \text{otherwise.} \end{cases}$$

Path 2. Figure 4.8 shows a state transition diagram in Path 2. From the figure, the events A_r, B'_r, and $(j_r = r + 1)$ imply

$$t_r = N{-}x{+}X, \quad t_{r+1} = N{-}x{-}W, \quad Z_r = S_r[N{-}x{+}X] = r{+}1{+}x, \quad Z_{r+1} = S_{r+1}[N{-}x{+}W].$$

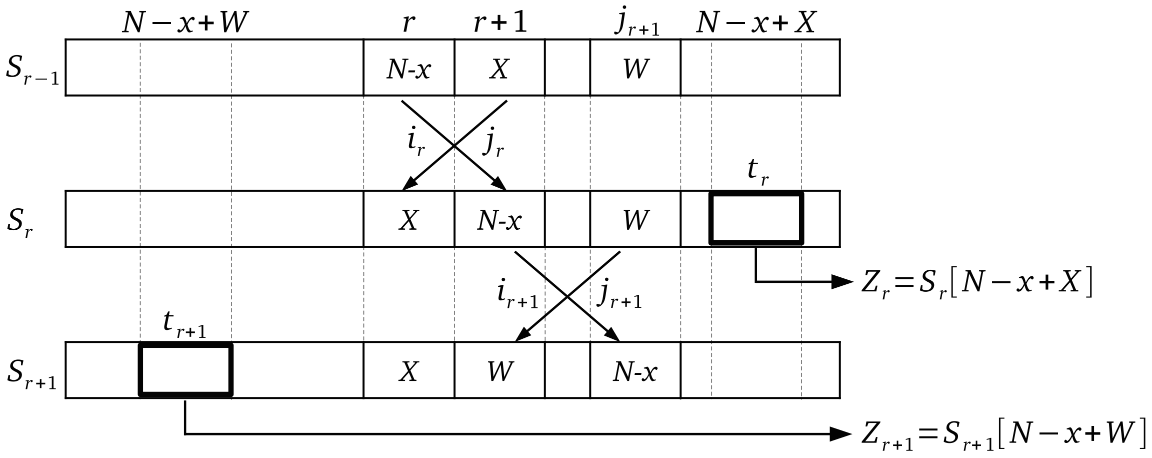

Figure 4.8: State transition diagram in Path 2 (Theorem 4.3).

Note that $X \neq W \Rightarrow N - x + X \neq N - x + W$, and then we have

$$\begin{aligned}\{C_r \mid B'_r \wedge A_r \wedge (j_r = r+1) &= \{S_{r+1}[N - x + W] = r + 1 + x \mid B'_r \wedge A_r \wedge (j_r = r)\} \\ &\Leftrightarrow \{(t_r, t_{r+1}) = (r+1, j_{r+1})\} \vee \{(t_r, t_{r+1}) = (j_{r+1}, t+1)\}.\end{aligned}$$

From the discussion of (i) and (ii) in Path 1, we obtain

$$\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r+1)) = \begin{cases} \frac{1}{N} + \frac{1}{N^2} + \frac{3}{N^3} + o(\frac{1}{N^3}) & \text{when } r = N - 2x - 1, \\ \frac{1}{N} + \frac{1}{N^2} + \frac{2}{N^3} + o(\frac{1}{N^3}) & \text{otherwise.} \end{cases}$$

Path 3. Figure 4.9 shows a state transition diagram in Path 3. Let $Y = S_r[j_r] \neq N - x$ and $X \neq W \neq Y$. From the figure, the events A_r, B'_r, and $(j_r = k \neq r, r+1)$ imply

$$t_r = X + Y, \quad t_{r+1} = N - x - W, \quad Z_r = S_r[X + Y] = r + 1 + x, \quad Z_{r+1} = S_{r+1}[N - x + W].$$

Note that t_r and t_{r+1} are independent, and then we have

$$\begin{aligned}\{C_r \mid B'_r \wedge A_r \wedge (j_r = r) &= \{S_{r+1}[N - x + W] = r + 1 + x \mid B'_r \wedge A_r \wedge (j_r = r)\} \\ &\Leftrightarrow \{(t_r, t_{r+1}) = (r+1, j_{r+1})\} \vee \{(t_r, t_{r+1}) = (j_{r+1}, t+1)\} \vee \{t_r = t_{r+1}\}.\end{aligned}$$

From the discussion of (i)–(iii) in Path 1, we obtain

$$\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)) = \begin{cases} \frac{2}{N} - \frac{1}{N^2} + \frac{3}{N^3} + o(\frac{1}{N^3}) & \text{when } r = N - 2x - 1, \\ \frac{2}{N} - \frac{1}{N^2} + \frac{2}{N^3} + o(\frac{1}{N^3}) & \text{otherwise.} \end{cases}$$

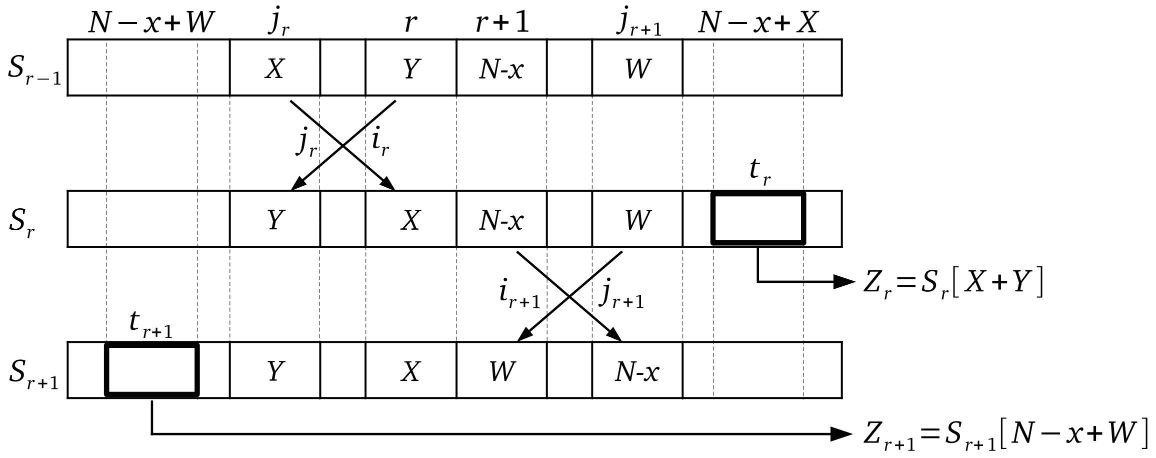

Figure 4.9: State transition diagram in Path 3 (Theorem 4.3).

In summary, we obtain

$$\begin{aligned}\Pr(A_r \mid B_r \wedge C_r) &\approx \frac{1}{N}\sum_{k=0}^{N-1}\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k)) \\ &= \frac{1}{N}\Bigg[\Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r)) + \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = r+1)) \\ &\quad + \sum_{\substack{k=0 \\ (k\neq r, r+1)}}^{N-1} \Pr(C_r \mid B'_r \wedge A_r \wedge (j_r = k))\Bigg],\end{aligned}$$

which is given as

$$\frac{1}{N}\sum_{r=0 \bmod N}^{N-1}\Pr(S_r[r+1] = N-x \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r+1+x)) \approx \frac{2}{N}\left(1 - \frac{1}{N} + \frac{2}{N^2}\right).$$

□

Remark 4.3. *The previous result of Theorem 4.2 is as follows:*

$$\Pr(S_r[r+1] = N-x \mid Z_{r+1} = Z_r \wedge Z_{r+1} = r+1+x) \approx \frac{2}{N}\left(1 - \frac{1}{N} + \frac{1}{N^2}\right).$$

After the revision, we improve the percentage of the relative error between the experimental value and the theoretical value from 0.387 % to 0.386 % (see Section 4.3). This is the result of revision in the same way as the proof of Theorem 4.1, but its revision shows that there was almost no effect of improving the relative error.

Corollary 4.1 ([IM16a, Corollary 1]). **(Integrated long-term Glimpse)** *After the r-th round of the PRGA for $r \geq 1$ and $\forall x \in [0, N-1]$, we have*

$$\Pr(S_r[r+1] = N - x \mid (Z_{r+1} = Z_r) \wedge (Z_{r+1} = r + 1 + x)) \approx \begin{cases} \dfrac{1}{N} + \dfrac{1}{N^3} & \textit{when } x = 0, \\ \dfrac{3}{N} & \textit{when } x = 1, \\ \dfrac{2}{N}\left(1 - \dfrac{1}{N} + \dfrac{2}{N^2}\right) & \textit{otherwise.} \end{cases}$$

4.2.3 Precise Biases on Specific Rounds

This subsection provides Theorems 4.4–4.6 and their proofs. Theorem 4.4 presents a precise bias on $r = 1$ of Theorem 4.1, and an event $(S_1[2] = 0)$ yields a positive bias when $Z_2 = Z_1$. Theorem 4.5 presents a precise bias on $r = 2$ of Theorem 4.1, and an event $(S_2[3] = 0)$ never occurs when $Z_3 = Z_2$. Theorem 4.6 presents a precise bias on $r = 2$ of Theorem 3.16, and an event $(S_2[j_2] = i_2 - Z_2)$ never occurs when $Z_2 = 1, 2$, or 129.

Theorem 4.4 ([IM16a, Theorem 5]). *After the first round of the PRGA, we have*

$$\Pr(S_1[2] = 0 \mid Z_2 = Z_1) \approx \Pr(S_0[1] = 1) + \frac{1}{N}\sum_{v=3}^{N-1} \Pr(S_0[1] = v).$$

Proof. We define main events as follows:

$$A := (S_1[2] = 0), \quad B := (Z_2 = Z_1),$$

where the target event $(A \mid B)$ is the case of $r = 1$ in Theorem 4.1. The proof mainly follows Theorem 4.1. Then, the probability of the event $(B \mid A)$ can be decomposed into three paths: $j_1 = 1$ (Path 1), $j_1 = 0, 2$ (Path 2), and $j_1 \neq 0, 1, 2$ (Path 3). Note that both $j_1 = S_0[1]$ and $j_2 = j_1 + S_1[2] = S_0[1]$ hold when the event A occurs. Let $X = S_1[1] \neq 0$.

Path 1. When $j_1 = 1$, $S_0[1] = X = 1$. Then, the event B always occurs when the event A occurs because $Z_2 = S_2[X] = S_2[1] = 0$ and $Z_1 = S_1[2X] = S_1[2] = 0$ (see Figure 4.4). Therefore, we obtain

$$\Pr(B \mid A \wedge (j_1 = 1)) = 1.$$

Path 2. When $j_1 = 0$, $S_0[1] = S_1[0] = 0$. On the other hand, when $j_1 = 2$, $S_0[1] = S1[2] = 2$. These facts are inconsistent with the assumption that the event A occurs, and then the event B never occurs. Therefore, we obtain

$$\Pr(B \mid A \wedge (j_1 = 0, 2)) = 0.$$

Path 3. Let $Y = S_1[j_1]$, and then $j_2 = S_0[1] = S_1[j_1] = Y$. When $X + Y = 2$, we have $Z_1 = S_1[2] = 0$ and $Z_2 = S_2[j_2] = 0$ because $Z_1 = S_1[X + Y]$ and $Z_2 = S_2[Y]$ from the discussion of Path 3 in the proof of Theorem 4.1 (see Figure 4.6), and thus the event B occurs when the event A occurs. Assuming that the event $(X + Y = 2)$ occurs with probability approximately $\frac{1}{N}$ (random association), and therefore we obtain

$$\Pr(B \mid A \wedge (j_1 \neq 0, 1, 2)) = \Pr(X + Y = 2) \approx \frac{1}{N}.$$

In summary, we obtain

$$\begin{aligned}\Pr(A \mid B) \approx \frac{1}{N} \sum_{k=0}^{N-1} \Pr(B \mid A \wedge (j_r = k)) &\approx \Pr(j_1 = 1) + \frac{1}{N} \sum_{v=3}^{N-1} \Pr(j_1 = v) \\ &= \Pr(S_0[1] = 1) + \frac{1}{N} \sum_{v=3}^{N-1} \Pr(S_0[1] = v),\end{aligned}$$

where $\Pr(S_0[1] = v)$ follows Lemma 3.1. □

Theorem 4.5 ([IM16a, Theorem 6]). *After the second round of the PRGA, we have*

$$\Pr(S_2[3] = 0 \mid Z_3 = Z_2) = 0.$$

Proof. We define main events as follows:

$$A := (S_2[3] = 0), \quad B := (Z_3 = Z_2),$$

where the event $(A \mid B)$ is the case of $r = 2$ in Theorem 4.1. The proof mainly follows Theorem 4.1. Then, the probability of the event $(B \mid A)$ can be decomposed into three paths: $j_2 = 2$ (Path 1), $j_2 = 3$ (Path 2), and $j_2 \neq 2, 3$ (Path 3). Note here that $j_2 = S_0[1] + S_1[2]$ and $j_3 = j_2 + S_2[3] = j_2$ when the event A occurs. Let $X = S_2[2]$.

Path 1. The discussion of Path 1 in the proof of Theorem 4.1 shows that the event $(Z_{r+1} = Z_r \mid S_r[r + 1] = 0)$ occurs only when either $r = 1$ or $r = 254$. Then, the event B never occurs, and therefore we obtain

$$\Pr(B \mid A \wedge (j_2 = 2)) = 0.$$

Path 2. The event B never occurs in Path 2 as we discussed in the proof of Theorem 4.1. Therefore, we obtain

$$\Pr(B \mid A \wedge (j_2 = 3)) = 0.$$

Path 3. Let $Y = S_2[j_2] \neq 0$. The discussion of Path 3 in the proof of Theorem 4.1 shows that the event $(Z_{r+1} = Z_r \mid S_r[r + 1] = 0)$ occurs when either $(X + Y, Y) = (r + 1, j_{r+1})$ or $(X + Y, Y) = (j_{r+1}, r + 1)$. Then, the event $(B \mid A)$ occurs when either $(X + Y, Y) = (3, j_3)$ or $(X + Y, Y) = (j_2, 3)$ (see Figure 4.6).

Case 1. We prove $(X+Y,Y) \neq (3,j_3)$. If the event $(Y=j_3)$ occurs, then $S_0[1]=0$ always holds because $j_3 = S_0[1]+S_1[2]$ and $S_1[2]=Y$. In this case, $S_1[0]=S_0[1]=0$ from the 5th step in Algorithm 2. This fact is inconsistent with the assumption of Path 3 because $S_1[0] \neq S_2[3]$. Therefore, we obtain $(X+Y,Y) \neq (3,j_3)$.

Case 2. We prove $(X+Y,Y)=(j_2,3)$. Similarly, if the event $(X+Y=j_2)$ occurs, then $S_0[1]=X$ always holds because $j_2=S_0[1]+S_1[2]$ and $S_1[2]=Y$, and $j_1=j_2$ always holds because $S_0[1]=S_1[j_1]=X$ and $S_1[j_2]=X$. The fact that an event $(j_1=j_2)$ means $Y=0$ because $j_1=S_0[1]$ and $j_2=S_0[1]=S_1[2]=j_1+Y$. Therefore, we obtain $(X+Y,Y) \neq (j_2,3)$.

From Cases 1 and 2, the event B never occurs in Path 3, and therefore we obtain

$$\Pr(B \mid A \wedge (j_2 \neq 2,3)) = 0.$$

In summary, the event $(B \mid A)$ never occurs, and we obtain

$$\Pr(A \mid B) = \frac{\Pr(A \wedge B)}{\Pr(B)} = \frac{\Pr(A)\Pr(B \mid A)}{\Pr(B_r)} = \frac{\Pr(A)\cdot 0}{\Pr(B_r)} = 0. \qquad \square$$

Theorem 4.6 ([IM16a, Theorem 7]). *After the second round of the PRGA, we have*

$$\Pr((S_2[j_2] = i_2 - Z_2) \wedge (Z_2 = 1,2,129)) = 0.$$

Proof. We prove that none of the events $(S_2[j_2]=2-Z_2)\wedge(Z_2=1)$, $(S_2[j_2]=2-Z_2)\wedge(Z_2=2)$, or $(S_2[j_2]=2-Z_2)\wedge(Z_2=129)$ occurs by reduction to absurdity. Through the proof, we use $i_1=1$ and $i_2=2$ for simplicity, and often use facts that $j_1=S_0[1](=S_1[j_1])$ and $j_2=j_1+S_1[2]$ from the 4th step in Algorithm 2.

Event 1. If the events $(S_2[j_2]=2-Z_2)$ and $(Z_2=1)$ occur simultaneously, then $S_2[j_2]=2-1=1$ always holds. From the 4th and 5th steps in Algorithm 2, we have

$$S_1[2] = S_2[j_2] = 1, \tag{4.1}$$

$$S_1[j_1] = S_0[1] = j_1, \tag{4.2}$$

$$j_2 = j_1 + S_1[2] = j_1 + 1. \tag{4.3}$$

Furthermore, from the 6th and 7th steps in Algorithm 2 and Equation (4.1), we have

$$Z_2 = S_2[S_2[i_2]+S_2[j_2]] = S_2[S_1[j_2]+1] = 1. \tag{4.4}$$

Combining Equations (4.1), (4.3), and (4.4), $j_2 = S_1[j_2]+1 = j_1+1$. Therefore, we obtain

$$S_1[j_2] = j_1. \tag{4.5}$$

Then, Equations (4.2) and (4.5) yield an inconsistent result of $j_1 = j_2$. Therefore, the events $(S_2[j_2] = 2 - Z_2)$ and $(Z_2 = 1)$ never occur simultaneously, and thus $\Pr((S_2[j_2] = 2 - Z_2) \wedge (Z_2 = 1)) = 0$.

Event 2. If the events $(S_2[j_2] = 2 - Z_2)$ and $(Z_2 = 2)$ occur simultaneously, then $S_2[j_2] = 2 - 2 = 0$ always holds, which implies $S_1[2] = S_2[j_2] = 0$ from the 4th and 5th steps in Algorithm 2. We prove that $S_0[2]$ is never swapped with $S_0[1]$ in the first round. Let us assume that $S_0[2]$ is swapped with $S_0[1]$, which implies $j_1 = 2$. By swapping, $S_0[1] = S_1[2] = 0$ and $S_0[1] = j_1$ are also applied. Apparently, this is a contradiction to $j_1 = 2$. Thus, $S_0[2]$ is never swapped, and $S_0[2] = S_1[2] = 0$ holds. This yields that an event $(Z_2 = 2)$ occurs under $S_0[2] = 0$, which is, however, in conflict with the fact[1] that the event $(Z_2 = 2)$ never occurs when $S_0[1] = 2$ or $S_0[2] = 0, 2$. Therefore, the events $(S_2[j_2] = 2 - Z_2)$ and $(Z_2 = 2)$ never occur simultaneously, and thus $\Pr((S_2[j_2] = 2 - Z_2) \wedge (Z_2 = 2)) = 0$.

Event 3. If the events $(S_2[j_2] = 2 - Z_2)$ and $(Z_2 = 129)$ occur simultaneously, then $S_2[j_2] = 2 - 129 = 129$ always holds, which implies $S_1[2] = S_2[j_2] = 129$ from the 4th and 5th steps in Algorithm 2. $S_0[1]$ is never swapped with $S_0[2]$ in the first round because it is necessary for swapping that all of $j_1 = 2$, $S_0[1] = S_1[2] = 129$, and $S_0[1] = j_1$, which induces a contradiction of $j_1 = 129 = 2$. Because $S_0[2]$ is never swapped, $S_0[1] \neq 2$ and $S_0[2] = S_1[2] = 129$. This yields that the event $(Z_2 = 129])$ occurs under $S_0[1] \neq 2$ and $S_0[2] = 129$, which is, however, in conflict with the fact[2] that the event $(Z_2 = 129)$ never occurs when $(S_0[1] \neq 2) \wedge (S_0[2] = 129)$ or $(S_0[1] \neq 2) \wedge (S_0[2] = 0)$. Therefore, the events $(S_2[j_2] = 2 - Z_2)$ and $(Z_2 = 129)$ never occur simultaneously, and thus $\Pr((S_2[j_2] = 2 - Z_2) \wedge (Z_2 = 129)) = 0$.

In summary, we obtain

$$\Pr((S_2[j_2] = i_2 - Z_2) \wedge (Z_2 = 1, 2, 129)) = 0. \qquad \square$$

4.3 Experimental Evaluations

We have performed experiments to check the accuracy of the theoretical values in all theorems. The number of samples for our experiments is at least $\mathcal{O}(N^3)$ according to Theorem 3.2. This is because each of the target events in all theorems has a relative bias with probability at least $\mathcal{O}(\frac{1}{N})$. Then, our experiments used N^3 randomly chosen keys of 16 bytes and N^3 keystream bytes for each key. This means that N^6 samples are used to check the accuracy of the theoretical values in Theorems 4.1–4.3. On the other hand, our experiments used N^5 samples randomly chosen keys of 16 bytes to check the accuracy of the theoretical values in Theorems 4.4–4.6, Therefore, the number of samples satisfies the condition to distinguish each of the target events from random distribution with constant probability of success.

We have evaluated the percentage of the relative error ϵ_{max} of the experimental values compared with the theoretical values (see Section 2.5.3). Table 4.1 shows the experimental

[1] It is described in the proof of Theorem 3 in [Sar15].

[2] It is described in the proof of Theorem 1 in [SGPM15].

Table 4.1: Comparison between experimental and theoretical values.

Results	Experimental Value	Theoretical Value	$\epsilon_{max}(\%)$
Theorem 4.1			
when $r = 0 \bmod N$	0.000030728 $\approx \frac{2}{N^2} + \frac{3.53}{N^3}$	0.000030518 $\approx \frac{2}{N^2} + \frac{0}{N^3}$	0.686
when $r = 1 \bmod N$	0.000045546 $\approx \frac{3}{N^2} - \frac{3.86}{N^3}$	0.000045657 $\approx \frac{3}{N^2} - \frac{2}{N^3}$	0.245
when $r = N-3 \bmod N$	0.000030431 $\approx \frac{2}{N^2} - \frac{1.45}{N^3}$	0.000030339 $\approx \frac{2}{N^2} - \frac{3}{N^3}$	0.304
when $r = N-2 \bmod N$	0.000045737 $\approx \frac{3}{N^2} - \frac{0.66}{N^3}$	0.000045836 $\approx \frac{3}{N^2} + \frac{1}{N^3}$	0.218
when $r = N-1 \bmod N$	0.000015217 $\approx \frac{1}{N^2} - \frac{0.70}{N^3}$	0.000015318 $\approx \frac{1}{N^2} + \frac{1}{N^3}$	0.667
when r is even and $r \neq 0, N-2 \bmod N$	0.000030524 $\approx \frac{2}{N^2} + \frac{0.11}{N^3}$	0.000030398 $\approx \frac{2}{N^2} - \frac{2}{N^3}$	0.415
when r is odd and $r \neq 1, N-3, N-1 \bmod N$	0.000030381 $\approx \frac{2}{N^2} - \frac{2.29}{N^3}$	0.000030279 $\approx \frac{2}{N^2} - \frac{4}{N^3}$	0.338
for the averaged result	0.000030513 $\approx \frac{2}{N^2} - \frac{0.08}{N^3}$	0.000030458 $\approx \frac{2}{N^2} - \frac{1}{N^3}$	0.182
Theorem 4.2			
when $x = 1$	0.003922408 $\approx \frac{1}{N} + \frac{1.06}{N^2}$	0.003906310 $\approx \frac{1}{N} + \frac{1}{N^3}$	0.410
when $x = N-1$	0.000030683 $\approx \frac{2}{N^2} + \frac{2.78}{N^3}$	0.000030518 $\approx \frac{2}{N^2} + \frac{0}{N^3}$	0.541
when $x \neq 1, N-1$	0.000015259 $\approx \frac{1}{N^2} + \frac{0}{N^3}$	0.000015259 $\approx \frac{1}{N^2} + \frac{0}{N^3}$	0.004
Theorem 4.3	0.007812333 $\approx \frac{2}{N} - \frac{0.01}{N^2}$	0.007782221 $\approx \frac{2}{N} - \frac{2}{N^2} + \frac{4}{N^3}$	0.386
Theorem 4.4	0.007801373 $\approx \frac{2}{N} - \frac{0.73}{N^2}$	0.007751621 $\approx \frac{2}{N} - \frac{4}{N^2}$	0.640
Theorem 4.5	0	0	–
Theorem 4.6	0	0	–

and theoretical values, and the percentage of the relative errors ϵ_{max}. Note that a polynomial expression evaluated the experimental value is also listed in each case. From the table, we can see that ϵ_{max} is small enough in each case, such as $\epsilon_{max} \leq 0.686$ (%). A slight difference between the experimental and theoretical value is due to assuming the probability of random association, and its strict analysis remains an open problem. As a result, we have checked the accuracy of the theoretical values in all theorems.

4.4 Chapter Conclusion

This chapter has precisely investigated the existing Glimpse Correlations from the following two approaches. One is to examine possibilities of new events with positive or negative biases on all values in addition to a known value. The other is to improve the conditions of the probability of known biases on specific rounds. As a result, we have proved cases with new biases theoretically in addition to the existing Glimpse Correlations. In the first approach, combining our new biases and known ones, the Long-term Glimpse can be integrated into biases of $S_r[r+1] \in [0, N-1]$ when $Z_{r+1} = Z_r$. In the second approach, we have successfully found that the events $(S_2[3] = 0 \mid Z_3 = Z_2)$ and $((S_2[j_2] = i_2 - Z_2) \wedge (Z_2 = 1, 2, 129))$ never occur.

Chapter 5

Key Correlations of the Internal State Variables

In WPA-TKIP, the range of $K[1]$ is limited to either from 32 to 63 or from 96 to 127, and the value of $K[0] + K[1]$ must be always even. Therefore, Sen Gupta et al. first presented in [GMM+14] that a probability distribution of $K[0] + K[1]$ has biases from a relation between $K[0]$ and $K[1]$ in WPA-TKIP (see Theorem 3.11 and Table 3.2).

They also presented significant key correlations of the keystream bytes in WPA-TKIP such as $Z_1 = -K[0] - K[1]$, $Z_3 = K[0] + K[1] + K[2] + 3$, $Z_{256} = -K[0]$, and $Z_{257} = -K[0] - K[1]$. Their observed key correlations can be updated to the existing set of the strongest short-term biases in the keystream bytes (see Table 3.1). As a result, they extended the IOWM attack in [IOWM13], particularly on WPA-TKIP, by using key correlations of the keystream bytes, and improved the efficiency for the attack.

This chapter investigates key correlations of the *unknown* internal state variables $\{S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1}, $t_{r+1}\}$ in generic RC4 and WPA-TKIP. A significant difference between ours and the previous work in [GMM+14] is whether the analysis target is the internal state variables or the keystream bytes. Actually, key correlations of the internal state variables are applied to the existing state recovery attacks, particularly on WPA-TKIP, and would improve the efficiency for the attack. We further focus on a difference between generic RC4 and WPA-TKIP, and found some different correlations. Such correlations reflect a difference of the probability distribution of $K[0] + K[1]$ in generic RC4 and WPA-TKIP.

Our motivation in this chapter is to prove key correlations of the internal state variables theoretically. Our theoretical proofs of key correlations can clarify how TKIP induces biases in the internal state. If we demonstrate how many correlations have been existed in the internal state, the RC4 key setting in WPA can be redesigned securely while maintaining congruity with TKIP. WPA-TKIP should have been designed in such a way that it can retain the security level of generic RC4. Our cryptanalysis would be also useful to investigate a generic construction of key setting including the known IV in such a way that it can retain the security level of the original scheme.

Our contributions in this chapter can be summarized as the following 22 theorems:

- Theorems 5.1 and 5.2 present $\Pr(S_0[i_1] = K[0])$ in generic RC4 and WPA-TKIP, respectively. Particularly, we emphasize that $\Pr(S_0[i_1] = K[0]) = 0$ in WPA-TKIP.

- Theorems 5.3 and 5.4 present $\Pr(S_0[i_1] = K[0] - K[1] - 3)$ in generic RC4 and WPA-TKIP, respectively. Theorems 5.5 and 5.6 present $\Pr(S_0[i_1] = K[0] - K[1] - 1)$ in generic RC4 and WPA-TKIP, respectively. Theorems 5.7 and 5.8 present $\Pr(S_0[i_1] = -K[0] - K[1] - 3)$ in generic RC4 and WPA-TKIP, respectively. Theorems 5.11 and 5.13 present $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$ and $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x)$ for $x \in \{-3, -1, 1\}$, respectively. These theorems only in WPA-TKIP provide approximately twice the probability of random association $\frac{1}{N}$.

- Theorem 5.9 presents that $\Pr(S_0[i_1] = K[0]+K[1]+K[2]+3)$ is a relatively low probability in comparison with the probability of random association $\frac{1}{N}$ in generic RC4 and WPA-TKIP.

- Theorem 5.10 presents that $\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ is a relatively high probability in comparison with the probability of random association $\frac{1}{N}$ in generic RC4 and WPA-TKIP. It is induced by the Roos Biases as Theorem 3.19, that is $\Pr(S_0[2] = K[0] + K[1] + K[2] + 3) \approx \left(1 - \frac{2}{N}\right) \cdot \left(1 - \frac{1}{N}\right)^{N+3} + \frac{1}{N}$.

- Theorem 5.12 presents that $\Pr(S_1[i_2] = K[1] + K[2] + 3)$ is approximately twice the probability of random association $\frac{1}{N}$ in generic RC4 and WPA-TKIP.

- Theorem 5.14 presents that $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3)$ shows a positive bias in generic RC4 but a negative bias in WPA-TKIP.

- Theorem 5.15 presents that $\Pr(S_{255}[i_{256}] = K[0])$ is a relatively high probability in comparison with the probability of random association $\frac{1}{N}$ in generic RC4 and WPA-TKIP. However, Theorem 5.16 presents that $\Pr(S_{255}[i_{256}] = K[1])$ is a relatively high probability only in WPA-TKIP.

- Theorem 5.17 presents $\Pr(S_r[i_{r+1}] = K[0]+K[1]+1)$ in both generic RC4 and WPA-TKIP for $0 \leq r \leq N$, and its distribution reflects the probability distribution of $K[0] + K[1]$.

- Theorems 5.18–5.22 provide theoretical analyses of the second round index j_2.

We further discuss secure RC4 key setting in WPA-TKIP in such a way that it can retain the security level of generic RC4. If the RC4 key setting is refined, it can be difficult to induce key correlations including the keystream bytes Z_r or the internal state variables $\{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$. In order to investigate toward secure RC4 key setting in WPA-TKIP, we carefully set an arbitrary three bytes of the RC4 key $\{K[x], K[y], K[z]\}$ from the known IV in the same way as the original setting in WPA-TKIP as follows:

$$\begin{aligned} K[x] &= (\texttt{IV16} \gg \texttt{8}) \mathbin{\&} \texttt{0xFF}, \\ K[y] &= ((\texttt{IV16} \gg \texttt{8}) \mid \texttt{0x20}) \mathbin{\&} \texttt{0x7F}, \\ K[z] &= \texttt{IV16} \mathbin{\&} \texttt{0xFF}. \end{aligned}$$

As a result of our investigations, the number of key correlations induced by our refined setting, e.g., $(x, y, z) = (9, 10, 11)$, can be reduced by approximately 70% in comparison with that in the original setting in WPA-TKIP.

The remainder of this chapter is organized as follows: Section 5.1 discusses new key correlations of the internal state variables observed by our experiments. Section 5.2 presents the theoretical proofs of newly observed key correlations. Section 5.3 demonstrates the experimental simulations in order to confirm the accuracy of the theoretical proofs. Section 5.4 discuss secure RC4 key setting in such a way that it can retain the security level of generic RC4. Section 5.5 concludes this chapter.

5.1 Experimental Observations

This section presents our experimental observations of new key correlations of the following unknown internal state variables in generic RC4 and WPA-TKIP: $S_r[i_{r+1}]$, $S_r[j_{r+1}]$, j_{r+1}, and t_{r+1} for $r \geq 0$. In [GMM+14], Sen Gupta et al. investigated key correlations of the keystream bytes Z_r by using a linear form

$$Z_r = a \cdot K[0] + b \cdot K[1] + c \cdot K[2] + d \tag{5.1}$$

for $a, b, c \in \{-1, 0, 1\}$ and $d \in \{-3, -2, -1, 0, 1, 2, 3\}$ for $r \geq 1$. We then extend their linear form in Equation (5.1) to

$$X_r = a \cdot Z_{r+1} + b \cdot K[0] + c \cdot K[1] + d \cdot K[2] + e, \tag{5.2}$$

where $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$, $a, b, c, d \in \{-1, 0, 1\}$, and $e \in \{-3, -2, -1, 0, 1, 2, 3\}$ for $r \geq 0$. Sen Gupta et al. extended the IOWM attack in [IOWM13], particularly on WPA-TKIP, by using their observed key correlations, and improved the efficiency for the plaintext recovery attack. Similarly, if we extend the state recovery attack, particularly on WPA-TKIP, by using our observed key correlations, we will improve the efficiency for the attack.

We have performed experiments with all $4 \cdot 3^4 \cdot 7$ equations defined by Equation (5.2) in each round. Our experiments have used 2^{32} randomly chosen keys of 16 bytes in generic RC4 and WPA-TKIP. Tables 5.1 and A.1 summarize the lists of significant observations with probability more than 0.0048 or less than 0.0020 in either generic RC4 or WPA-TKIP. We can see from the tables that there exists a certain event with a bias only in WPA-TKIP but no bias in generic RC4. Particularly, we emphasize that an target event $(S_0[i_1] = K[0])$ yields an impossible

Table 5.1: New key correlations by Equation (5.2) in generic RC4 and WPA-TKIP.

X_r	Key correlations	RC4	WPA-TKIP	Remarks
$S_0[i_1]$	$K[0]$	0.001450	0	Theorems 5.1 and 5.2
	$K[0]-K[1]-3$	0.005337	0.007848	Theorems 5.3 and 5.4
	$K[0]-K[1]-1$	0.003922	0.007877	Theorems 5.5 and 5.6
	$-K[0]-K[1]-3$	0.005336	0.008437	Theorems 5.7 and 5.8
	$K[0]+K[1]+K[2]+3$	0.001492	0.001491	Theorem 5.9
$S_1[i_2]$	$K[0]+K[1]+K[2]+3$	0.360357	0.361718	Theorem 5.10
	$-K[0]-K[1]+K[2]-1$	0.005305	0.008197	Theorem 5.11
	$K[1]+K[2]+3$	0.008157	0.008092	Theorem 5.12
	$K[0]-K[1]+K[2]-3$	0.005295	0.008163	Theorem 5.13
	$K[0]-K[1]+K[2]-1$	0.005290	0.008171	Theorem 5.13
	$K[0]-K[1]+K[2]+1$	0.005309	0.008171	Theorem 5.13
	$K[0]-K[1]+K[2]+3$	0.005310	0.002838	Theorem 5.14
$S_{255}[i_{256}]$	$K[0]$	0.137294	0.138047	Theorem 5.15
	$K[1]$	0.003911	0.037189	Theorem 5.16
$S_r[i_{r+1}]$	$K[0]+K[1]+1$	Figure 5.1		Theorem 5.17
j_2	$K[2]$	0.004428	0.005571	Theorem 5.18
	$-K[0]-K[1]+K[2]-2$	0.003921	0.004574	Theorem 5.19
	$-K[0]-K[1]+K[2]$	0.003919	0.005573	Theorem 5.19
	$-K[0]-K[1]+K[2]+2$	0.003912	0.004545	Theorem 5.19
	$-K[0]+K[1]+K[2]$	0.003921	0.005501	Theorem 5.20
	$-K[1]+K[2]-2$	0.003911	0.005479	Theorem 5.21
	$-K[1]+K[2]+3$	0.003899	0.005476	Theorem 5.21
	$K[0]-K[1]+K[2]$	0.003918	0.005618	Theorem 5.22

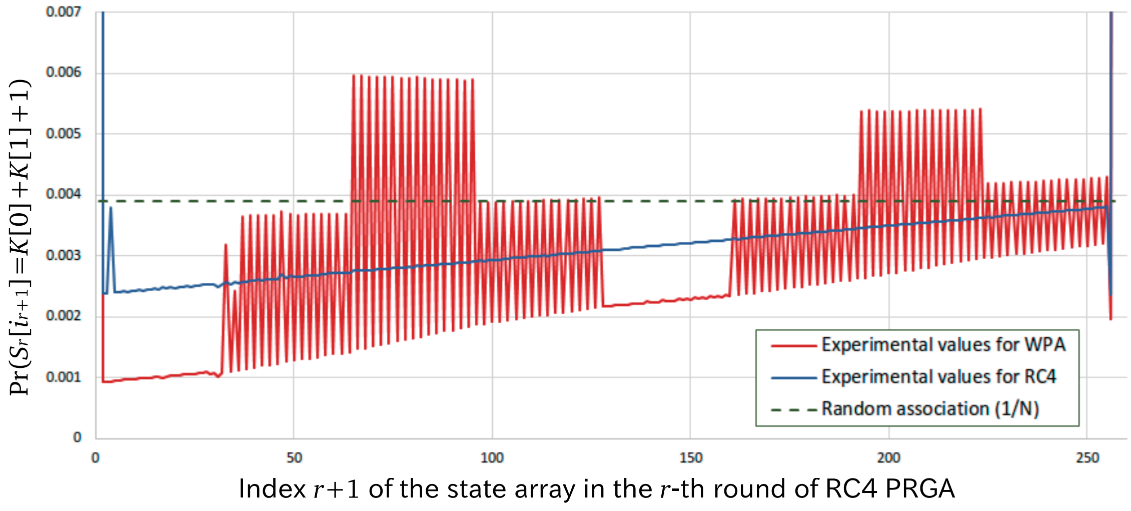

Figure 5.1: Observation of the event $(S_r[i_{r+1}] = K[0] + K[1] + 1)$.

condition in WPA-TKIP, and thus the probability of the target event is 0. Then, the value of $S_0[i_1]$ varies from 0 to $N-1$ except for $K[0]$.

We will provide the theoretical proofs of significant key correlations listed in Table 5.1. In the following proofs, we often use the Roos Biases (see Theorem 3.19), Nested Roos Biases (see Theorem 3.20), and probability distribution of $K[0]+K[1]$ (see Theorem 3.11), which are denoted by $\alpha_y = \Pr(S_0[y] = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x])$, $\beta_y = \Pr(S_0[S_0[y]] = \frac{y(y+1)}{2} + \sum_{x=0}^{y} K[x])$, and $\gamma_v = \Pr(K[0]+K[1] = v)$, respectively.

5.2 New Results

This section provides 22 theorems and their proofs. In our proofs, we often assume that the certain event occurs with probability approximately $\frac{1}{N}$, which is called the probability of *random association*. This is because it is difficult to demonstrate all events in the state transition of RC4, and it is a natural assumption based on the pseudorandomness of stream ciphers. The correctness of this assumption can be confirmed by experimental evaluations in Section 5.3. If this assumption is correct, the relative error between the experimental and theoretical value in each theorem will be small enough, and vice versa. Owing to this assumption, we often use the symbol of the approximate equation "≈" throughout this section.

5.2.1 Key Correlations of $S_0[i_1]$

This subsection provides Theorems 5.1–5.9 and their proofs. Theorems 5.1 and 5.2 present that an event $(S_0[i_1] = K[0])$ yields a negative bias in generic RC4 and never occurs in WPA-TKIP, respectively. Theorems 5.3 and 5.4 present that an event $(S_0[i_1] = K[0] - K[1] - 3)$ yields a positive bias in generic RC4 and occurs with twice the probability of random association $\frac{1}{N}$ in WPA-TKIP, respectively. Theorems 5.5 and 5.6 present that an event $(S_0[i_1] = K[0] - K[1] - 1)$ yields a slight bias in generic RC4 and occurs with twice the probability of random association $\frac{1}{N}$ in WPA-TKIP, respectively. Theorems 5.7 and 5.8 present that an event $(S_0[i_1] = -K[0] - K[1] - 3)$ yields a positive bias in generic RC4 and occurs with twice the probability of random association $\frac{1}{N}$ in WPA-TKIP, respectively. Theorem 5.9 presents that an event $(S_0[i_1] = K[0] + K[1] + K[2] + 3)$ yields a negative bias in both generic RC4 and WPA-TKIP. Note that Theorems 5.4, 5.6, and 5.8 mean that the first round of the internal state variable $S_0[i_1]$ can be guessed with twice the probability of random association $\frac{1}{N}$ by using known $K[0]$ and $K[1]$ in WPA-TKIP.

Theorem 5.1 ([IM16b, Theorem 1]). *In the initial state of the PRGA, we have*

$$\Pr(S_0[i_1] = K[0])_{\text{RC4}} \approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{N-2}.$$

Proof. Figure 5.2 shows a state transition diagram in the first two rounds of the KSA. From the 6th step in Algorithm 1, both $j_1^K = j_0^K + S_0^K[0] + K[0] = 0 + 0 + K[0] = K[0]$ and

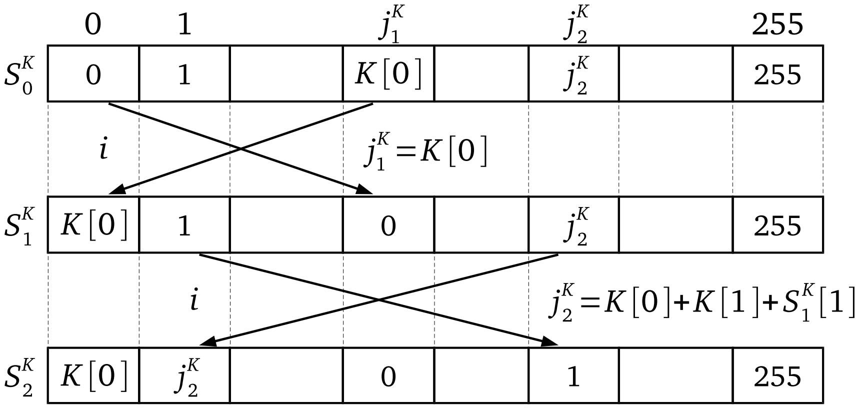

Figure 5.2: State transition diagram in the first two rounds of the KSA.

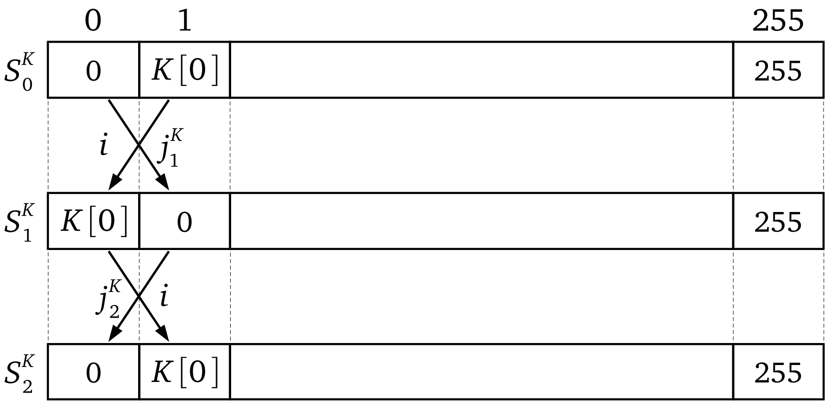

Figure 5.3: State transition diagram in Path 1-1 (Theorem 5.1).

$j_2^K = j_1^K + S_1^K[1] + K[1] = K[0] + K[1] + S_1^K[1]$. The probability of the target event ($S_0[i_1] = K[0]$) can be decomposed into three paths: $K[0] + K[1] = 0$ (Path 1), $K[0] + K[1] = 255$ (Path 2), and $K[0] + K[1] \neq 0, 255$ (Path 3). Both Paths 1 and 2 are further divided into two subpaths: $K[0] = 1$ (Paths 1-1 and 2-1) and $K[0] \neq 1$ (Paths 1-2 and 2-2), respectively. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) and $S_N^K[1]$ for simplicity.

Path 1-1. Figure 5.3 shows a state transition diagram in Path 1-1. After the second round of the KSA, $S_2^K[1] = K[0]$ always holds because $j_1^K = K[0] = 1$ and $j_2^K = K[0] + K[1] + S_1^K[1] = 0 + 0 = 0$. Furthermore, $S_r^K[1] = S_2^K[1]$ for $3 \leq r \leq N$ when $j_r^K \neq 1$ during the remaining $N - 2$ rounds of the KSA, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-2}$ because we assume that $j_r^K = 1$ for each round with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] \mid \text{Path 1-1}) \approx \left(1 - \frac{1}{N}\right)^{N-2}.$$

Path 1-2. Figure 5.4 shows a state transition diagram in Path 1-2. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds because $j_1^K = K[0] \neq 1$ and $j_2^K = (K[0] +$

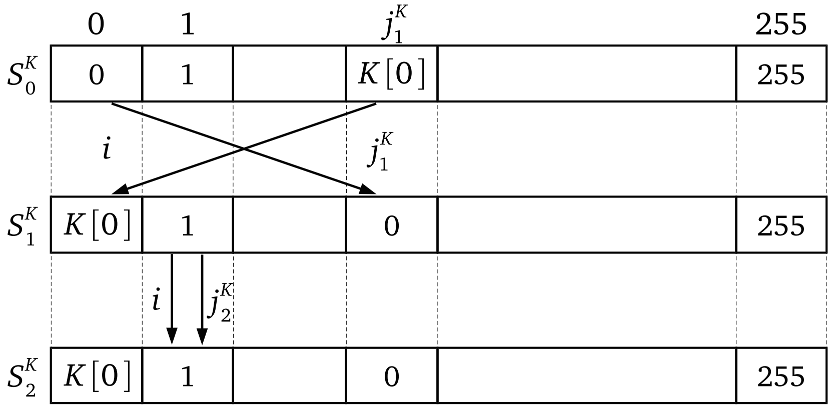

Figure 5.4: State transition diagram in Path 1-2 (Theorem 5.1).

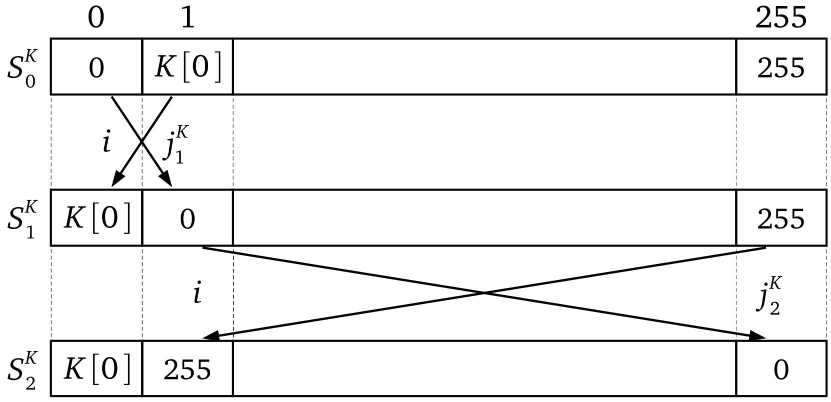

Figure 5.5: State transition diagram in Path 2-1 (Theorem 5.1).

$K[1]) + S_1^K[1] = 0 + 1 = 1$. Then, the target event $(S_0[1] = K[0])$ never occurs because $S_r^K[1] \neq K[0]$ always holds for $r \geq 2$ from Algorithm 1. Therefore, we obtain

$$\Pr(S_0[1] = K[0] \mid \text{Path 1-2}) = 0.$$

Path 2-1. Figure 5.5 shows a state transition diagram in Path 2-1. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds in the same way as the case of Path 1-2. Then, the target event $(S_0[1] = K[0])$ never occurs. Therefore, we obtain

$$\Pr(S_0[1] = K[0] \mid \text{Path 2-1}) = 0.$$

Path 2-2. Figure 5.6 shows a state transition diagram in Path 2-2. After the second round of the KSA, $S_2^K[1] = K[0]$ always holds in the same way as the case of Path 1-1. Then, the target event $(S_0[1] = K[0])$ occurs when $S_r[1] = S_2^K[1]$ for $3 \leq r \leq N$. Therefore, we obtain

$$\Pr(S_0[1] = K[0] \mid \text{Path 2-2}) \approx \left(1 - \frac{1}{N}\right)^{N-2}.$$

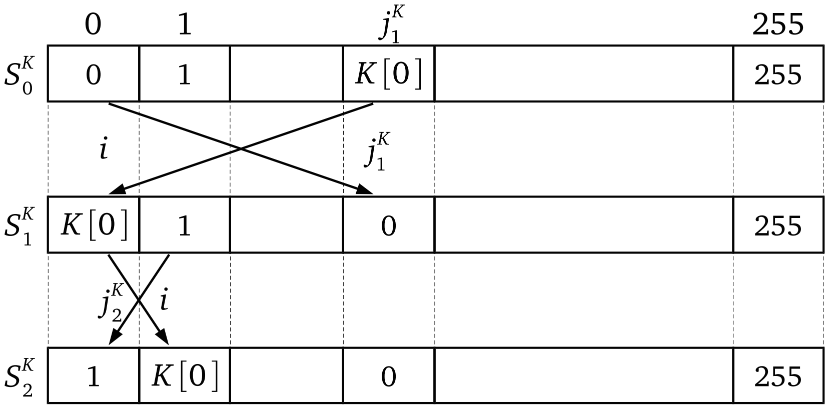

Figure 5.6: State transition diagram in Path 2-2 (Theorem 5.1).

Path 3. Figure 5.2 shows a state transition diagram in Path 3. After the second round of the KSA, $S_2^K[0] = K[0]$ always holds in the same way as the cases of Paths 1-2 and 2-1. Then, the target event $(S_0[1] = K[0])$ never occurs. Therefore, we obtain

$$\Pr(S_0[1] = K[0] \mid \text{Path 3}) = 0.$$

The target event $(S_0[1] = K[0])$ occurs only in either Paths 1-1 or 2-2. Both $K[0]$ and $K[1]$ are generated uniformly at random, and therefore we obtain

$$\begin{aligned}\Pr(S_0[1] = K[0])_{\text{RC4}} &= \Pr(S_0[1] = K[0] \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\ &\quad + \Pr(S_0[1] = K[0] \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2}) \\ &\approx \left(1 - \frac{1}{N}\right)^{N-2} \cdot \frac{1}{N^2} + \left(1 - \frac{1}{N}\right)^{N-2} \cdot \frac{1}{N} \cdot \left(1 - \frac{1}{N}\right) = \frac{1}{N}\left(1 - \frac{1}{N}\right)^{N-2}.\end{aligned}$$

□

Theorem 5.2 ([IM16b, Theorem 2]). *In the initial state of the PRGA in WPA-TKIP, we have*

$$\Pr(S_0[i_1] = K[0])_{\text{WPA}} = 0.$$

Proof. The target event $(S_0[i_1] = K[0])$ occurs when either $K[0]+K[1] = 0$ or 255, and Theorem 3.11 presents that neither $K[0] + K[1] = 0$ nor 255 in WPA-TKIP. Therefore, we obtain

$$\begin{aligned}\Pr(S_0[i_1] = K[0])_{\text{WPA}} &= \Pr(S_0[i_1] = K[0] \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\ &\quad + \Pr(S_0[i_1] = K[0] \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2}) \\ &\approx \left(1 - \frac{1}{N}\right)^{N-2} \cdot 0 + \left(1 - \frac{1}{N}\right)^{N-2} \cdot 0 = 0.\end{aligned}$$

□

Theorem 5.3 ([IM16b, Theorem 3]). *In the initial state of the PRGA, we have*

$$\Pr(S_0[i_1] = K[0] - K[1] - 3)_{\text{RC4}} \approx \frac{2}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1).$$

Proof. The probability of the target event ($S_0[i_1] = K[0] - K[1] - 3$) can be decomposed into two paths: $K[1] = 126, 254$ (Path 1) and $K[1] \neq 126, 254$ (Path 2). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. Because $K[0] - K[1] - 3 = K[0] + K[1] + 1$ when either $K[1] = 126$ or 254, the target event ($S_0[1] = K[0] - K[1] - 3$) occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 1}) = \alpha_1.$$

Path 2. Because $K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ when neither $K[1] = 126$ nor 254, the target event ($S_0[1] = K[0] - K[1] - 3$) never occurs if $S_0[1] = K[0] + K[1] + 1$. On the other hand, if $S_0[1] \neq K[0] + K[1] + 1$, we then assume that the target event ($S_0[1] = K[0] - K[1] - 3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \approx \frac{1}{N}(1 - \alpha_1).$$

$K[1]$ is generated uniformly at random, and therefore we obtain

$$\begin{aligned} \Pr(S_0[1] = K[0] - K[1] - 3)_{\text{RC4}} &= \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \frac{2}{N}\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1). \end{aligned}$$ □

Before showing Theorems 5.4 and 5.6, we prove Lemma 5.1. Lemma 5.1 presents a probability distribution of $K[0] - K[1]$ in WPA-TKIP.

Lemma 5.1 ([IM16b, Lemma 1]). *For $0 \leq v \leq N - 1$, a distribution of $K[0] - K[1] = v$ in WPA-TKIP is given by*

$$\begin{aligned} &\Pr(K[0] - K[1] = v) = \frac{1}{4} && \textit{when } v \in \{0, 96, 128, 224\}, \\ &\Pr(K[0] - K[1] = v) = 0 && \textit{otherwise.} \end{aligned}$$

Proof. The value of $K[0] - K[1]$ depends on that of $K[0]$, and therefore the probability distribution of $K[0] - K[1]$ can be obtained directly from Table 5.2. □

Theorem 5.4 ([IM16b, Theorem 4]). *In the initial state of the PRGA in WPA-TKIP, we have*

$$\begin{aligned} &\Pr(S_0[i_1] = K[0] - K[1] - 3)_{\text{WPA}} \\ &\approx \frac{4}{N}\alpha_1 + \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{91} + \left(1 - \frac{1}{N}\right)^{123} + \left(1 - \frac{1}{N}\right)^{219} + \left(1 - \frac{1}{N}\right)^{251}\right)\left(1 - \frac{4}{N}\right). \end{aligned}$$

Proof. Note that the range of $K[1]$ is limited to either from 32 to 63 or from 96 to 127 in WPA-TKIP (see Table 5.2). Then, as with the discussion in the proof of Theorem 5.3, the probability

Table 5.2: Probability distribution of $K[0]-K[1]$ in WPA-TKIP.

$K[0]$	$K[1]$ (depends on $K[0]$)		$K[0]-K[1]$
Range	Value	Range	Value
0–31	$K[0]+32$	32–63	224
32–63	$K[0]$	32–63	0
64–95	$K[0]+32$	96–127	224
96–127	$K[0]$	96–127	0
128–159	$K[0]-96$	32–63	96
160–191	$K[0]-128$	32–63	128
192–223	$K[0]-96$	96–127	96
224–255	$K[0]-128$	96–127	128

of the target event ($S_0[i_1]=K[0]-K[1]-3$) in WPA-TKIP can be decomposed into two paths: $K[1]=126$ (Path 1) and $K[1]\neq 126$ (Path 2). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1=1$) for simplicity.

Path 1. Because $K[0]-K[1]-3=K[0]+K[1]+1$ when $K[1]=126$, the target event ($S_0[1]=K[0]-K[1]-3$) occurs if and only if $S_0[1]=K[0]+K[1]+1$. Therefore, we obtain

$$\Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path 1})=\alpha_1.$$

Path 2. Because $K[0]-K[1]-3\neq K[0]+K[1]+1$ when $K[1]\neq 126$, the target event ($S_0[1]=K[0]-K[1]-3$) never occurs if $S_0[1]=K[0]+K[1]+1$. Now, we focus on the probability distribution of $K[0]-K[1]$ in WPA-TKIP (see Lemma 5.1). Assuming that the target event ($S_0[1]=K[0]-K[1]-3$) occurs, $S_0[1]$ can be one of the following four values: 93, 125, 221, or 253. Then, the probability in Path 2 can be further decomposed into four paths: $K[0]-K[1]=96$ (Path 2-1), $K[0]-K[1]=128$ (Path 2-2), $K[0]-K[1]=224$ (Path 2-3), and $K[0]-K[1]=0$ (Path 2-4).

Path 2-1. After the second round of the KSA, both $S_2^K[1]=K[0]+K[1]+1\neq 93$ (we can compute the sum of $K[0]$ and $K[1]$ from Table 5.2) and $S_2^K[93]=93$ from Algorithm 1. After that, if $S_r^K[93]\neq S_2^K[93]=93$ for $3\leq r\leq 93$, the target event ($S_0[1]=K[0]-K[1]-3=93$) never occurs in the same way as the discussion of Theorem 5.1 (Path 1-2 in the proof). If $S_r^K[93]=S_2^K[93]=93$, whose probability is approximately $\left(1-\frac{1}{N}\right)^{91}$ because we assume that $j_r^K=93$ for each round with probability approximately $\frac{1}{N}$ (random association), then we also assume that the target event ($S_0[1]=K[0]-K[1]-3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1]=K[0]-K[1]-3 \mid \text{Path 2}\wedge\text{Path 2-1})\approx\frac{1}{N}\left(1-\frac{1}{N}\right)^{91}.$$

The probabilities of the target event ($S_0[1]=K[0]-K[1]-3$) under the conditions of

Path 2-2, Path 2-3, and Path 2-4 can be obtained in the same way as the discussion of Path 2-1. Therefore, we obtain

$$\begin{aligned}
\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-2}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{123}, \\
\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-3}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{219}, \\
\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-4}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{251}.
\end{aligned}$$

The probability of these subpaths is taken from Lemma 5.1. In summary, we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-1}) \cdot \Pr(\text{Path 2-1} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-2}) \cdot \Pr(\text{Path 2-2} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-3}) \cdot \Pr(\text{Path 2-3} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2} \wedge \text{Path 2-4}) \cdot \Pr(\text{Path 2-4} \mid \text{Path 2}) \\
&\quad \approx \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{91} + \left(1 - \frac{1}{N}\right)^{123} + \left(1 - \frac{1}{N}\right)^{219} + \left(1 - \frac{1}{N}\right)^{251}\right).
\end{aligned}$$

Note that $\Pr(K[1] = 126) = \frac{1}{4}$ in WPA-TKIP (see Table 5.2). Therefore, we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 3) \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \frac{4}{N}\alpha_1 + \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{91} + \left(1 - \frac{1}{N}\right)^{123} + \left(1 - \frac{1}{N}\right)^{219} + \left(1 - \frac{1}{N}\right)^{251}\right)\left(1 - \frac{4}{N}\right).
\end{aligned}$$

□

Theorem 5.5 ([IM16b, Theorem 5])**.** *In the initial state of the PRGA, we have*

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1)_{\text{RC4}} \\
&\quad \approx \frac{1}{N^2}\left(1 - \frac{1}{N}\right)\left(\left(1 - \frac{1}{N}\right)^{N-3} + 1\right) + \frac{1}{N}\left(1 + \frac{2}{N}\right)\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1).
\end{aligned}$$

Proof. The probability of the target event $(S_0[i_1] = K[0] - K[1] - 1)$ can be decomposed into four paths: $K[1] = 0$ (Path 1), $K[1] = 127$ (Path 2), $K[1] = 255$ (Path 3), and $K[1] \neq 0, 127, 255$ (Path 4). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. In the first two rounds of the KSA, both $j_1^K = K[0]$ and $j_2^K = K[0] + K[1] + S_1^K[1]$ (see Figure 5.2). When $K[0] = 1$, both $S_2^K[1] = 0$ and $K[0] - K[1] - 1 = 0$ always hold because $j_1^K = 1$ and $S_1^K[1] = 0$. After that, $S_r^K[1] = S_2^K[1]$ for $3 \leq r \leq N$ when $j_r^K \neq 1$ during the remaining $N-2$ rounds of the KSA, whose probability is approximately $\left(1-\frac{1}{N}\right)^{N-2}$ because we assume that $j_1^K = 1$ for each round with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1} \wedge K[0] = 1) \approx \left(1-\frac{1}{N}\right)^{N-2}.$$

On the other hand, when $K[0] \neq 1$, both $S_2^K[1] = K[0]+1$ and $K[0]-K[1]-1 = K[0]-1$. We then assume that the target event $(S_0[1] = K[0] - K[1] - 1)$ occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1} \wedge K[0] \neq 1) \approx \frac{1}{N}.$$

$K[0]$ is generated uniformly at random, and $K[0]$ and $K[1]$ are mutually independent. In summary, we obtain

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path 1}) \\
&\quad = \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path 1} \wedge K[0] = 1) \cdot \Pr(K[0] = 1 \mid \text{Path 1}) \\
&\qquad + \Pr(S_0[i_1] = K[0] - K[1] - 1 \mid \text{Path 1} \wedge K[0] \neq 1) \cdot \Pr(K[0] \neq 1 \mid \text{Path 1}) \\
&\quad \approx \left(1-\frac{1}{N}\right)^{N-2} \cdot \frac{1}{N} + \frac{1}{N} \cdot \left(1-\frac{1}{N}\right) = \frac{1}{N}\left(1-\frac{1}{N}\right)\left(\left(1-\frac{1}{N}\right)^{N-3} + 1\right).
\end{aligned}$$

Path 2. Because $K[0] - K[1] - 1 = K[0] + K[1] + 1$ when $K[1] = 127$, the target event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2}) = \alpha_1.$$

Path 3. Because $K[0] - K[1] - 1 = K[0] + K[1] + 1$ when $K[1] = 255$, the target event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if $S_0[1] = K[0] + K[1] + 1$. From the discussion in Theorem 5.1, the event $(S_0[1] = K[0])$ occurs if and only if either $(K[0] + K[1] = 0) \wedge (K[0] = 1)$ or $(K[0] + K[1] = 255) \wedge (K[0] \neq 1)$. We assume that both $K[1] = 255$ and $S_0[1] = K[0] + K[1] + 1$, and the target event $(S_0[1] = K[0] - K[1] - 1)$ occurs if and only if either $K[0] = 0$ or 1. Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 3}) = \Pr(K[0] = 0, 1) \cdot \alpha_1.$$

Path 4. Because $K[0] - K[1] - 1 \neq K[0] + K[1] + 1$ when neither $K[1] = 0$, 127, nor 255, the target event $(S_0[1] = K[0] - K[1] - 1)$ never occurs if $S_0[1] = K[0] + K[1] + 1$. When $S_0[1] \neq K[0] + K[1] + 1$, we assume that the target event $(S_0[1] = K[0] - K[1] - 1)$ occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 4}) \approx \frac{1}{N} \cdot (1 - \alpha_1).$$

$K[1]$ is generated uniformly at random, and therefore we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1) \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 3}) \cdot \Pr(\text{Path 3}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 4}) \cdot \Pr(\text{Path 4}) \\
&\quad \approx \frac{1}{N^2}\left(1 - \frac{1}{N}\right)\left(\left(1 - \frac{1}{N}\right)^{N-3} + 1\right) + \frac{1}{N}\left(1 + \frac{2}{N}\right)\alpha_1 + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1),
\end{aligned}$$

where $\alpha_1 = \Pr(S_0[1] = K[0] + K[1] + 1) \approx \left(\frac{N-1}{N}\right)^{N+2} + \frac{1}{N}$. □

Theorem 5.6 ([IM16b, Theorem 6])**.** *In the initial state of the PRGA in WPA-TKIP, we have*

$$\begin{aligned}
&\Pr(S_0[i_1] = K[0] - K[1] - 1)_{\text{WPA}} \\
&\quad \approx \frac{4}{N}\alpha_1 + \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{93} + \left(1 - \frac{1}{N}\right)^{125} + \left(1 - \frac{1}{N}\right)^{221} + \left(1 - \frac{1}{N}\right)^{253}\right)\left(1 - \frac{4}{N}\right).
\end{aligned}$$

Proof. The proof itself is similar to that of Theorem 5.4. Note that the range of $K[1]$ is limited to either from 32 to 63 or from 96 to 127 in WPA-TKIP (see Table 5.2). Then, as with the discussion in the proof of Theorem 5.5, the probability of the target event ($S_0[i_1] = K[0] - K[1] - 1$) in WPA-TKIP can be decomposed into two paths: $K[1] = 127$ (Path 1) and $K[1] \neq 127$ (Path 2). In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. Because $K[0] - K[1] - 1 = K[0] + K[1] + 1$ when $K[1] = 127$, the target event ($S_0[1] = K[0] - K[1] - 1$) occurs if and only if $S_0[1] = K[0] + K[1] + 1$. Therefore, we obtain

$$\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1}) = \alpha_1.$$

Path 2. Because $K[0] - K[1] - 1 \neq K[0] + K[1] + 1$ when $K[1] \neq 127$, the target event ($S_0[1] = K[0] - K[1] - 1$) never occurs if $S_0[1] = K[0] + K[1] + 1$. Assuming that the target event ($S_0[1] = K[0] - K[1] - 1$) occurs, $S_0[1]$ can be one of the following values from Lemma 5.1: 95, 127, 223, or 255. Then, the probability in Path 2 can be further decomposed in four paths: $K[0] - K[1] = 96$ (Path 2-1), $K[0] - K[1] = 128$ (Path 2-2), $K[0] - K[1] = 224$ (Path 2-3), and $K[0] - K[1] = 0$ (Path 2-4). The probabilities of the target event ($S_0[1] = K[0] - K[1] - 1$) under the conditions of all subpaths can be computed in the same way as in the discussion in the proof of Theorem 5.4. Therefore, we obtain

$$\begin{aligned}
\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-1}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{93}, \\
\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-2}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{125}, \\
\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-3}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{221}, \\
\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-4}) &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{253}.
\end{aligned}$$

The probabilities of these subpaths are taken from Lemma 5.1, and therefore we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2}) \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-1}) \cdot \Pr(\text{Path 2-1} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-2}) \cdot \Pr(\text{Path 2-2} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-3}) \cdot \Pr(\text{Path 2-3} \mid \text{Path 2}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2} \wedge \text{Path 2-4}) \cdot \Pr(\text{Path 2-4} \mid \text{Path 2}) \\
&\quad \approx \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{93} + \left(1 - \frac{1}{N}\right)^{125} + \left(1 - \frac{1}{N}\right)^{221} + \left(1 - \frac{1}{N}\right)^{253}\right).
\end{aligned}$$

Note that $\Pr(K[1] = 126) = \frac{1}{4}$ in WPA-TKIP (see Table 5.2). In summary, we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 1) \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[1] = K[0] - K[1] - 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \frac{4}{N}\alpha_1 + \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{93} + \left(1 - \frac{1}{N}\right)^{125} + \left(1 - \frac{1}{N}\right)^{221} + \left(1 - \frac{1}{N}\right)^{253}\right)\left(1 - \frac{4}{N}\right).
\end{aligned}$$

□

Theorem 5.7 ([IM17, Theorem 1]). *In the initial state of the PRGA in generic RC4, we have*

$$\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\text{RC4}} \approx \frac{2}{N}\left(\alpha_1 + \frac{1}{N}(1 - \alpha_1)\right) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1).$$

Proof. The probability of the target event $(S_0[i_1] = -K[0] - K[1] - 3)$ in generic RC4 can be decomposed into two paths: $K[0] + K[1] = 126, 254$ (Path 1) and $K[0] + K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\text{RC4}}$. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ $(i_1 = 1)$ for simplicity.

Path 1. Because $-K[0] - K[1] - 3 = K[0] + K[1] + 1$, the target event $(S_0[1] = -K[0] - K[1] - 3)$ always occurs when $S_0[1] = K[0] + K[1] + 1$. In addition, when $S_0[1] \neq K[0] + K[1] + 1$, we assume that the target event ($S_0[1] = -K[0] - K[1] - 3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path } 1) = \alpha_1 + \frac{1}{N}(1 - \alpha_1).$$

Path 2. Because $-K[0]-K[1]-3 \neq K[0]+K[1]+1$, the target event ($S_0[1] = -K[0]-K[1]-3$) never occurs if $S_0[1] = K[0]+K[1]+1$. When $S_0[1] \neq K[0]+K[1]+1$, we assume that the target event ($S_0[1] = -K[0]-K[1]-3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path } 2) \approx \frac{1}{N}(1 - \alpha_1).$$

K is generated uniformly at random in generic RC4, and therefore we obtain

$$\begin{aligned}\Pr(S_0[1] = K[0] - K[1] - 3)_{\text{RC4}} &= \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path } 1) \cdot \Pr(\text{Path } 1)\\ &\quad + \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path } 2) \cdot \Pr(\text{Path } 2)\\ &\approx \frac{2}{N}(\alpha_1 + \frac{1}{N}(1-\alpha_1)) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1 - \alpha_1).\end{aligned}$$ □

Before showing Theorem 5.8, we prove Lemma 5.2.

Lemma 5.2 ([IM17, Corollary 1])**.** *For $0 \leq v \leq N-1$, a distribution of $-K[0] - K[1] = v$ in WPA-TKIP is given by*

$$\begin{aligned}&\Pr(-K[0] - K[1] = v) = 0 && \textit{if } v \textit{ is odd},\\ &\Pr(-K[0] - K[1] = v) = 0 && \textit{if } v \textit{ is even and } v \in [97, 128] \cup [225, 256],\\ &\Pr(-K[0] - K[1] = v) = \frac{2}{256} && \textit{if } v \textit{ is even and } v \in [1, 32] \cup [65, 96] \cup [129, 160] \cup [193, 224],\\ &\Pr(-K[0] - K[1] = v) = \frac{4}{256} && \textit{if } v \textit{ is even and } v \in [33, 64] \cup [161, 192].\end{aligned}$$

Proof. The value of $-K[0] - K[1]$ depends on that of $K[0]$, and therefore the probability distribution of $-K[0] - K[1]$ can be obtained directly from Table 5.3. □

Theorem 5.8 ([IM17, Theorem 2])**.** *In the initial state of the PRGA in WPA-TKIP for $0 \leq x \leq N-1$, we have*

$$\begin{aligned}&\Pr(S_0[i_1] = -K[0] - K[1] - 3)_{\text{WPA}}\\ &\quad\approx \frac{4}{N}\left(\alpha_1 + \frac{1}{N}(1-\alpha_1)\right) + \frac{1}{N}\sum_{x \neq 2,130} \Pr(-K[0] - K[1] = x)\left(1 - \frac{1}{N}\right)^{x-5}.\end{aligned}$$

Proof. The probability of the target event ($S_0[i_1] = -K[0] - K[1] - 3$) in WPA-TKIP can be decomposed into two paths: $-K[0] - K[1] = 2, 130$ (Path 1) and $-K[0] - K[1] \neq 2, 130$ (Path

Table 5.3: Probability distribution of $-K[0] - K[1]$ in WPA-TKIP.

$K[0]$	$K[1]$ (depends on $K[0]$)		$-K[0] - K[1]$ (only even)	
Range	Value	Range	Value	Range
0–31	$K[0] + 32$	32–63	$-2K[0] - 32$	161–224
32–63	$K[0]$	32–63	$-2K[0]$	129–192
64–95	$K[0] + 32$	96–127	$-2K[0] - 32$	33–96
96–127	$K[0]$	96–127	$-2K[0]$	1–64
128–159	$K[0] - 96$	32–63	$-2K[0] + 96$	35–96
160–191	$K[0] - 128$	32–63	$-2K[0] + 128$	1–64
192–223	$K[0] - 96$	96–127	$-2K[0] + 96$	161–224
224–255	$K[0] - 128$	96–127	$-2K[0] + 128$	129–192

2). These paths include all events in order to compute $\Pr(S_0[i_1] = -K[0]-K[1]-3)_{\text{WPA}}$. Under such conditions, we have

$$-K[0] - K[1] = x \Leftrightarrow K[0] + K[1] = N - x. \tag{5.3}$$

In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. Because $-K[0] - K[1] - 3 = K[0] + K[1] + 1$ from Equation (5.3), the target event ($S_0[1] = -K[0] - K[1] - 3$) always occurs when $S_0[1] = K[0] + K[1] + 1$. In addition, when $S_0[1] \neq K[0]+K[1]+1$, we assume that the target event ($S_0[1] = -K[0]-K[1]-3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path } 1) \approx \alpha_1 + \frac{1}{N}(1 - \alpha_1).$$

Path 2. Let $-K[0] - K[1] = x$. Because $-K[0] - K[1] - 3 \neq K[0] + K[1] + 1$ from Equation (5.3), the target event ($S_0[1] = -K[0] - K[1] - 3$ ($= x - 3$) never occurs when $S_0[1] = K[0] + K[1] + 1$. After the second round of the KSA, both $S_2^K[1] = K[0] + K[1] + 1 = N - x + 1$ and $S_2^K[x - 3] = x - 3$ from Equation (5.3) and Algorithm 1. Thereafter, if $S_r^K[x - 3] \neq S_2^K[x - 3]$ for $3 \leq r \leq x - 3$, the target event ($S_0[1] = -K[0] - K[1] - 3$) never occurs. When $S_r^K[x - 3] = S_2^K[x - 3] = x - 3$ is satisfied, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{x-5}$, we assume that the target event ($S_0[1] = -K[0] - K[1] - 3$) occurs with probability approximately $\frac{1}{N}$ (random association) because $S_{x-2}[1]$ may be swapped from $S_{x-3}[x - 3]$. Therefore, we obtain

$$\Pr(S_0[1] = -K[0] - K[1] - 3 \mid \text{Path } 2) \approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{x-5}.$$

In summary, we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] - K[1] - 3)_{\text{WPA}} \\
&\quad = \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path } 1) \cdot \Pr(\text{Path } 1)
\end{aligned}$$

$$
\begin{aligned}
&+ \Pr(S_0[1] = K[0] - K[1] - 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\approx \frac{4}{N}\left(\alpha_1 + \frac{1}{N}(1-\alpha_1)\right) + \frac{1}{N} \sum_{x \neq 2,130} \Pr(-K[0] - K[1] = x)\left(1 - \frac{1}{N}\right)^{x-5},
\end{aligned}
$$

where $\Pr(-K[0] - K[1] = x)$ follows Lemma 5.2. □

Theorem 5.9 ([IM17, Theorem 3]). *In the initial state of the PRGA, we have*

$$\Pr(S_0[i_1] = K[0] + K[1] + K[2] + 3) \approx \frac{1}{N}\left(1 - \frac{2}{N}\right)\left(1 - \frac{1}{N}\right)^{N-2} + \frac{1}{N^2}\left(3 - \frac{2}{N}\right).$$

Proof. Both $S_1^K[1] = 1$ and $S_2^K[2] = 2$ with high probability from Algorithm 1, and we obtain

$$
\begin{aligned}
j_1^K &= K[0], && (5.4)\\
j_2^K &= K[0] + K[1] + S_1^K[1] = K[0] + K[1] + 1, && (5.5)\\
j_3^K &= K[0] + K[1] + K[2] + S_1^K[1] + S_2^K[2] && (5.6)\\
&= K[0] + K[1] + K[2] + 3. && (5.7)
\end{aligned}
$$

When the above equations hold, $S_3^K[2] = K[0] + K[1] + K[2] + 3$ always holds from the 7th step in Algorithm 1. Thus, the target event ($S_0[i_1] = K[0] + K[1] + K[2] + 3$) never occurs because $S_r^K[i_1] \neq K[0] + K[1] + K[2] + 3$ always holds for $r \geq 3$. Then, the probability of the target event ($S_0[i_1] = K[0] + K[1] + K[2] + 3$) can be decomposed into two paths: $j_1^K = 1, 2$ (Path 1) and $j_1^K \neq 1, 2$ (Path 2). Path 2 is further divided into three subpaths: $j_2^K = 2$ (Path 2-1), $j_2^K \neq 2 \wedge K[2] = 254$ (Path 2-2), and $j_2^K \neq 2 \wedge K[2] \neq 254$ (Path 2-3). These paths include all events in order to compute $\Pr(S_0[i_1] = K[0] + K[1] + K[2] + 3)$. In the following proof, we use $S_0[1]$ instead of $S_0[i_1]$ ($i_1 = 1$) for simplicity.

Path 1. When $j_1^K = 1$, $S_1^K[1] \neq 1$ from the 7th step in Algorithm 1. Thus, $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds because $j_3^K \neq K[0] + K[1] + K[2] + 3$ from Equation (5.7). Similarly, when $j_1^K = 2$, $S_3^K[2] \neq K[0]+K[1]+K[2]+3$ always holds. We then assume that the target event ($S_0[1] = K[0] + K[1] + K[2] + 3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \approx \frac{1}{N}.$$

Path 2-1. When $j_2^K = 2$, $S_3^K[2] \neq K[0] + K[1] + K[2] + 3$ always holds in the same way as the discussion in Path 1. We then assume that the target event ($S_0[1] = K[0]+K[1]+K[2]+3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-1}) \approx \frac{1}{N}.$$

Path 2-2. Except in the above paths, Equations (5.4)–(5.7) always hold because we obtain both $S_1^K[1] = 1$ and $S_2^K[2] = 2$. When $K[2] = 254$, $j_2^K = j_3^K = K[0] + K[1] + K[2] + 3$ because $K[2]+3 = 1$. Thus, we obtain both $S_3^K[1] = K[0]+K[1]+K[2]+3$ and $S_3^K[2] = 1$ from the 7th step in Algorithm 1. After the third round of the KSA, $S_r^K[1] = S_3^K[1]$ for $4 \leq r \leq N$ when $j_r^K \neq 1$ during the remaining $N-3$ rounds of the KSA, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-3}$ because we assume that $j_r^K = 1$ with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-2}) \approx \left(1 - \frac{1}{N}\right)^{N-3}.$$

Path 2-3. As with the discussion in Path 2-2, Equations (5.4)–(5.7) always hold, and $j_2^K \neq j_3^K$ because $K[2] \neq 254$. Therefore, the target event $(S_0[1] = K[0] + K[1] + K[2] + 3)$ never occurs, and we obtain

$$\Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-3}) = 0.$$

In summary, the target event $(S_0[1] = K[0] + K[1] + K[2] + 3)$ occurs only in Paths 1, 2-1, and 2-2, and we obtain

$$\begin{aligned}
&\Pr(S_0[1] = K[0] + K[1] + K[2] + 3) \\
&\quad = \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\
&\qquad + \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-1}) \cdot \Pr(\text{Path 2-1}) \\
&\qquad + \Pr(S_0[1] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2}) \\
&\quad \approx \frac{1}{N} \cdot \frac{2}{N} + \frac{1}{N} \cdot \frac{1}{N}\left(1 - \frac{2}{N}\right) + \left(1 - \frac{1}{N}\right)^{N-3} \cdot \frac{1}{N}\left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) \\
&\quad = \frac{1}{N}\left(1 - \frac{2}{N}\right)\left(1 - \frac{1}{N}\right)^{N-2} + \frac{1}{N^2}\left(3 - \frac{2}{N}\right),
\end{aligned}$$

where we assume that four events $(j_1^K = 1)$, $(j_1^K = 2)$, $(j_2^K = 2)$, and $(K[2] = 254)$ occur with probability approximately $\frac{1}{N}$ (random association). □

5.2.2 Key Correlations of $S_1[i_2]$

This subsection provides Theorems 5.10–5.14 and their proofs. Theorem 5.10 presents that an event $(S_1[i_2] = K[0]+K[1]+K[2]+3)$ occurs with relatively high probability in both generic RC4 and WPA-TKIP. It is induced by the Roos Biases, that is $\alpha_2 = \Pr(S_0[2] = K[0]+K[1]+K[2]+3)$. Theorems 5.11 and 5.13 present that four events of $S_1[i_2]$ yield a positive bias in both generic RC4 and WPA-TKIP. Theorem 5.12 presents that an event $(S_1[i_2] = K[1] + K[2] + 3)$ occurs with twice the probability of random association $\frac{1}{N}$ in both generic RC4 and WPA-TKIP. Theorem 5.14 presents that an event $(S_1[i_2] = K[0] - K[1] + K[2] + 3)$ yields a positive bias in generic RC4 but a negative bias in WPA-TKIP. Note that Theorems 5.10–5.13 mean that the second round of the internal state $S_1[i_2]$ can be guessed in high probability by using known RC4 key bytes $\{K[0], K[1], K[2]\}$ in WPA-TKIP. In order to prove the following theorems, let us denote the results of Theorems 5.9 and 5.10 as $\beta = \Pr(S_0[1] = K[0] + K[1] + K[2] + 3)$ and $\gamma = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3)$, respectively.

Theorem 5.10 ([IM17, Theorem 4])**.** *After the first round of the PRGA, we have*

$$\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3) \approx \beta \cdot \Pr(S_0[1] = 2) + \alpha_2 \cdot \big(1 - \Pr(S_0[1] = 2)\big).$$

Proof. The probability of the target event $(S_1[i_2] = K[0] + K[1] + K[2] + 3)$ can be decomposed into two paths: $j_1 = 2$ (Path 1) and $j_1 \neq 2$ (Path 2). These paths include all events in order to compute $\Pr(S_1[i_2] = K[0] + K[1] + K[2] + 3)$. Note that $j_1 = S_0[1]$ from the 4th step in Algorithm 2. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ $(i_2 = 2)$ for simplicity.

Path 1. In the condition of Path 1, the target event $(S_1[2] = K[0] + K[1] + K[2] + 3)$ always occurs if and only if $S_0[1] = K[0] + K[1] + K[2] + 3$ from the 5th step in Algorithm 2. We assume that events $(j_1 = 2)$ and $(S_0[1] = K[0]+K[1]+K[2]+3)$ are mutually independent. Therefore, we obtain

$$\Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) = \beta.$$

Path 2. In the condition of Path 2, the target event $(S_1[2] = K[0] + K[1] + K[2] + 3)$ always occurs if and only if $S_0[2] = K[0] + K[1] + K[2] + 3$ from the 5th step in Algorithm 2. We assume that events $(j_1 \neq 2)$ and $(S_0[2] = K[0]+K[1]+K[2]+3)$ are mutually independent. Therefore, we obtain

$$\Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2}) = \alpha_2.$$

In summary, we obtain

$$\begin{aligned}
&\Pr(S_1[2] = K[0] + K[1] + K[2] + 3)\\
&\quad = \Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1})\\
&\qquad + \Pr(S_1[2] = K[0] + K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2})\\
&\quad \approx \beta \cdot \Pr(j_1 = 2) + \alpha_2 \cdot \big(1 - \Pr(j_1 = 2)\big)\\
&\quad = \beta \cdot \Pr(S_0[1] = 2) + \alpha_2 \cdot \big(1 - \Pr(S_0[1] = 2)\big),
\end{aligned}$$

where $\Pr(S_0[1] = 2)$ follows Lemmas 3.1 and 3.4 in generic RC4 and WPA-TKIP. □

Theorem 5.11 ([IM17, Theorem 5])**.** *After the first round of the PRGA, we have*

$$\begin{aligned}&\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)\\ &\approx \begin{cases}\frac{2}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\gamma) & \textit{for RC4,}\\ \frac{4}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1-\gamma) & \textit{for WPA-TKIP.}\end{cases}\end{aligned}$$

Proof. The probability of the target event ($S_1[i_2] = -K[0]-K[1]+K[2]-1$) can be decomposed into two paths: $K[0] + K[1] = 126, 254$ (Path 1) and $K[0] + K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ ($i_2 = 2$) for simplicity.

Path 1. Because $-K[0] - K[1] + K[2] - 1 = K[0] + K[1] + K[2] + 3$, the target event ($S_1[2] = -K[0] - K[1] + K[2] - 1$) always occurs when $S_1[2] = K[0] + K[1] + K[2] + 3$. In addition, when $S_0[1] \neq K[0] + K[1] + 1$, we assume that the target event ($S_1[2] = -K[0] - K[1] + K[2] - 1$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 1}) = \gamma + \frac{1}{N}(1-\gamma).$$

Path 2. Because $-K[0] - K[1] + K[2] - 1 \neq K[0] + K[1] + K[2] + 3$, the target event ($S_1[2] = -K[0] - K[1] + K[2] - 1$) never occurs when $S_1[2] = K[0] + K[1] + K[2] + 3$. When $S_1[2] \neq K[0] + K[1] + K[2] + 3$, we assume that the target event ($S_1[2] = -K[0] - K[1] + K[2] - 1$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 2}) = \frac{1}{N}(1-\gamma).$$

Note that the probability of $K[0] + K[1] = 126$ and 254 in WPA-TKIP is $\frac{2}{N}$ from Theorem 3.11, respectively. However, that in generic RC4 is $\frac{1}{N}$ because K is generated uniformly at random. In summary, we obtain

$$\begin{aligned}&\Pr(S_1[2] = -K[0] - K[1] + K[2] - 1)\\ &= \Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1})\\ &\quad + \Pr(S_1[2] = -K[0] - K[1] + K[2] - 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2})\\ &\approx \begin{cases}\frac{2}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\gamma) & \text{for RC4,}\\ \frac{4}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1-\gamma) & \text{for WPA-TKIP.}\end{cases}\end{aligned}$$

□

Before showing Theorem 5.12, we prove Lemma 5.3. Lemma 5.3 presents that an event

($S_0[2] = K[1] + K[2] + 3$) yields a positive bias in both generic RC4 and WPA-TKIP. In order to prove the following theorems, let us denote the result of Lemma 5.3 as $\eta = \Pr(S_0[2] = K[1] + K[2] + 3)$.

Lemma 5.3 ([IM17, Lemma 1])**.** *After the first round of the PRGA, we have*

$$\Pr(S_0[2] = K[1] + K[2] + 3) \approx \frac{3}{N}\left(1 - \frac{1}{N}\right)^{N-2} + \frac{1}{N}\left(1 - \frac{2}{N}\right)\left(1 - \frac{3}{N}\right) + \frac{3}{N^3}\left(1 - \frac{2}{N}\right).$$

Proof. The probability of the target event ($S_0[2] = K[1] + K[2] + 3$) can be decomposed into four paths: $j_1^K = 0$ (Path 1), $j_1^K = 1$ (Path 2), $j_1^K = 2$ (Path 3), and $j_1^K \neq 0, 1, 2$ (Path 4). Paths 1–3 are further divided into two subpaths: $j_2^K = 2$ (Paths 1-1, 2-1, and 3-1) and $j_2^K \neq 2$ (Paths 1-2, 2-2, and 3-2). These paths include all events in order to compute $\Pr(S_1[i_2] = -K[0] - K[1] + K[2] - 1)$. In the following proof, we assume that the values of index j^K are distributed with probability $\frac{1}{N}$ (random association).

Path 1-1. Because $K[0] = 0$, $S_1^K[1] = 1$, and $S_2^K[2] = 1$, $j_3^K = K[1] + K[2] + 2$ from Equation (5.6). Then, $S_3^K[0] = 0$, $S_3^K[1] = 2$, and $S_3^K[2] = K[1] + K[2] + 2$ from the 7th step in Algorithm 1. When $K[1] + K[2] + 3 = 0$ or 2, the target event ($S_0[2] = K[1] + K[2] + 3$) never occurs. On the other hand, when $K[1] + K[2] + 3 \neq 0$ and 2 are satisfied, we assume that the target event ($S_0[2] = K[1] + K[2] + 3$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 1-1}) \approx \frac{1}{N}\left(1 - \frac{2}{N}\right).$$

Similarly, we obtain the probability of the target event ($S_0[2] = K[1] + K[2] + 3$) under the conditions of Paths 2-1, 3-1, and 4.

Path 1-2. Because $K[0] = 0$, $S_1^K[1] = 1$, and $S_2^K[2] = 2$, $j_3^K = K[1] + K[2] + 3$ from Equation (5.6). Then, $S_3^K[2] = K[1] + K[2] + 2$ from the 7th step in Algorithm 1. After the third round of the KSA, $S_r^K[2] = S_3^K[2]$ for $4 \leq r \leq N$ when $j_r^K \neq 2$ during the remaining $N - 3$ rounds of the KSA, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-3}$. Therefore, we obtain

$$\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 1-2}) \approx \left(1 - \frac{1}{N}\right)^{N-3}.$$

Similarly, we obtain the probability of the event $S_0[2] = K[1] + K[2] + 3$ under the conditions of Paths 2-2 and 3-2.

In summary, we get

$$\begin{aligned}
&\Pr(S_0[2] = K[1] + K[2] + 3) \\
&\quad = \Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\
&\qquad + \Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 1-2}) \cdot \Pr(\text{Path 1-2})
\end{aligned}$$

$$
\begin{aligned}
&+\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 2-1}) \cdot \Pr(\text{Path 2-1})\\
&+\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 2-2}) \cdot \Pr(\text{Path 2-2})\\
&+\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 3-1}) \cdot \Pr(\text{Path 3-1})\\
&+\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 3-2}) \cdot \Pr(\text{Path 3-2})\\
&+\Pr(S_0[2] = K[1] + K[2] + 3 \mid \text{Path 4}) \cdot \Pr(\text{Path 4})\\
\approx\ & \frac{3}{N}\left(1-\frac{1}{N}\right)^{N-2} + \frac{1}{N}\left(1-\frac{2}{N}\right)\left(1-\frac{3}{N}\right) + \frac{3}{N^3}\left(1-\frac{2}{N}\right).
\end{aligned}
$$

□

Theorem 5.12 ([IM17, Theorem 6]). *After the first round of the PRGA, we have*

$$\Pr(S_1[i_2] = K[1] + K[2] + 3) \approx \eta\left(1-\frac{1}{N}\right) + \frac{1}{N^2}.$$

Proof. The probability of the target event $(S_1[i_2] = K[1] + K[2] + 3)$ can be decomposed into two paths: $j_1 = 2$ (Path 1) and $j_1 \neq 2$ (Path 2). These paths include all events in order to compute $\Pr(S_1[i_2] = K[1] + K[2] + 3)$. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ $(i_2 = 2)$ for simplicity.

Path 1. Because $S_1[2] = S_0[1]$ from the 5th step in Algorithm 2, the target event $(S_1[2] = K[1] + K[2] + 3)$ always occurs if and only if $S_0[1] = K[1] + K[2] + 3$. We then assume that $K[1]+K[2]+3 = 2$ $(j_1 = S_0[1])$ with probability $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 1}) \approx \frac{1}{N}.$$

Path 2. Because $S_1[2] = S_0[2]$ from the 5th step in Algorithm 2, the target event $(S_1[2] = K[1]+K[2]+3)$ always occurs if and only if $S_0[2] = K[1]+K[2]+3$. We then assume that both events $(j_1 \neq 2)$ and $(S_0[2] = K[1] + K[2] + 3)$ are mutually independent. Therefore, we obtain

$$\Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 2}) \approx \eta.$$

In summary, we obtain

$$
\begin{aligned}
\Pr(S_1[2] = K[1] + K[2] + 3) &= \Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 1}) \cdot \Pr(\text{Path 1})\\
&\quad + \Pr(S_1[2] = K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2})\\
&\approx \eta\left(1-\frac{1}{N}\right) + \frac{1}{N^2}.
\end{aligned}
$$

□

Theorem 5.13 ([IM17, Theorem 7]). *After the first round of the PRGA for $x \in \{-3, -1, 1\}$,* *we have*

$$\begin{aligned}&\Pr(S_1[i_2] = K[0] - K[1] + K[2] + x)\\ &\approx \begin{cases} \frac{2}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\gamma) & \textit{for RC4,}\\ \frac{4}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{4}{N}\right)(1-\gamma) & \textit{for WPA-TKIP.}\end{cases}\end{aligned}$$

Proof. We can prove Theorem 5.13 in the same way as Theorem 5.11. □

Theorem 5.14 ([IM17, Theorem 8])**.** *After the first round of the PRGA, we have*

$$\begin{aligned}&\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3)\\ &\approx \begin{cases} \frac{2}{N}\left(\gamma + \frac{1}{N}(1-\gamma)\right) + \frac{1}{N}\left(1 - \frac{2}{N}\right)(1-\gamma) & \textit{for RC4,}\\ \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{N-2} + \left(4 - \frac{1}{N}\right)(1-\gamma)\right) & \textit{for WPA-TKIP.}\end{cases}\end{aligned}$$

Proof. The probability of the target event $(S_1[i_2] = K[0] - K[1] + K[2] + 3)$ in generic RC4 is proved in the same way as Theorem 5.11. The probability of the target event $(S_1[i_2] = K[0] - K[1] + K[2] + 3)$ in WPA-TKIP can be decomposed into two paths: $K[0] = K[1]$ (Path 1) and $K[0] \neq K[1]$ (Path 2). Path 1 is further divided into 2 subpaths: $K[2] = 254$ (Path 1-1) and $K[2] \neq 254$ (Path 1-2). These paths include all events in order to compute $\Pr(S_1[i_2] = K[0] - K[1] + K[2] + 3)$. In the following proof, we use $S_1[2]$ instead of $S_1[i_2]$ $(i_2 = 2)$ for simplicity.

Path 1-1. $K[0] - K[1] + K[2] + 3 = 1$ and Equations (5.4), (5.5), and (5.7) always hold. Then, $S_3^K[2] = S_2^K[j_3^K] = S_2^K[j_2^K] = S_1^K[i_1] = S_1^K[1] = S_0^K[1] = 1$ $(= K[0] - K[1] + K[2] + 3)$ from Algorithm 1 because $j_3^K = j_2^K = K[0] + K[1] + 1$ (note that $K[2] = 254$). After the third round of the KSA, $S_1[2] = S_3^K[2]$ when the values of index j are not equal to 2 during the subsequent $N-2$ rounds, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-2}$. Therefore, we obtain

$$\Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-1}) \approx \left(1 - \frac{1}{N}\right)^{N-2}.$$

Path 1-2. Because $K[0] - K[1] + K[2] + 3 \neq K[0] + K[1] + K[2] + 3$ (note that $K[1] \neq 0, 128$ in WPA-TKIP from Theorem 3.11), the target event $(S_1[2] = K[0] - K[1] + K[2] + 3)$ never occurs when $S_1[2] = K[0] + K[1] + K[2] + 3$. When $S_1[2] \neq K[0] + K[1] + K[2] + 3$, we assume that the target event $(S_1[2] = K[0] - K[1] + K[2] + 3)$ occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-2}) \approx \frac{1}{N}(1-\gamma).$$

Similarly, we obtain the probability of the target event ($S_1[2] = K[0] - K[1] + K[2] + 3$) under the condition of Path 2.

Note that $\Pr(K[0] = K[1]) = \frac{1}{4}$ in WPA-TKIP from Theorem 3.11. Therefore, we obtain

$$\begin{aligned}
&\Pr(S_1[2] = K[0] - K[1] + K[2] + 3)_{\text{WPA}} \\
&\quad = \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-1}) \cdot \Pr(\text{Path 1-1}) \\
&\qquad + \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 1-2}) \cdot \Pr(\text{Path 1-2}) \\
&\qquad + \Pr(S_1[2] = K[0] - K[1] + K[2] + 3 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\
&\quad \approx \frac{1}{4N}\left(\left(1 - \frac{1}{N}\right)^{N-2} + \left(4 - \frac{1}{N}\right)(1 - \gamma)\right).
\end{aligned}$$

□

5.2.3 Key Correlations of $S_{255}[i_{256}]$

This subsection provides Theorems 5.15 and 5.16 and their proofs. Theorem 5.15 presents that an event ($S_{255}[i_{256}] = K[0]$) occurs with high probability in generic RC4 and WPA-TKIP. On the contrary, Theorem 5.16 presents that an event ($S_{255}[i_{256}] = K[1]$) occurs with high probability only in WPA-TKIP.

Theorem 5.15 ([IM16b, Theorem 7])**.** *After the* 255*-th round of the PRGA, we have*

$$\Pr(S_{255}[i_{256}] = K[0]) \approx \alpha_0\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1 - \alpha_0)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right).$$

Proof. The probability of the target event ($S_{255}[i_{256}] = K[0]$) can be decomposed into two paths: $S_0[0] = K[0]$ (Path 1) and $S_0[0] \neq K[0]$ (Path 2). In the following proof, we use $S_{255}[0]$ instead of $S_{255}[i_{256}]$ ($i_{256} = 0$) for simplicity.

Path 1. The target event ($S_{255}[0] = K[0]$) always occurs if and only if $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{255}$ because we assume that $j_r = 0$ for each round with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_{255}[0] = K[0] \mid \text{Path 1}) \approx \left(1 - \frac{1}{N}\right)^{255}.$$

Path 2. The target event ($S_{255}[0] = K[0]$) never occurs when $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$. Except when $S_r[0] = S_0[0]$ for $1 \leq r \leq 255$, whose probability is approximately $\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right)$, we assume that the target event ($S_{255}[0] = K[0]$) occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_{255}[0] = K[0] \mid \text{Path 2}) \approx \frac{1}{N}\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right).$$

In summary, we obtain

$$\begin{aligned}\Pr(S_{255}[0]=K[0]) &= \Pr(S_{255}[0]=K[0]\mid \text{Path 1})\cdot\Pr(\text{Path 1})\\ &\quad+\Pr(S_{255}[0]=K[0]\mid \text{Path 2})\cdot\Pr(\text{Path 2})\\ &\approx \alpha_0\Big(1-\frac{1}{N}\Big)^{255}+\frac{1}{N}(1-\alpha_0)\Big(1-\Big(1-\frac{1}{N}\Big)^{255}\Big),\end{aligned}$$

where $\alpha_0=\Pr(S_0[0]=K[0])\approx\big(1-\frac{1}{N}\big)^N+\frac{1}{N}$. □

Before showing Theorem 5.16, we prove Lemma 5.4 that an event $(S_0[0]=K[1])$ occurs with high probability only in WPA-TKIP.

Lemma 5.4 ([IM16b, Lemma 2]). *In the initial state of the PRGA, we have*

$$\Pr(S_0[0]=K[1])\approx\begin{cases}\dfrac{1}{N}-\dfrac{1}{N^2}\Big(1-\alpha_0\Big) & \textit{for RC4,}\\[2ex] \dfrac{1}{4}\Big(\dfrac{3}{N}+\Big(1-\dfrac{3}{N}\Big)\alpha_0\Big) & \textit{for WPA-TKIP.}\end{cases}$$

Proof. The probability of the target event $(S_0[0]=K[1])$ can be decomposed into two paths: $K[1]=K[0]$ (Path 1) and $K[1]\neq K[0]$ (Path 2).

Path 1. The target event $(S_0[0]=K[1])$ always occurs if and only if $S_0[0]=K[0]$. Therefore, we obtain

$$\Pr(S_0[0]=K[1]\mid \text{Path 1})=\alpha_0.$$

Path 2. The target event $(S_0[0]=K[1])$ never occurs when $S_0[0]=K[0]$. When $S_0[0]\neq K[0]$, we assume that the target event $(S_0[0]=K[1])$ occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_0[0]=K[1]\mid \text{Path 2})\approx\frac{1}{N}\cdot(1-\alpha_0).$$

In summary, we obtain

$$\begin{aligned}\Pr(S_0[0]=K[1]) &= \Pr(S_0[0]=K[1]\mid \text{Path 1})\cdot\Pr(\text{Path 1})\\ &\quad+\Pr(S_0[0]=K[1]\mid \text{Path 2})\cdot\Pr(\text{Path 2})\\ &\approx\begin{cases}\alpha_0\cdot\dfrac{1}{N}+\dfrac{1}{N}(1-\alpha_0)\cdot\Big(1-\dfrac{1}{N}\Big)=\dfrac{1}{N}-\dfrac{1}{N^2}\Big(1-\alpha_0\Big) & \text{for RC4,}\\[2ex] \alpha_0\cdot\dfrac{1}{4}+\dfrac{1}{N}(1-\alpha_0)\cdot\dfrac{3}{4}=\dfrac{1}{4}\Big(\dfrac{3}{N}+\Big(1-\dfrac{3}{N}\Big)\alpha_0\Big) & \text{for WPA-TKIP,}\end{cases}\end{aligned}$$

where $\alpha_0=\Pr(S_0[0]=K[0])\approx\big(1-\frac{1}{N}\big)^N+\frac{1}{N}$. □

Lemma 5.4 reflects that the probability of the event $(K[1] = K[0])$ in WPA-TKIP, $\frac{1}{4}$, is higher than that in generic RC4, $\frac{1}{N}$.

Theorem 5.16 ([IM16b, Theorem 8])**.** *After the* 255*-th round of the PRGA, we have*

$$\Pr(S_{255}[i_{256}] = K[1]) \approx \delta\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1-\delta)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right),$$

where δ is $\Pr(S_0[0] = K[1])$ given as Lemma 5.4.

Proof. The proof itself is similar to that of Theorem 5.15, and uses the probability of the event $(S_0[0] = K[1])$ given as Lemma 5.4 instead of the probability of the event $(S_0[0] = K[0])$. Therefore, we obtain

$$\begin{aligned}\Pr(S_{255}[0] = K[1]) &= \Pr(S_{255}[0] = K[1] \mid S_0[0] = K[1]) \cdot \Pr(S_0[0] = K[1]) \\ &\quad + \Pr(S_{255}[0] = K[1] \mid S_0[0] \neq K[1]) \cdot \Pr(S_0[0] \neq K[1]) \\ &\approx \delta\left(1 - \frac{1}{N}\right)^{255} + \frac{1}{N}(1-\delta)\left(1 - \left(1 - \frac{1}{N}\right)^{255}\right),\end{aligned}$$

where δ is $\Pr(S_0[0] = K[1])$ given as Lemma 5.4. □

5.2.4 Key Correlations of $S_r[i_{r+1}]$ for $0 \leq r \leq N$

This subsection provides Theorem 5.17 and its proof. Theorem 5.17 presents $\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ for $0 \leq r \leq N$, whose the experimental result is listed in Figure 5.1. Before showing the proof of Theorem 5.17, we prove Lemmas 5.5 and 5.6, which are distributions of the internal state in the first two rounds of the PRGA.

Lemma 5.5 ([IM16b, Lemma 3])**.** *In the initial state of the PRGA for $0 \leq x \leq N-1$, we have*

$$\Pr(S_0[x] = K[0] + K[1] + 1) \approx \begin{cases} \left(1 - \frac{1}{N}\right)^{N+2} + \frac{1}{N} & \text{when } x = 1, \\ \frac{1}{N^2}\left(1 - \frac{1}{N}\right)^{2} & \text{when } x = 0 \text{ for WPA-TKIP}, \\ \frac{1}{N}\left(1 - \frac{1}{N}\right)\left(\frac{1}{N}\left(1 - \frac{x+1}{N}\right) + \left(1 - \frac{1}{N}\right)^{N-x-2}\right) & \text{otherwise.} \end{cases}$$

Proof. When $x = 1$, the probability of the target event $(S_0[1] = K[0] + K[1] + 1)$ follows the result in Theorem 3.19. Therefore, we obtain

$$\Pr(S_0[1] = K[0] + K[1] + 1) \approx \left(1 - \frac{1}{N}\right)^{N+2} + \frac{1}{N}.$$

On the other hand, the probability of the target event $(S_0[x] = K[0] + K[1] + 1)$ for $x \in$

$[0, N]\backslash\{1\}$ can be decomposed into two paths: $S^K_x[j^K_{x+1}] = K[0] + K[1] + 1$ (Path 1) and $S^K_x[j^K_{x+1}] \neq K[0] + K[1] + 1$ (Path 2).

Path 1. From the 7th step in Algorithm 1, $S^K_{x+1}[x] = K[0] + K[1] + 1$ always holds because $S^K_{x+1}[x]$ must be swapped from $S^K_x[j^K_{x+1}]$. In addition, when $S^K_r[x] = S^K_{x+1}[x]$ for $x + 2 \leq r \leq N$, whose probability is approximately $\left(1 - \frac{1}{N}\right)^{N-x-1}$ because we assume that $j^K_r = x$ for each round with probability approximately $\frac{1}{N}$ (random association), the target event ($S_0[x] = K[0] + K[1] + 1$) always occurs. Therefore, we obtain

$$\Pr(S_0[x] = K[0] + K[1] + 1 \mid \text{Path 1}) \approx \left(1 - \frac{1}{N}\right)^{N-x-1}.$$

Path 2. Let y be satisfied by $S^K_x[y] = K[0]+K[1]+1$. In the same way as the discussion of Path 1, $S^K_{x+1}[x] \neq K[0]+K[1]+1$ always holds. After the $x+1$-th round, when $x \geq y$, the target event ($S_0[x] = K[0]+K[1]+1$) never occurs because $S^K_r[x] \neq K[0]+K[1]+1$ always holds for $x + 1 \leq r \leq N$ from Algorithm 1. On the contrary, when $x < y$, whose probability is $1-\frac{x+1}{N}$, we assume that the target event ($S_0[x] = K[0]+K[1]+1$) occurs with probability approximately $\frac{1}{N}$ (random association). In order to satisfy $x < y$, we must further consider $K[0] = 1$, whose probability is $\frac{1}{N}$. When $K[0] \neq 1$, $S^K_2[1] = K[0] + K[1] + 1$ always holds from the discussion in Theorem 5.1. Thus, the target event ($S_0[x] = K[0] + K[1] + 1$) never occurs because $S^K_r[x] \neq K[0]+K[1]+1$ always holds for $2 \leq r \leq N$ from Algorithm 1. Therefore, we obtain

$$\Pr(S_0[x] = K[0] + K[1] + 1 \mid \text{Path 2}) = \frac{1}{N^2}\left(1 - \frac{x+1}{N}\right).$$

We assume that the event ($S^K_x[j^K_{x+1}] = K[0] + K[1] + 1$) occurs with probability approximately $\frac{1}{N}$ (random association). In summary, we obtain

$$\begin{aligned}\Pr(S_0[x] = K[0] + K[1] + 1) &= \Pr(S_0[x] = K[0] + K[1] + 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \Pr(S_0[x] = K[0] + K[1] + 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \frac{1}{N}\left(1 - \frac{1}{N}\right)\left(\frac{1}{N}\left(1 - \frac{x+1}{N}\right) + \left(1 - \frac{1}{N}\right)^{N-x-2}\right).\end{aligned}$$

When $x = 0$ in WPA-TKIP, the target event ($S_0[0] = K[0] + K[1] + 1$) never occurs under the condition of $S^K_0[j^K_1] = K[0] + K[1] + 1$ (Path 1) because $S^K_0[j^K_1] = K[0]$ from the 6th step in Algorithm 1. In this case, $K[1] \neq 255$ always holds in WPA-TKIP. Thus, the target event ($S_0[0] = K[0] + K[1] + 1$) occurs only under the condition of Path 2, whose probability is given simply as $\frac{1}{N^2}\left(1 - \frac{1}{N}\right)^2$. □

Lemma 5.6 ([IM16b, Lemma 4]). *After the first round of the PRGA for* $0 \leq x \leq N - 1$, *we* *have*

$$\Pr(S_1[x] = K[0] + K[1] + 1) = \begin{cases} \beta_1 & \textit{when } x = 1, \\ \alpha_1\gamma_{x-1} + (1-\beta_1)\epsilon_x & \textit{otherwise,} \end{cases}$$

where ϵ_x *is* $\Pr(S_0[x] = K[0] + K[1] + 1)$ *given as Lemma 5.5.*

Proof. When $x = 1$, the probability of the target event $(S_1[1] = K[0] + K[1] + 1)$ follows the result in Theorem 3.20 because $S_1[1] = S_1[i_1] = S_0[j_1] = S_0[S_0[1]]$ from the 4th and the 5th steps in Algorithm 2. Therefore, we obtain

$$\Pr(S_1[1] = K[0] + K[1] + 1) = \beta_1.$$

On the other hand, the probability of the target event $(S_1[x] = K[0] + K[1] + 1)$ for $x \in [0, N-1]\backslash\{1\}$ can be decomposed into two paths: $S_0[1] = K[0] + K[1] + 1$ (Path 1) and $S_0[x] = K[0] + K[1] + 1$ (Path 2).

Path 1. From the 5th step in Algorithm 2, the target event $(S_1[x] = K[0] + K[1] + 1)$ always occurs if and only if $j_1 = x$ because $S_1[j_1]$ must be swapped from $S_0[i_1] = S_0[1]$. Although events $(S_0[1] = K[0] + K[1] + 1)$ and $(j_1 = x)$ are not mutually independent, events $(S_0[1] = K[0] + K[1] + 1)$ and $(K[0] + K[1] + 1 = x)$ become independent by converting $j_1 = x$ into $j_1 = S_0[1] = K[0] + K[1] + 1 = x$. Therefore, we obtain

$$\Pr(S_1[x] = K[0] + K[1] + 1 \mid \text{Path 1}) = \Pr(K[0] + K[1] = x - 1).$$

Path 2. In the same way as the discussion of Path 1, the target event $(S_1[x] = K[0]+K[1]+1)$ never occurs. When $j_1 \neq x$, $S_1[x] = S_0[x] = K[0] + K[1] + 1$ always holds, and $S_1[1] \neq K[0] + K[1] + 1$ because $S_1[1] = S_0[j_1] \neq S_0[x]$ from the 5th step in Algorithm 2. We assume that events $(S_0[x] = K[0] + K[1] + 1)$ and $S_1[1] \neq K[0] + K[1] + 1$ are mutually independent. Therefore, we obtain

$$\Pr(S_1[x] = K[0] + K[1] + 1 \mid \text{Path 2}) = \Pr(S_1[1] \neq K[0] + K[1] + 1).$$

In summary, we obtain

$$\begin{aligned}\Pr(S_1[x] = K[0] + K[1] + 1) = &\Pr(S_1[x] = K[0] + K[1] + 1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &+ \Pr(S_1[x] = K[0] + K[1] + 1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ = &\alpha_1\gamma_{x-1} + (1-\beta_1)\epsilon_x,\end{aligned}$$

where $\alpha_1 = \Pr(S_0[1] = K[0] + K[1] + 1)$, $\beta_1 = \Pr(S_0[S_0[1]] = K[0] + K[1] + 1)$, $\gamma_{x-1} = \Pr(K[0] + K[1] = x - 1)$, and $\epsilon_x = \Pr(S_0[x] = K[0] + K[1] + 1)$, which is given as Lemma 5.5. □

Theorem 5.17 ([IM16b, Theorem 9]). *After the r-th round of the PRGA for $0 \leq r \leq N$, we have*

$$\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$$
$$\approx \begin{cases} \alpha_1 & \text{when } r = 0, \\ \alpha_1\gamma_1 + (1-\beta_1)\epsilon_2 & \text{when } r = 1, \\ \epsilon_0\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\epsilon_0)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{when } r = N-1, \\ \zeta_1\left(1-\frac{1}{N}\right)^{N-1} + \frac{1}{N}(1-\zeta_1)\left(1-\left(1-\frac{1}{N}\right)^{N-1}\right) & \text{when } r = N, \\ \zeta_{r+1}\left(1-\frac{1}{N}\right)^{r-1} + \frac{1}{N}\sum_{x=1}^{r-1}\eta_x\left(1-\frac{1}{N}\right)^{r-x-1} & \text{otherwise,} \end{cases}$$

where $\epsilon_r = \Pr(S_0[r] = K[0] + K[1] + 1)$ is given as Lemma 5.5, $\zeta_r = \Pr(S_1[r] = K[0] + K[1] + 1)$ is given as Lemma 5.6, and $\eta_r = \Pr(S_r[i_{r+1}] = K[0] + K[1] + 1)$ is given as this theorem.

Proof. When $r = 0$ and 1, the probability of the target events $(S_0[i_1] = K[0] + K[1] + 1)$ and $(S_1[i_2] = K[0]+K[1]+1)$ follow the result in Lemmas 5.5 and 5.6, respectively. When $r = N-1$ and N, both the target events $(S_{N-1}[i_N] = K[0] + K[1] + 1)$ and $(S_N[i_{N+1}] = K[0] + K[1] + 1)$ can be proved in the same way as the proof of Theorem 5.15. In other cases, the probability of the target event $(S_r[i_{r+1}] = K[0] + K[1] + 1)$ for $2 \leq r \leq N-2$ can be decomposed in two paths: $S_1[i_{r+1}] = K[0] + K[1] + 1$ (Path 1) and $S_x[i_{x+1}] = K[0] + K[1] + 1$ for $1 \leq x \leq r-1$ (Path 2).

Path 1. The target event $(S_r[i_{r+1}] = K[0]+K[1]+1)$ always occurs when $S_y[i_{r+1}] = S_1[i_{r+1}]$ for $2 \leq y \leq r$, whose probability is approximately $\left(1-\frac{1}{N}\right)^{r-1}$ because we assume that $j_y = i_{r+1}$ for each round with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 1}) \approx \left(1 - \frac{1}{N}\right)^{r-1}.$$

Path 2. From the 5th step in Algorithm 2, the event $(S_{x+1}[i_{r+1}] = K[0]+K[1]+1)$ always occurs if and only if $j_{x+1} = i_{r+1}$ because $S_{x+1}[j_{x+1}] = S_{x+1}[i_{r+1}]$ must be swapped from $S_x[i_{x+1}]$. After the $x+1$-th round, the target event $(S_r[i_{r+1}] = K[0]+K[1]+1)$ occurs when $S_y[i_{r+1}] = S_{x+1}[i_{r+1}]$ for $x+2 \leq y \leq r$, whose probability is approximately $\left(1-\frac{1}{N}\right)^{r-x-1}$ because we assume that $j_y = i_{r+1}$ for each round with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(S_r[i_{r+1}] = K[0] + K[1] + 1 \mid \text{Path 2}) \approx \frac{1}{N}\left(1 - \frac{1}{N}\right)^{r-x-1}.$$

Note that the range of x varies depending on the value of r in Path 2. In summary, we obtain

$$\begin{aligned}\Pr(S_r[i_{r+1}] = K[0]+K[1]+1) &= \Pr(S_r[i_{r+1}] = K[0]+K[1]+1 \mid \text{Path 1}) \cdot \Pr(\text{Path 1}) \\ &\quad + \sum_{x=1}^{r-1} \Pr(S_r[i_{r+1}] = K[0]+K[1]+1 \mid \text{Path 2}) \cdot \Pr(\text{Path 2}) \\ &\approx \zeta_{r+1}\left(1-\frac{1}{N}\right)^{r-1} + \frac{1}{N}\sum_{x=1}^{r-1}\eta_x\left(1-\frac{1}{N}\right)^{r-x-1},\end{aligned}$$

where $\zeta_r = \Pr(S_1[r] = K[0]+K[1]+1)$ and $\eta_r = \Pr(S_r[i_{r+1}] = K[0]+K[1]+1)$, which is recursive probability in this theorem. □

5.2.5 Key Correlations of j_2

This subsection provides Theorems 5.18–5.22 and their proofs. Theorem 5.18 presents that an event $(j_2 = K[2])$ yields a positive bias in both generic RC4 and WPA-TKIP. On the contrary, Theorems 5.19–5.22 present that seven events on j_2 yield positive biases only in WPA-TKIP but not biases in generic RC4. Now, we present only the proof of Theorem 5.18 because Theorems 5.19–5.22 are proved in the same way as Theorem 5.18. In order to prove the following theorems, let us denote the result of Theorem 5.10 as $\gamma = \Pr(S_1[2] = K[0]+K[1]+K[2]+3)$.

Theorem 5.18 ([IM17, Theorem 9])**.** *After the second round of the PRGA, we have*

$$\Pr(j_2 = K[2]) \approx \begin{cases} \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \textit{for RC4,} \\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \textit{for WPA-TKIP.}\end{cases}$$

Proof. The probability of the target event $(j_2 = K[2])$ can be decomposed into two paths: $K[0]+K[1] = 126, 254$ (Path 1) and $K[0]+K[1] \neq 126, 254$ (Path 2). These paths include all events in order to compute $\Pr(j_2 = K[2])$. Note that $j_2 = S_0[1] + S_1[2]$ from the 4th step in Algorithm 2.

Path 1. Assuming that events $(S_0[1] = K[0]+K[1]+1)$ and $(S_1[2] = K[0]+K[1]+K[2]+3)$ occur simultaneously, and we obtain

$$\begin{aligned} j_2 &= S_0[1] + S_1[2] \\ &= (K[0]+K[1]+1) + (K[0]+K[1]+K[2]+3) \\ &= 2K[0]+2K[1]+K[2]+4.\end{aligned}$$

When the above condition is satisfied, the target event $(j_2 = K[2])$ always occurs because $K[2] = 2K[0]+2K[1]+K[2]+4$. On the other hand, when the above condition is not satisfied, we assume that the target event $(j_2 = K[2])$ occurs with probability $\frac{1}{N}$ (random association). We also assume that events $(S_0[1] = K[0]+K[1]+1)$ and $(S_1[2] =$

$K[0]+K[1]+K[2]+3)$ are mutually independent. Therefore, we obtain

$$\Pr(j_2 = K[2] \mid \text{path } 1) \approx \alpha_1\gamma + \frac{1}{N}(1-\alpha_1\gamma).$$

Path 2. Because $K[2] \neq 2K[0]+2K[1]+K[2]+4$, the target event $(j_2 = K[2])$ never occurs when events $(S_0[1] = K[0]+K[1]+1)$ and $(S_1[2] = K[0]+K[1]+K[2]+3)$ occur simultaneously. When either $S_0[1] \neq K[0]+K[1]+1$ or $S_1[2] \neq K[0]+K[1]+K[2]+3$, we assume that the target event $(j_2 = K[2])$ occurs with probability approximately $\frac{1}{N}$ (random association). Therefore, we obtain

$$\Pr(j_2 = K[2] \mid \text{Path } 2) \approx \frac{1}{N}(1-\alpha_1\gamma).$$

Note that the probability of $K[0]+K[1] = 126$ and 254 in WPA-TKIP is $\frac{2}{N}$ from Theorem 3.11, respectively. On the other hand, that in generic RC4 is $\frac{1}{N}$ because K is generated uniformly at random. In summary, we obtain

$$\begin{aligned}\Pr(j_2 = K[2]) &= \Pr(j_2 = K[2] \mid \text{Path } 1)\cdot\Pr(\text{Path } 1)\\ &\quad + \Pr(j_2 = K[2] \mid \text{Path } 2)\cdot\Pr(\text{Path } 2)\\ &\approx \begin{cases} \frac{2}{N}\left(\alpha_1\gamma + \frac{1}{N}(1-\alpha_1\gamma)\right) + \frac{1}{N}\left(1-\frac{2}{N}\right)(1-\alpha_1\gamma) & \text{for RC4,}\\ \frac{4}{N}\left(\alpha_1\gamma + \frac{1}{N}(1-\alpha_1\gamma)\right) + \frac{1}{N}\left(1-\frac{4}{N}\right)(1-\alpha_1\gamma) & \text{for WPA-TKIP,}\end{cases}\\ &= \begin{cases} \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \text{for RC4,}\\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \text{for WPA-TKIP.}\end{cases}\end{aligned}$$

□

Theorem 5.19 ([IM17, Theorem 10])**.** *After the second round of the PRGA for $x \in \{-2, 0, 2\}$, we have*

$$\Pr(j_2 = -K[0]-K[1]+K[2]+x) \approx \begin{cases} \frac{1}{N} & \textit{for RC4,}\\ \frac{1}{N} + \frac{1}{N}\alpha_1\gamma & \textit{when } x = \pm 2 \textit{ for WPA-TKIP,}\\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \textit{when } x = 0 \textit{ for WPA-TKIP.}\end{cases}$$

Theorem 5.20 ([IM17, Theorem 11])**.** *After the second round of the PRGA, we have*

$$\Pr(j_2 = -K[0]+K[1]+K[2]) \approx \begin{cases} \frac{1}{N} & \textit{for RC4,}\\ \frac{1}{N} + \frac{3}{N}\alpha_1\gamma & \textit{for WPA-TKIP.}\end{cases}$$

Theorem 5.21 ([IM17, Theorem 12]). *After the second round of the PRGA for $x \in \{-2, 3\}$, we have*

$$\Pr(j_2 = -K[1] + K[2] + x) \approx \begin{cases} \dfrac{1}{N} & \textit{for RC4,} \\ \dfrac{1}{N} + \dfrac{3}{N}\alpha_1\gamma & \textit{for WPA-TKIP.} \end{cases}$$

Theorem 5.22 ([IM17, Theorem 13]). *After the second round of the PRGA, we have*

$$\Pr(j_2 = K[0] - K[1] + K[2]) \approx \begin{cases} \dfrac{1}{N} & \textit{for RC4,} \\ \dfrac{1}{N} + \dfrac{3}{N}\alpha_1\gamma & \textit{for WPA-TKIP.} \end{cases}$$

5.3 Experimental Evaluations

We have performed experiments to check the accuracy of the theoretical values in all theorems. Our experiments used N^5 samples generated from randomly chosen keys in generic RC4 and WPA-TKIP. Because each of the target events in all theorems has a relative bias with a probability of at least $\mathcal{O}(\frac{1}{N})$, the number of samples to distinguish each of the target events from random distribution is at least $\mathcal{O}(N^3)$ according to Theorem 3.2.

We have evaluated the percentage of the relative error ϵ_{max} of the experimental values compared with the theoretical values (see Section 2.5.3). Tables 5.4 and 5.5 show comparison between the experimental and theoretical values, and the percentage of the relative error ϵ_{max} in both generic RC4 and WPA-TKIP, respectively.

We can see from Table 5.4 that ϵ_{max} is small enough in each case in generic RC4, such as $\epsilon_{max} \leq 0.735$ (%). Therefore, we have checked the accuracy of the theoretical values in generic RC4.

We can see from Table 5.5 that ϵ_{max} is small enough in each case of $S_0[i_1]$ and $S_1[i_2]$ in WPA-TKIP, such as $\epsilon_{max} \leq 1.013$ (%). Therefore, we have checked the accuracy of the theoretical values of $S_0[i_1]$ and $S_1[i_2]$ in WPA-TKIP. However, the theoretical values of j_2 in WPA-TKIP produce slightly big error ϵ_{max}, such as 3.178 (%). We will continue to refine the theoretical values in j_2 in WPA-TKIP.

Figures 5.7 and 5.8 show comparison between the experimental and theoretical values in Theorem 5.17 for generic RC4 and WPA-TKIP, and the percentage of the relative error ϵ_{max}, respectively. From the figures, these distributions almost match overall, but differences between the experimental and theoretical values are considerable, such as $\epsilon_{max} \leq 64.028$ (%). Let us investigate why such differences are induced in generic RC4 and WPA-TKIP. As far as we have checked experimentally, it has made clear that there exist big differences between the experimental and theoretical result in Lemma 5.6. Therefore, we will refine the proof of Lemma 5.6 precisely, which remains an open problem.

Table 5.4: Comparison between experimental and theoretical values in generic RC4.

Key correlation		Experimental value	Theoretical value	ϵ_{max} (%)
$S_0[i_1]$	$K[0]$	0.001449605	0.001445489	0.289
	$K[0]-K[1]-3$	0.005332558	0.005325263	0.139
	$K[0]-K[1]-1$	0.003922530	0.003909411	0.337
	$-K[0]-K[1]-3$	0.005333309	0.005344544	0.213
	$K[0]+K[1]+K[2]+3$	0.001490745	0.001479853	0.735
$S_1[i_2]$	$K[0]+K[1]+K[2]+3$	0.360360690	0.362016405	0.460
	$-K[0]-K[1]+K[2]-1$	0.005305673	0.005320377	0.280
	$K[1]+K[2]+3$	0.008158548	0.008150313	0.103
	$K[0]-K[1]+K[2]-3$	0.005295155	0.005320377	0.479
	$K[0]-K[1]+K[2]-1$	0.005289180	0.005320377	0.592
	$K[0]-K[1]+K[2]+1$	0.005309594	0.005320377	0.206
	$K[0]-K[1]+K[2]+3$	0.005310594	0.005302926	0.147
$S_{255}[i_{256}]$	$K[0]$	0.138038917	0.138325988	0.208
	$K[1]$	0.003909105	0.003893102	0.412
$S_r[i_{r+1}]$	$K[0]+K[1]+1$	Figures 5.7 and 5.8		
j_2	$-K[0]-K[1]+K[2]-2$	0.003920799	0.003906250	0.374
	$-K[0]-K[1]+K[2]$	0.003919381	0.003906250	0.338
	$-K[0]-K[1]+K[2]+2$	0.003910929	0.003906250	0.123
	$-K[0]+K[1]+K[2]$	0.003920399	0.003906250	0.364
	$-K[1]+K[2]-2$	0.003910053	0.003906250	0.100
	$-K[1]+K[2]+3$	0.003897939	0.003906250	0.216
	$K[2]$	0.004430372	0.004426926	0.080
	$K[0]-K[1]+K[2]$	0.003917895	0.003906250	0.300

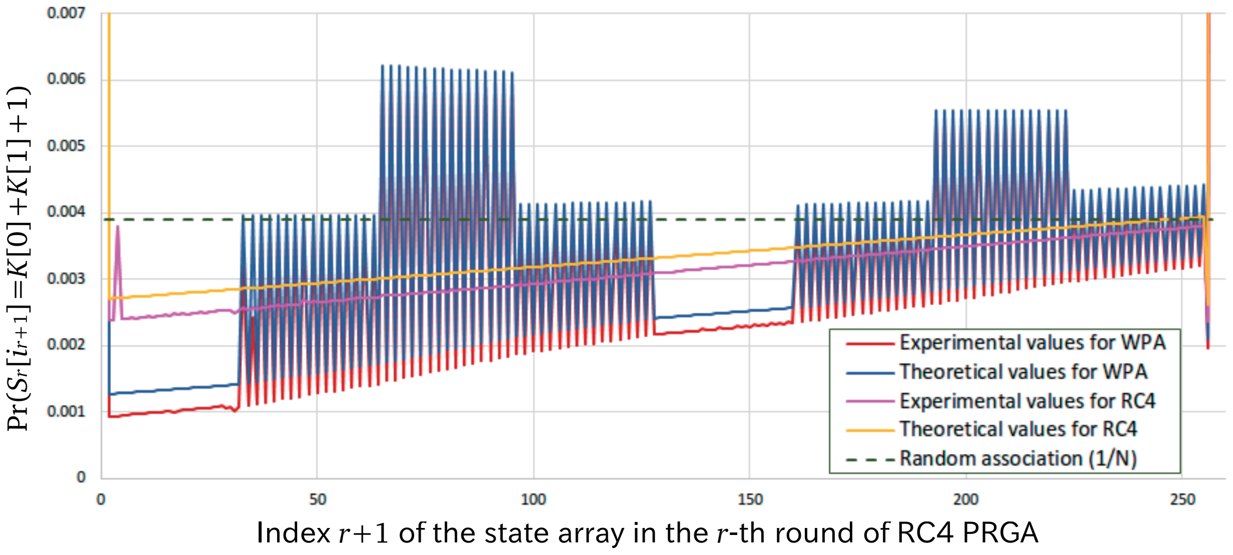

Figure 5.7: Comparison between experimental and theoretical values in Theorem 5.17.

Table 5.5: Comparison between experimental and theoretical values in WPA-TKIP.

Key correlation		Experimental value	Theoretical value	ϵ_{max} (%)
$S_0[i_1]$	$K[0]$	0	0	–
	$K[0]-K[1]-3$	0.007823541	0.007788309	0.452
	$K[0]-K[1]-1$	0.007851853	0.007772441	1.013
	$-K[0]-K[1]-3$	0.008408305	0.008375244	0.395
	$K[0]+K[1]+K[2]+3$	0.001491090	0.001479853	0.758
$S_1[i_2]$	$K[0]+K[1]+K[2]+3$	0.361751935	0.362723221	0.269
	$-K[0]-K[1]+K[2]-1$	0.008174625	0.008148630	0.320
	$K[1]+K[2]+3$	0.008173397	0.008150313	0.284
	$K[0]-K[1]+K[2]-3$	0.008140906	0.008148630	0.097
	$K[0]-K[1]+K[2]-1$	0.008147205	0.008148630	0.020
	$K[0]-K[1]+K[2]+1$	0.008150390	0.008148630	0.024
	$K[0]-K[1]+K[2]+3$	0.002835497	0.002849060	0.482
$S_{255}[i_{256}]$	$K[0]$	0.138038917	0.138325988	0.208
	$K[1]$	0.037186225	0.037105932	0.217
$S_r[i_{r+1}]$	$K[0]+K[1]+1$	Figures 5.7 and 5.8		
j_2	$-K[0]-K[1]+K[2]-2$	0.004573276	0.004427953	3.180
	$-K[0]-K[1]+K[2]$	0.005562336	0.005471358	1.638
	$-K[0]-K[1]+K[2]+2$	0.004543826	0.004427953	2.553
	$-K[0]+K[1]+K[2]$	0.005490766	0.005471358	0.356
	$-K[1]+K[2]-2$	0.005468425	0.005471358	0.056
	$-K[1]+K[2]+3$	0.005468472	0.005471358	0.055
	$K[2]$	0.005560613	0.005471358	1.608
	$K[0]-K[1]+K[2]$	0.005607004	0.005471358	2.422

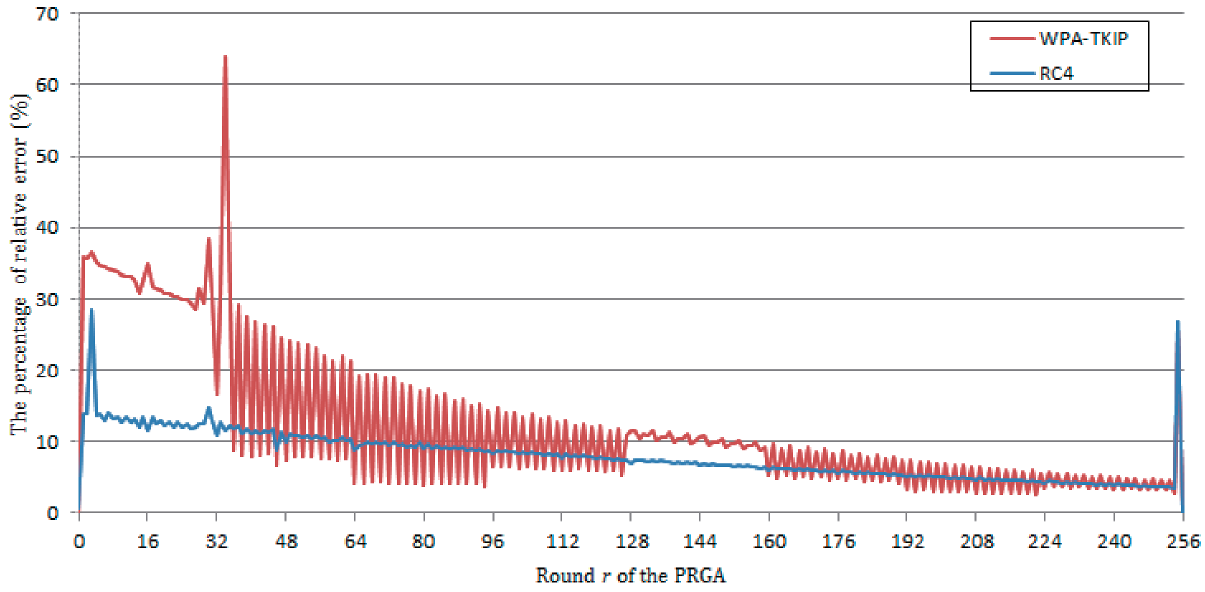

Figure 5.8: Percentage of relative error ϵ_{max} between experimental and theoretical values in Theorem 5.17.

5.4 Toward Secure RC4 Key Setting in WPA-TKIP

Many key recovery attacks on WEP have been proposed in [FMS01, VV07, Kle08, TWP08, TAO+10, SSVV13] over the past two decades. One of the greatest factors to enable the attacks is that the first three bytes of the RC4 key $\{K[0], K[1], K[2]\}$ in WEP are derived from the known IV. Actually, IV can be obtained easily by observing packets in wireless networks. For example, Fluhrer et al. pointed out in [FMS01] that the remaining RC4 key bytes $\{K[3], K[4], \ldots, K[15]\}$ are derived from the keystream bytes when specific IVs are used, and demonstrated how to recover the RC4 key by observing approximately $4,000,000$–$6,000,000$ packets (refer to Section 3.3.3 for details).

WPA-TKIP improved the RC4 key setting to avoid the FMS attack in [FMS01]. However, weaknesses in WPA-TKIP using the known IV have been also reported over past five years. For example, Sen Gupta et al. presented key correlations of the keystream bytes Z_r in [GMM+14], Paterson et al. presented IV-dependent biases in [PPS14], and we presented key correlations of the internal state variables $\{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$ in this chapter. Ideally, WPA-TKIP should be constructed in such a way that it can retain the security level of generic RC4.

This section investigated secure RC4 key setting in WPA-TKIP in such a way that it can retain the security level of generic RC4. If the RC4 key setting is refined, it can be difficult to induce IV-dependent biases and key correlations including the keystream bytes Z_r or the internal state variables $\{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$. In order to investigate secure RC4 key setting in WPA-TKIP, we use the following linear forms

$$Z_{r+1} = b \cdot K[x] + c \cdot K[y] + d \cdot K[z] + e, \tag{5.8}$$

$$X_r = a \cdot Z_{r+1} + b \cdot K[x] + c \cdot K[y] + d \cdot K[z] + e, \tag{5.9}$$

where $X_r \in \{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$, $a, b, c, d \in \{0, \pm 1\}$, $e \in \{0, \pm 1, \pm 2, \pm 3\}$, and $x, y, z \in \{0, 1, 2, \ldots, 15\}$ for $r \geq 0$. Thus, we need to carefully set arbitrary three bytes of the RC4 key $\{K[x], K[y], K[z]\}$ (instead of $\{K[0], K[1], K[2]\}$ in the original setting) derived from the known IV as follows:

$$K[x] = (\texttt{IV16} \gg 8)\ \&\ \texttt{0xFF}, \tag{5.10}$$

$$K[y] = ((\texttt{IV16} \gg 8)\ |\ \texttt{0x20})\ \&\ \texttt{0x7F}, \tag{5.11}$$

$$K[z] = \texttt{IV16}\ \&\ \texttt{0xFF}. \tag{5.12}$$

We have performed experiments in order to examine all the equations defined by Equations (5.8) and (5.9) in the first 256 rounds with 2^{32} randomly chosen 16-byte RC4 keys in the setting with 240 cases of $\{x, y, z\}$ defined by Equations (5.10)–(5.12).

Table B.1 in Appendix B shows the number of key correlations induced by both the original setting in WPA-TKIP and our proposed setting. We summarize the list of key correlations including the keystream bytes Z_r or unknown internal state variables X_r with more than 0.00395 or 0.0048 as positive biases and less than 0.00385 or 0.0020 as negative biases, respectively. From the table, we can confirm that the number of key correlations induced by the refined RC4 key setting, e.g., $(x, y, z) = (9, 10, 11)$, can be reduced by approximately 70% in comparison with that in the original setting. Therefore, we have refined the RC4 key setting in WPA-TKIP.

5.5 Chapter Conclusion

This chapter has precisely investigated key correlations of the unknown internal state variables in both generic RC4 and WPA-TKIP. Actually, key correlations of the internal state variables could be effective for the state recovery attacks on WPA-TKIP because the correlations include the known (IV-related) RC4 key bytes in WPA-TKIP. From our investigations, we have found hundreds of correlations with positive or negative biases. Then, we have proved significant key correlations theoretically, which are correlations of $S_0[i_1]$, $S_1[i_2]$, $S_{255}[i_{256}]$, $S_r[i_{r+1}]$ for $0 \leq r \leq N$, and j_2. Particularly, we emphasize that the probability of the event $(S_0[i_1] = K[0])$ in WPA-TKIP is 0 (see Theorem 5.2). Thus, the value of $S_0[i_1]$ is varied from 0 to 255, except for $K[0]$. As a result, our theoretical proofs have clarified how TKIP induces biases of the internal state in generic RC4. We have further provided the secure RC4 key setting in WPA-TKIP. Our proposed setting has reduced the number of key correlations by approximately 70% in comparison with the original setting. We believe that our proposed setting will be adopted in WPA-TKIP in the future.

Chapter 6

Iterated RC4 Key Correlations of the Keystream Bytes

In [SVV10], Sepehrdad et al. investigated key correlations of the keystream bytes experimentally. Their investigations are limited to ℓ rounds. Thus, no correlations between $K[r \bmod \ell]$ and Z_r for $r \geq \ell$ have been investigated, although $K[r \bmod \ell]$ may be iterated to use to produce Z_r for $r \geq \ell$.

This chapter focuses on key correlations of the keystream bytes, and investigates them in detail. We first discuss new key correlations that events $(Z_r = K[0] - K[r \bmod \ell] - r)$ for arbitrary round r induce positive biases, where $(K[0], K[r \bmod \ell])$ pairs in our key correlations are *iterated* every ℓ rounds. Therefore, we hereinafter refer to the newly observed key correlations as the *iterated RC4 key correlations*.

By combining our key correlations with the existing ones, e.g., $Z_1 = K[0] - K[1] - 1$ and $Z_{x \cdot \ell} = -x \cdot \ell$ $(x = 1, 2, \ldots, 7)$, we can integrate the iterated RC4 key correlations completely. Our contributions can be summarized as follows:

- Theorem 6.1 presents that events $(Z_r = K[0] - K[r \bmod \ell] - r)$ induce positive biases in both generic RC4 and WPA-TKIP, except when $r = 1, 2, x \cdot \ell$ $(x = 1, 2, \ldots, 7)$.
- Theorem 6.2 presents that an event $(Z_1 = K[0] - K[1] - 1)$ induces an negative bias in only WPA-TKIP.
- Theorem 6.3 presents that an event $(Z_2 = K[0] - K[2] - 2)$ does not induce a bias in both generic RC4 and WPA-TKIP.

We further discuss how to apply key correlations of the keystream bytes to the plaintext recovery attack on WPA-TKIP as the following three approaches:

- Section 6.4.1 discusses how to extend the IOWM attack in [IOWM13] (see Section 3.2.1), particularly on WPA-TKIP, using our iterated RC4 key correlations. In [GMM$^+$14], Sen Gupta et al. extended the IOWM attack, called the SMMPS attack (see Section 3.2.2), and achieved significant improvement for recovering four bytes of a plaintext $\{P_1, P_3, P_{256}, P_{257}\}$ on WPA-TKIP. Their improvement can be achieved by using key correlations of the keystream bytes based on the first three bytes of the RC4 key $\{K[0], K[1], K[2]\}$, which are known values in WPA-TKIP. In the same way as the SMMPS attack, we extend the IOWM attack, and achieve significant improvement for recovering eight bytes of a plaintext on WPA-TKIP using our iterated RC4 key correlations. In fact, the number of samples for recovering P_{17}, P_{18}, P_{33}, P_{34}, P_{49}, P_{50}, P_{66}, and P_{82} on WPA-TKIP can be reduced to $2^{17.727}/2^{23.178}$, $2^{17.800}/2^{23.210}$, $2^{18.955}/2^{23.770}$, $2^{19.035}/2^{23.791}$, $2^{20.297}/2^{24.114}$, $2^{20.386}/2^{24.135}$, $2^{21.869}/2^{24.479}$, and $2^{23.505}/2^{24.820}$, respectively.

- Section 6.4.2 discusses how to extend the ABPPS attack in [ABP+13] (see Section 3.2.1), particularly on WPA-TKIP using key correlations of the keystream bytes. Specifically, our proposed algorithm considers key correlations of the keystream bytes instead of all possible short-term biases only for round $r \in \{1, 3, 17, 18, 33, 34, 49, 50, 66, 82, 256, 257\}$. By comparing our proposed algorithm with the existing attack algorithms in [IOWM13, ABP+13, PPS14], we experimentally clarify which algorithm can effectively recover P_1, P_3, P_{17}, P_{18}, P_{33}, P_{34}, P_{49}, P_{50}, P_{66}, P_{82}, P_{256}, and P_{257} on WPA-TKIP. As a result, we achieve significant improvement for recovering five bytes of a plaintext on WPA-TKIP using our proposed algorithm. In fact, the number of samples for recovering P_3, P_{18}, P_{34}, P_{50}, and P_{66} on WPA-TKIP can be reduced to $2^{20}/2^{27}$, $2^{24}/2^{28}$, $2^{25}/2^{26}$, $2^{26}/2^{28}$, and $2^{28}/2^{29}$, respectively.
- Section 6.4.3 discusses how to optimize the plaintext recovery of the first 257 bytes on WPA-TKIP. By combining our proposed attack in Section 6.4.2 with the existing attacks (the IOWM attack, the ABPPS attack, the SMMPS attack, and the PPS attack), we experimentally clarify whether the plaintext recovery of the first 257 bytes on WPA-TKIP can be optimized or not. As a result, we achieve to recover the first 257 bytes of a plaintext on WPA-TKIP from approximately 2^{30} ciphertexts with a success probability of approximately 90.8%, whose probability is approximately 6.0% higher than the success probability of the PPS attack.

Our results imply that WPA-TKIP further lowers the security level of generic RC4.

The remainder of this chapter is organized as follows: Section 6.1 discusses the iterated RC4 key correlations observed by our experiments. Section 6.2 presents the theoretical proofs of new iterated RC4 key correlations. Section 6.3 demonstrates the experimental simulations in order to confirm the accuracy of the theoretical proofs. Section 6.4 discusses how to apply key correlations of the keystream bytes to the plaintext recovery attack on WPA-TKIP. Section 6.5 concludes this chapter.

6.1 Experimental Observations

This section presents our experimental observations of new key correlations of the keystream bytes in both generic RC4 and WPA-TKIP. In [SVV10], Sepehrdad et al. investigated key correlations of the keystream bytes Z_r by using a linear form

$$(a_0 \cdot K[0] + \cdots + a_{\ell-1} \cdot K[\ell-1] + a_\ell \cdot Z_1 + \cdots + a_{2\ell-1} \cdot Z_\ell) \bmod N = b, \tag{6.1}$$

where $a_i \in \{-1, 0, 1\}$ for $0 \le i \le 2\ell - 1$. However, they did not investigate key correlations of the keystream bytes over ℓ rounds.

We also focus on key correlations of the keystream bytes $\{Z_1, Z_3, Z_4\}$ proved by Sarkar in [Sar14], and predict that there might exist correlations between $(K[0], K[r \bmod \ell])$ pairs and Z_r. Then, we performed experiments for investigating correlations based on $(K[0], K[r \bmod \ell])$ pairs with 256 bytes of the keystream generated from N^4 randomly chosen keys.

Figures 6.1 and 6.2 show our experimental observations in generic RC4 and WPA-TKIP, respectively. From our experimental observations, we have observed new key correlations of the keystream bytes as follows:

Observation 6.1. *For any arbitrary secret key K, the following key correlations of the keystream*

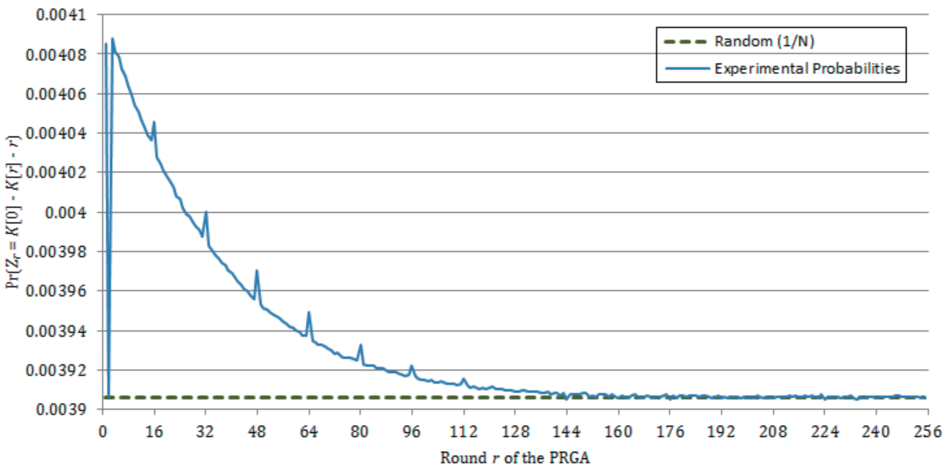

Figure 6.1: Observations of the iterated RC4 key correlations in generic RC4.

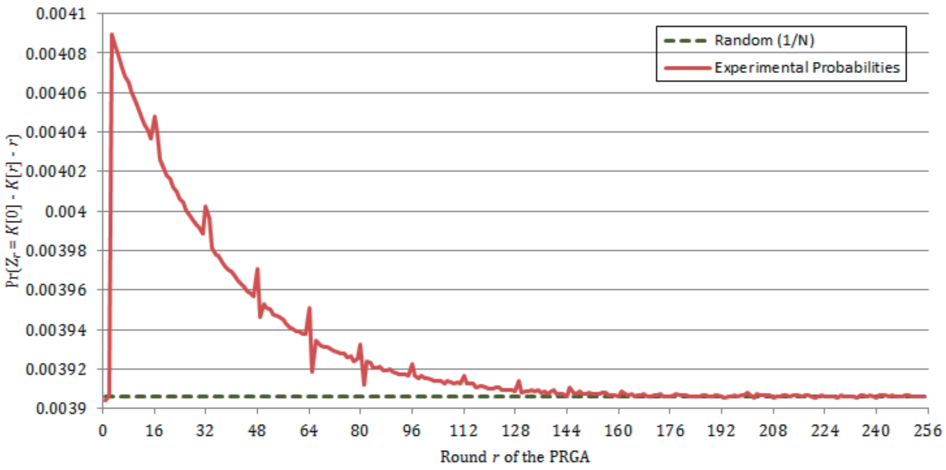

Figure 6.2: Observations of the iterated RC4 key correlations in WPA-TKIP.

bytes Z_r in both generic RC4 and WPA-TKIP induce biases:

$$Z_r = K[0] - K[r \bmod \ell] - r.$$

Predictably, we demonstrate that there exist key correlations between $(K[0], K[r \bmod \ell])$ pairs and Z_r. $(K[0], K[r \bmod \ell])$ pairs are *iterated* every ℓ rounds. Therefore, we refer to our newly observed key correlations as *iterated RC4 key correlations.* By combining our key correlations with the existing ones, we can integrate the iterated RC4 key correlations completely. Our motivation is to prove the iterated RC4 key correlations theoretically.

6.2 New Results

This section provides Theorems 6.1–6.3 and their proofs, which are theoretical proofs of Observation 6.1. Theorem 6.1 presents that events $(Z_r = K[0]-K[r \bmod \ell]-r)$ induce positive biases in both generic RC4 and WPA-TKIP, except when $r = 1, 2, x \cdot \ell$ $(x = 1, 2, \ldots, 7)$. Note that Theorem 6.1 includes the precise proofs of Propositions 3.1 and 3.2. Theorem 6.2 presents that an event $(Z_1 = K[0]-K[1]-1)$ induces a negative bias in only WPA-TKIP, and a positive bias in generic RC4 as Theorem 3.21. Theorem 6.3 presents that an event $(Z_2 = K[0]-K[2]-2)$ does not induce a bias in both generic RC4 and WPA-TKIP. As a result, by combining Theorems 6.1–6.3 with Theorems 3.21 and 3.10, Observation 6.1 can be proven completely.

The proof of Theorem 6.1 uses Lemma 3.1, which is denoted by $\zeta_{u,v} = \Pr(S_0[u] = v)$. Lemma 3.1 presents that the initial state S_0 generated from the KSA is non-randomness [Man01].

In our proofs, we often assume that the certain event occurs with probability approximately $\frac{1}{N}$, which is called the probability of *random association.* This is because it is difficult to demonstrate all events in the state transition of RC4, and it is a natural assumption based on the pseudorandomness of stream ciphers. The correctness of this assumption can be confirmed by experimental evaluations in Section 6.3. If this assumption is correct, the relative error between the experimental and theoretical value in each theorem will be small enough, and vice versa. Owing to this assumption, we often use the symbol of the approximate equation "≈" throughout this section.

Theorem 6.1 ([IM18a, Theorem 7])**.** *For any arbitrary secret key K and round r, except when $r = 1, 2, x \cdot \ell$ $(x = 1, 2, \ldots, 7)$, key correlations of the keystream bytes Z_r in both generic RC4 and WPA-TKIP are given by*

$$\Pr(Z_r = K[0] - K[r \bmod \ell] - r) \approx \alpha_r + \frac{1}{N}(1 - \alpha_r),$$

where α_r, β_r, γ_r, and δ_r are given by

$$\alpha_r \approx \left(\beta_r + \frac{1}{N(N-1)}(1 - \beta_r)\right) \cdot \gamma_r \cdot \left(\delta_r + \frac{1}{N}(1 - \delta_r)\right),$$

$$\begin{aligned}
\beta_r &\approx \frac{1}{N} \cdot \frac{N-r-1}{N} \cdot \frac{\prod_{x=3}^{r}(N-x-1)}{\prod_{x=0}^{r-3}(N-x)}, \\
\gamma_r &\approx \left(1-\frac{1}{N}\right)^{N-r-1} \cdot \frac{1}{N} \cdot \sum_{x=r+1}^{N-1} \left(1-\frac{1}{N}\right)^{x} \cdot \left(1-\frac{1}{N}\right)^{x-r-1} \cdot \left(1-\frac{2}{N}\right)^{N-x-1}, \\
\delta_r &\approx \left(1-\sum_{v=2}^{r} \zeta_{1,v} - \sum_{x=r+1}^{N-1} \frac{\zeta_{1,x}}{N-r-2}\right) \cdot \frac{N-r+1}{N-1}.
\end{aligned}$$

Proof. We consider the following three phases to prove the major path for the target event. In the following proof, $f_i = \frac{i(i+1)}{2} + \sum_{x=0}^{i} K[x \bmod \ell]$ for $i \geq 0$.

Phase 1. From the initial to the $(r+1)$-th round of the KSA, we assume that all the following events occur:

$$\begin{aligned}
j_1^K &= K[0] = f_0 \notin \{1, 2, \ldots, r-1, r, f_{r-1}\}, \\
j_2^K &= K[0] + K[1] + S_1^K[1] = f_1 \notin \{2, 3, \ldots, r-1, r, f_0, f_{r-1}\}, \\
j_3^K &= K[0] + \sum_{x=1}^{2}(K[x] + S_x^K[x]) = f_2 \notin \{3, 4, \ldots, r-1, r, f_0, f_{r-1}\}, \\
&\vdots \\
j_{r-1}^K &= K[0] + \sum_{x=1}^{r-2}(K[x \bmod \ell] + S_x^K[x]) = f_{r-2} \notin \{r-1, r, f_0, f_{r-1}\}, \\
j_r^K &= K[0] + \sum_{x=1}^{r-1}(K[x \bmod \ell] + S_x^K[x]) = f_{r-1}, \\
j_{r+1}^K &= K[0] + \sum_{x=1}^{r}(K[x \bmod \ell] + S_x^K[x]) = f_r = f_0.
\end{aligned}$$

Figure 6.3 shows a state transition when the above assumptions hold and $r = 3$. Note that $f_{r-1} = f_{r-1} - (f_r - f_0) = K[0] - K[r \bmod \ell] - r$ when the above event $(f_r = f_0)$ occurs. Under the assumptions, both $S_{r+1}^K[r-1] = K[0] - K[r \bmod \ell] - r$ and $S_{r+1}^K[r] = 0$ always hold simultaneously after the $(r+1)$-th round of the KSA.

We now rewrite $S_x^K[x]$ into $S_1[x]$ for $x \in [1, r-1]$ as follows:

$$\begin{aligned}
j_1^K &= K[0] = f_0 \notin \{1, 2, \ldots, r-1, r, f_{r-1}\} \text{ w.p. } \frac{N-r-1}{N}, \\
j_2^K &= K[0] + K[1] + S_1^K[1] = f_1 \notin \{2, 3, \ldots, r-1, r, f_0, f_{r-1}\} \text{ w.p. } \frac{N-r-1}{N}, \\
j_3^K &= K[0] + \sum_{x=1}^{2}(K[x] + S_1^K[x]) = f_2 \notin \{3, 4, \ldots, r-1, r, f_0, f_{r-1}\} \text{ w.p. } \frac{N-r}{N-1}, \\
&\vdots
\end{aligned}$$

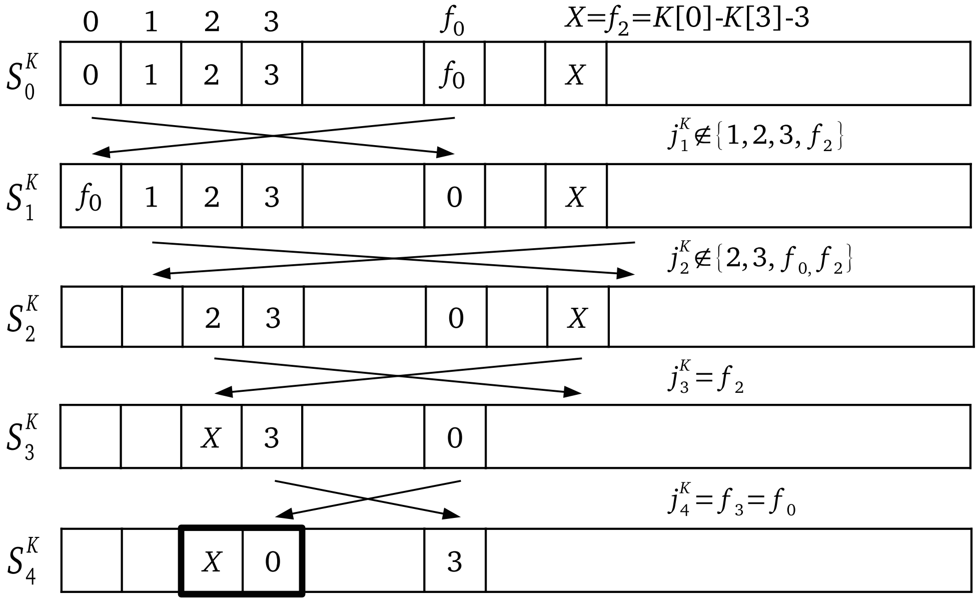
0
1
2
3
f_0
X=f_2=K[0]-K[3]-3
S_0^K
$j_1^K \notin \{1,2,3,f_2\}$
S_1^K
$j_2^K \notin \{2,3,f_{0},f_2\}$
S_2^K
$j_3^K = f_2$
S_3^K
$j_4^K = f_3 = f_0$
S_4^K

Figure 6.3: State transition diagram of the major path in Phase 1 when $r = 3$.

$$\begin{aligned}
j^K_{r-1} &= K[0] + \sum_{x=1}^{r-2}(K[x \bmod \ell] + S_1^K[x]) = f_{r-2} \notin \{r-1, r, f_0, f_{r-1}\} \text{ w.p. } \frac{N-4}{N-r+3},\\
j^K_{r} &= K[0] + \sum_{x=1}^{r-1}(K[x \bmod \ell] + S_1^K[x]) = f_{r-1} \text{ w.p. } 1,\\
j^K_{r+1} &= K[0] + \sum_{x=1}^{r}(K[x \bmod \ell] + S_1^K[x]) = f_{r} = f_0 \text{ w.p. } \frac{1}{N}.
\end{aligned}$$

This is because $S_1^K[x]$ is never swapped during the first x rounds when all the individual events occur. Note that the internal state in RC4 is a permutation, and then each of the individual events occurs with the above described probability. Therefore, the probability that all events occur simultaneously is given by

$$\beta_r \approx \frac{1}{N} \cdot \frac{N-r-1}{N} \cdot \frac{\prod_{x=3}^{r}(N-x-1)}{\prod_{x=0}^{r-3}(N-x)}.$$

On the other hand, if any individual event does not occur, we then assume that both $S^K_{r+1}[r-1] = K[0] - K[r \bmod \ell] - r$ and $S^K_{r+1}[r] = 0$ hold simultaneously with probability approximately $\frac{1}{N}$ (random association). The probability of random association in this case is $\frac{1}{N(N-1)}$ because the internal state in RC4 is a permutation. Therefore, the probability in that case is given by $\frac{1}{N(N-1)}(1 - \beta_r)$.

Phase 2. From the $(r+2)$-th round to the end of the KSA, we assume that all the following events occur:

- From the $(r+2)$-th round to the end of the KSA, we assume that the values of j^K

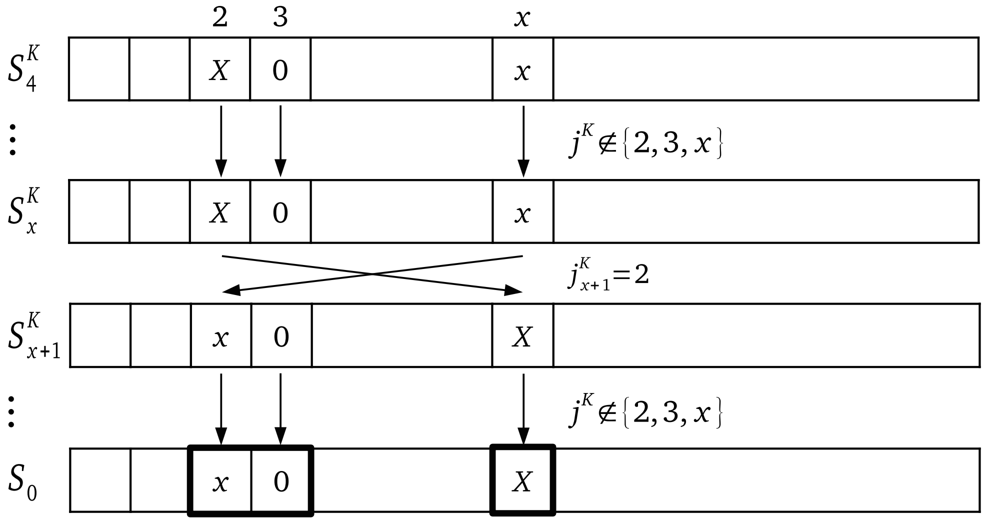

Figure 6.4: State transition diagram of the major path in Phase 2 when $r = 3$.

are not equal to r. This event occurs with probability approximately $(1 - \frac{1}{N})^{N-r-1}$.

- For an index $x \in [r+1, N-1]$, we assume that $S_x^K[x] = x$. This event occurs with probability approximately $(1 - \frac{1}{N})^x$.
- From the $(r+2)$-th to the x-th round of the KSA, we assume that the values of j^K are not equal to $r - 1$. This event occurs with probability approximately $(1 - \frac{1}{N})^{x-r-1}$.
- At the $(x + 1)$-th round of the KSA, we assume that $j_{x+1}^K = r - 1$. This event occurs with probability approximately $\frac{1}{N}$. Thus, $S_{x+1}^K[r - 1] = x$ owing to the swap operation.
- For the remaining $N - x - 1$ rounds of the KSA, we assume that the values of j^K do not touch the indices $r - 1$ and x. This event occurs with probability approximately $(1 - \frac{2}{N})^{N-x-1}$.

Figure 6.4 shows a state transition when the above assumptions hold and $r = 3$. Under the above assumptions, all of $S_0[r - 1] = x$, $S_0[r] = 0$, and $S_0[x] = K[0] - K[r \bmod \ell] - r$ always hold simultaneously after the end of the KSA. Therefore, the probability that all events occur simultaneously is given by

$$\gamma_r \approx \left(1 - \frac{1}{N}\right)^{N-r-1} \cdot \frac{1}{N} \cdot \sum_{x=r+1}^{N-1} \left(1 - \frac{1}{N}\right)^x \cdot \left(1 - \frac{1}{N}\right)^{x-r-1} \cdot \left(1 - \frac{2}{N}\right)^{N-x-1}.$$

Phase 3. From the initial to the $(r - 1)$-th round of the PRGA, we assume that all of the following events occur:

$$\begin{aligned} j_1 &= S_0[1] \notin \{2, 3, \ldots, r-1, r, x\}, \\ j_2 &= \sum_{u=0}^{1} S_u[u+1] \notin \{3, 4, \ldots, r-1, r, x\}, \end{aligned}$$

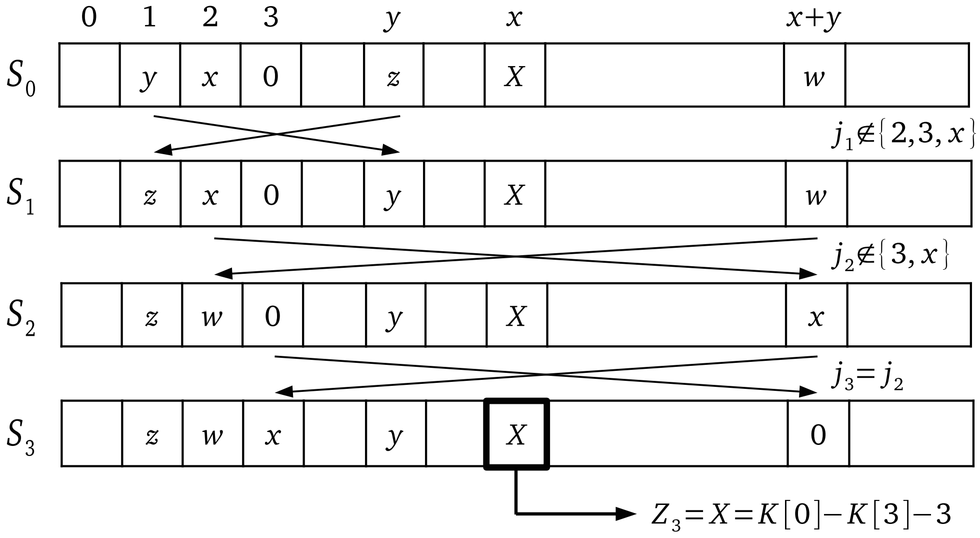

Figure 6.5: State transition diagram of the major path in Phase 3 when $r = 3$.

$$\begin{aligned} &\vdots \\ j_{r-2} &= \sum_{u=0}^{r-3} S_u[u+1] \notin \{r-1, r, x\}, \\ j_{r-1} &= \sum_{u=0}^{r-2} S_u[u+1] \notin \{r, x\}. \end{aligned}$$

Figure 6.5 shows a state transition when the above assumptions hold and $r = 3$. We note that the values of j do not touch the index r and $x \in [r+1, N-1]$ from the initial to the $(r-1)$-th round of the PRGA. Under the above assumptions, $S_r[r] = S_{r-1}[j_r] = S_{r-1}[j_{r-1}] = S_{r-2}[r-1] = S_0[r-1] = x$ and $S_r[j_r] = S_{r-1}[r] = S_0[r] = 0$ always hold simultaneously after the $(r-1)$-th round of the PRGA. After that, the PRGA outputs $Z_r = S_r[S_r[r] + S_r[j_r]] = S_r[x] = S_0[x] = K[0] - K[r \bmod \ell] - r$.

As with the discussion in Phase 1, we now rewrite S_u into S_0 as follows:

$$\begin{aligned} j_1 &= S_0[1] \notin \{2, 3, \ldots, r-1, r, x\} \text{ w.p. } 1 - \sum_{v=2}^{r} \zeta_{1,v} - \sum_{x=r+1}^{N-1} \frac{\zeta_{1,x}}{N-r-2}, \\ j_2 &= \sum_{u=0}^{1} S_0[u+1] \notin \{3, 4, \ldots, r-1, r, x\} \text{ w.p. } \frac{N-r+1}{N-1}, \\ &\vdots \\ j_{r-2} &= \sum_{u=0}^{r-3} S_0[u+1] \notin \{r-1, r, x\} \text{ w.p. } \frac{N-3}{N-r+3}, \\ j_{r-1} &= \sum_{u=0}^{r-2} S_0[u+1] \notin \{r, x\} \text{ w.p. } \frac{N-2}{N-r+2}. \end{aligned}$$

Note that the internal state in RC4 is a permutation, and then each of the individual events occurs with the above described probability[1]. Therefore, the probability that all the above events occur simultaneously is given by

$$\begin{aligned}\delta_r &\approx \left(1-\sum_{v=2}^{r}\zeta_{1,v}-\sum_{x=r+1}^{N-1}\frac{\zeta_{1,x}}{N-r-2}\right)\cdot\frac{\prod_{y=2}^{r-1}(N-y)}{\prod_{y=1}^{r-2}(N-y)}\\ &= (1-\sum_{v=2}^{r}\zeta_{1,v}-\sum_{x=r+1}^{N-1}\frac{\zeta_{1,x}}{N-r-2})\cdot\frac{N-r+1}{N-1}.\end{aligned}$$

On the other hand, if any individual event does not occur, we then assume that the PRGA outputs $Z_r = K[0] - K[r \bmod \ell] - r$ with probability approximately $\frac{1}{N}$ (random association). Therefore, the probability in that case is given by $\frac{1}{N}(1-\delta_r)$.

We assume that all events in the above three phases are mutually independent. Therefore, we obtain the probability of the major path as

$$\alpha_r \approx \left(\beta_r + \frac{1}{N(N-1)}(1-\beta_r)\right)\cdot\gamma_r\cdot\left(\delta_r+\frac{1}{N}(1-\delta_r)\right).$$

If any phase does not hold, we then assume that $Z_r = K[0] - K[r \bmod \ell] - r$ with probability approximately $\frac{1}{N}$ (random association). In summary, we obtain

$$\Pr(Z_r = K[0] - K[r \bmod \ell] - r) \approx \alpha_r + \frac{1}{N}(1-\alpha_r). \qquad \square$$

Theorem 6.2 ([IM18a, Theorem 9]). *For any arbitrary secret key K, a key correlation of the keystream byte Z_1 in WPA-TKIP is given by*

$$\Pr(Z_1 = K[0] - K[1] - 1) \approx \frac{1}{N}(1-\alpha_1),$$

where $\alpha_1 \approx \frac{1}{N^2}\cdot(1-\frac{2}{N})\cdot(1-\frac{1}{N})^{N-2}\cdot\sum_{x=2}^{N-1}(1-\frac{1}{N})^{x}\cdot(1-\frac{1}{N})^{x-2}\cdot(1-\frac{2}{N})^{N-x-1}$.

Proof. The major path for the target event is as follows:

- We assume that $K[0] \neq 0, 1$ and $K[1] = 255$. This event occurs with probability approximately $\frac{2}{N}(1-\frac{1}{N})$.
- After the second round of the KSA, $S_2^K[1] = 0$ because $j_2^K = K[0] + K[1] + 1 = K[0]$.
- From the third round to the end of the KSA, we assume that the values of j^K are not equal to 1. This event occurs with probability approximately $(1-\frac{1}{N})^{N-2}$.
- For an index $x \in [2, N-1]$, we assume that $S_x^K[x] = x$. This event occurs with probability approximately $(1-\frac{1}{N})^{x}$.

[1] $\Pr(S_0[1] = x)$ is an average probability because the range of x is from $r+1$ to $N-1$.

- For the third to the x-th round of the KSA, we assume that the values of j^K are not equal to 0. This event occurs with probability approximately $(1-\frac{1}{N})^{x-2}$.
- At the $(x+1)$-th round of the KSA, we assume that $j^K_{x+1} = 0$. This event occurs with probability approximately $\frac{1}{N}$ (random association). Thus, $S^K_{x+1}[r-1] = x$ owing to the swap operation.
- For the remaining $N-x-1$ rounds of the KSA, we assume that the values of j^K do not touch the indices 0 and x. This event occurs with probability approximately $(1-\frac{2}{N})^{N-x-1}$.

If all the individual events occur, $S_0[0] = x$, $S_0[1] = 0$, and $S_0[x] = K[0]$ always hold simultaneously after the end of the KSA, and then the PRGA outputs $Z_1 = K[0] = K[0] - K[1] - 1$ as $K[1] = 255$. We assume that the individual events in the major path become mutually independent. Therefore, all events occur with probability approximately $\alpha_1 \approx \frac{1}{N^2} \cdot (1-\frac{2}{N}) \cdot (1-\frac{1}{N})^{N-2} \sum_{x=2}^{N-1} (1-\frac{1}{N})^x \cdot (1-\frac{1}{N})^{x-2} \cdot (1-\frac{2}{N})^{N-x-1}$. On the other hand, Theorem 3.11 presents that the range of $K[1]$ is limited to either from 32 to 63 or from 96 to 127 in WPA-TKIP [GMM+14]. Thus, the target event never occurs because $K[1] \neq 255$ in WPA-TKIP.

We assume that $Z_1 = K[0]-K[1]-1$ with probability approximately $\frac{1}{N}$ (random association), except for the major path. Therefore, we obtain $\Pr(Z_1 = K[0] - K[1] - 1) \approx \frac{1}{N}(1-\alpha_1)$. □

Theorem 6.3 ([IM18a, Theorem 10]). *For any arbitrary secret key K, a key correlation of the keystream byte Z_2 in both generic RC4 and WPA-TKIP is given by*

$$\Pr(Z_2 = K[0] - K[2] - 2) \approx \frac{1}{N}.$$

Proof. We prove the major path for the target event in the same way as the proof of Theorem 6.1 when $r = 2$. After the end of the KSA, $S_0[1] = x$, $S_0[2] = 0$, and $S_0[x] = K[0] - K[2] - 2$ always hold simultaneously (see Phase 2 in the proof of Theorem 6.1). In addition, $S_0[1] \neq 2$ always hold because $x \in [3, N-1]$ during Phase 2 in the proof of Theorem 6.1.

Figure 6.6 shows a state transition diagram from the initial to the second round of the PRGA. According to the state transition diagram, the PRGA outputs $Z_2 = 0$. Then, the target event occurs only when $K[0] - K[2] - 2 = 0$, whose probability is $\frac{1}{N}$ because the RC4 key is generated uniformly at random. Therefore, we obtain the probability of the major path as $\frac{1}{N}\alpha_2$.

We assume that the target event occurs with probability approximately $\frac{1}{N}$ (random association), except for the major path. In summary, we obtain

$$\Pr(Z_2 = K[0] - K[2] - 2) \approx \frac{1}{N}\alpha_2 + \frac{1}{N}(1-\alpha_2) = \frac{1}{N},$$

where $\alpha_2 \approx \frac{1}{N^2} \cdot (1-\frac{3}{N}) \cdot (1-\frac{1}{N})^{N-3} \sum_{x=3}^{N-1} (1-\frac{1}{N})^x \cdot (1-\frac{1}{N})^{x-3} \cdot (1-\frac{2}{N})^{N-x-1}$. □

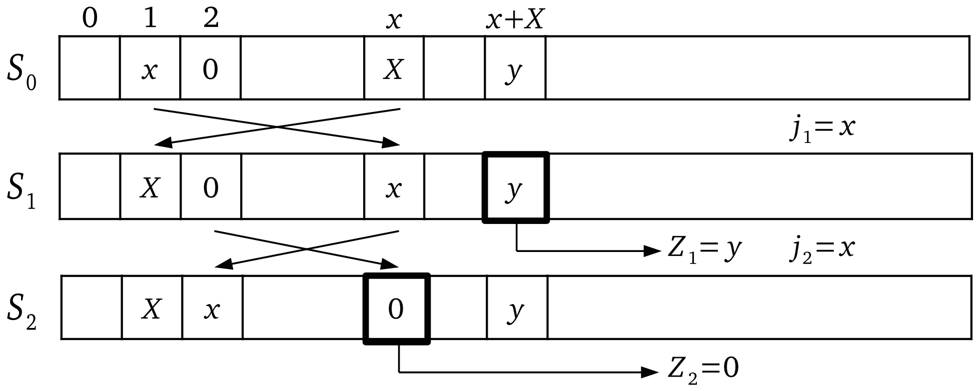

Figure 6.6: State transition diagram of the major path in the case of Z_2.

6.3 Experimental Evaluations

We have performed experiments to check the accuracy of the theoretical values in all theorems. Our experiments used N^5 samples generated from randomly chosen keys in generic RC4 and WPA-TKIP. Because each of the target events has a relative bias with a probability of at least $\mathcal{O}(\frac{1}{N})$, the number of samples to distinguish each of the target event from random distribution is at least $\mathcal{O}(N^3)$ according to Theorem 3.2.

We have evaluated the percentage of the relative error ϵ_{max} of the experimental values compared with the theoretical values (see Section 2.5.3). Figures 6.7–6.9 show comparisons between the experimental and theoretical probabilities in generic RC4 and WPA-TKIP, and the percentage of the relative error ϵ_{max}, respectively. We can see that ϵ_{max} is small enough in each case in both generic RC4 and WPA-TKIP, such as $\epsilon_{max} \leq 0.456$ (%). Therefore, we have checked the accuracy of the theoretical values in all theorems.

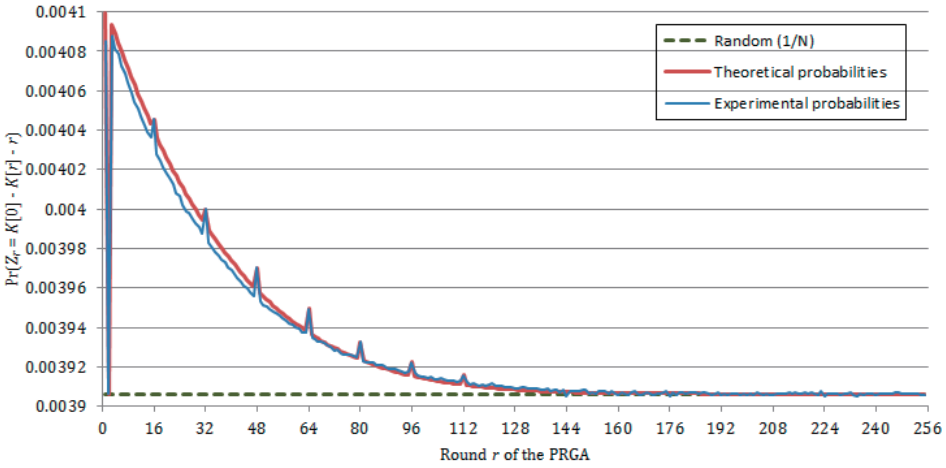

Figure 6.7: Comparison between experimental and theoretical probabilities in generic RC4.

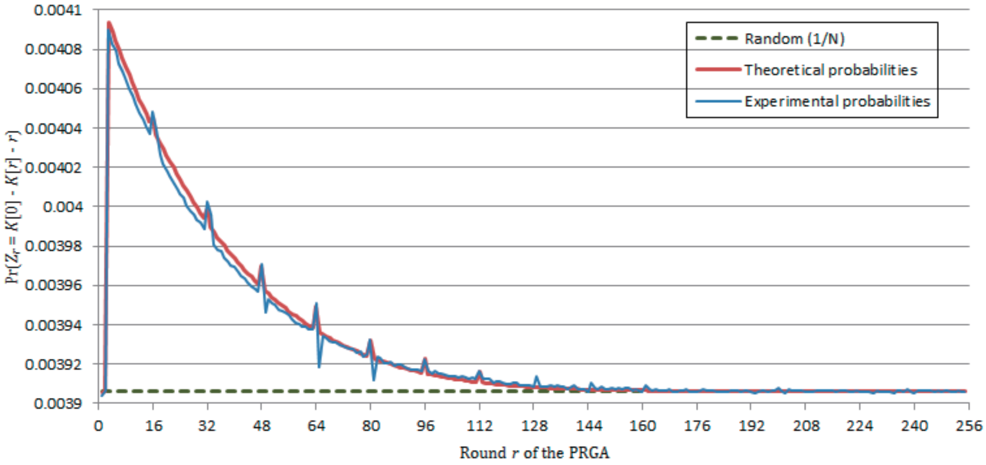

Figure 6.8: Comparison between experimental and theoretical probabilities in WPA-TKIP.

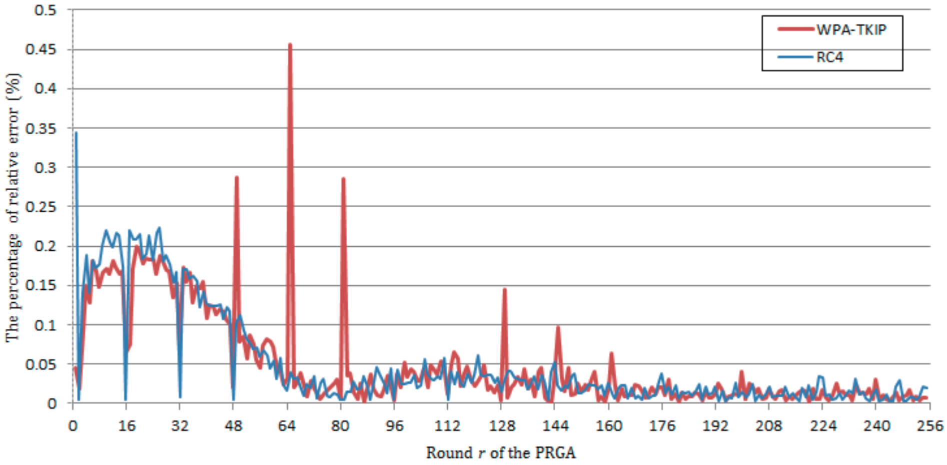

Figure 6.9: Percentage of relative error ϵ_{max} between experimental and theoretical probabilities in both generic RC4 and WPA-TKIP.

6.4 Applications to Plaintext Recovery on WPA-TKIP

6.4.1 Extension of the IOWM Attack

This subsection discusses how to extend the IOWM attack in [IOWM13], particularly on WPA-TKIP, using our iterated RC4 key correlations. Our attack is similar to the SMMPS attack in [GMM+14] (see Section 3.2.2). When the iterated RC4 key correlations induce higher biases than certain events used in the IOWM attack, our attack can be improved in the same way as the SMMPS attack.

We have compared the iterated RC4 key correlations with a set of the strongest biases in [IOWM13] (see Table 3.1). As a result, the iterated RC4 key correlations of the keystream bytes $\{Z_{17}, Z_{18}, Z_{33}, Z_{34}, Z_{49}, Z_{50}, Z_{66}, Z_{82}\}$ induce higher biases than the corresponding events used in the IOWM attack. Thus, we reduce the number of ciphertexts for recovering the corresponding bytes of a plaintext on WPA-TKIP according to Theorem 3.2. Table 6.1 shows

Table 6.1: Significant improvement for recovering eight bytes of a plaintext on WPA-TKIP.

Round	Iterated RC4 key correlations			Biases used in [IOWM13]		
	Event	Probability	# of ciphertexts	Event	Probability	# of ciphertexts
17	$Z_{17} = K[0] - K[1] - 17$	$2^{-8} \cdot (1 + 2^{-4.863})$	$2^{17.727}$	$Z_{17} = 17$	$2^{-8} \cdot (1 + 2^{-7.589})$	$2^{23.178}$
18	$Z_{18} = K[0] - K[2] - 18$	$2^{-8} \cdot (1 + 2^{-4.900})$	$2^{17.800}$	$Z_{18} = 18$	$2^{-8} \cdot (1 + 2^{-7.605})$	$2^{23.210}$
33	$Z_{33} = K[0] - K[1] - 33$	$2^{-8} \cdot (1 + 2^{-5.477})$	$2^{18.955}$	$Z_{33} = 0$	$2^{-8} \cdot (1 + 2^{-7.885})$	$2^{23.770}$
34	$Z_{34} = K[0] - K[2] - 34$	$2^{-8} \cdot (1 + 2^{-5.518})$	$2^{19.035}$	$Z_{34} = 0$	$2^{-8} \cdot (1 + 2^{-7.896})$	$2^{23.791}$
49	$Z_{49} = K[0] - K[1] - 49$	$2^{-8} \cdot (1 + 2^{-6.149})$	$2^{20.297}$	$Z_{49} = 0$	$2^{-8} \cdot (1 + 2^{-8.057})$	$2^{24.114}$
50	$Z_{50} = K[0] - K[2] - 50$	$2^{-8} \cdot (1 + 2^{-6.193})$	$2^{20.386}$	$Z_{50} = 0$	$2^{-8} \cdot (1 + 2^{-8.068})$	$2^{24.135}$
66	$Z_{66} = K[0] - K[2] - 66$	$2^{-8} \cdot (1 + 2^{-6.934})$	$2^{21.869}$	$Z_{66} = 0$	$2^{-8} \cdot (1 + 2^{-8.239})$	$2^{24.479}$
82	$Z_{82} = K[0] - K[2] - 82$	$2^{-8} \cdot (1 + 2^{-7.752})$	$2^{23.505}$	$Z_{82} = 0$	$2^{-8} \cdot (1 + 2^{-8.410})$	$2^{24.820}$

significant improvement for recovering eight bytes of a plaintext on WPA-TKIP in comparison with the IOWM attack.

To summarize our results, by using our iterated RC4 key correlations instead of the corresponding events used in the IOWM attack, the number of ciphertexts for recovering P_{17}, P_{18}, P_{33}, P_{34}, P_{49}, P_{50}, P_{66}, and P_{82} on WPA-TKIP can be reduced to $2^{17.727}/2^{23.178}$, $2^{17.800}/2^{23.210}$, $2^{18.955}/2^{23.770}$, $2^{19.035}/2^{23.791}$, $2^{20.297}/2^{24.114}$, $2^{20.386}/2^{24.135}$, $2^{21.869}/2^{24.479}$, and $2^{23.505}/2^{24.820}$, respectively.

6.4.2 Extension of the ABPPS Attack

This subsection discusses how to extend the ABPPS attack in [ABP+13], particularly on WPA-TKIP, using key correlations of the keystream bytes. We propose a plaintext recovery algorithm that considers key correlations of the keystream bytes instead of all possible short-term biases only for round $r \in \{1, 3, 17, 18, 33, 34, 49, 50, 66, 82, 256, 257\}$ as the following four steps:

Step 1. Estimate the accurate distributions of the keystream bytes Z_r in the first 257 rounds:

$$p_{r,k} := \begin{cases} \Pr(Z_r = -K[0] - K[1] + k) & \text{when } r = 1, 257, \\ \Pr(Z_r = K[0] + K[1] + K[2] + k) & \text{when } r = 3, \\ \Pr(Z_r = K[0] - K[1] + k) & \text{when } r = 17, 33, 49, \\ \Pr(Z_r = K[0] - K[2] + k) & \text{when } r = 18, 34, 50, 66, 82, \\ \Pr(Z_r = -K[0] + k) & \text{when } r = 256, \\ \Pr(Z_r = k) & \text{otherwise,} \end{cases}$$

where $k = \text{0x00}, \ldots, \text{0xFF}$ and $p_{r,k}$ is taken from randomly chosen keys.

Step 2. Assuming that we obtain S ciphertexts $\{C_1, \ldots, C_S\}$ for the attack in the broadcast setting. Let $C_{j,r}$ be the r-th round of ciphertext C_j. For any candidate plaintext byte μ

in each round and $k = 0\text{x}00, ..., 0\text{xFF}$, the vector $(N^{(\mu)}_{0\text{x}00}, ..., N^{(\mu)}_{0\text{xFF}})$ with

$$N^{(\mu)}_k = \begin{cases} |\{j \mid C_{j,r} = (-K[0] - K[1] + k) \oplus \mu\}_{1\le j\le S}| & \text{when } r = 1, 257, \\ |\{j \mid C_{j,r} = (K[0] + K[1] + K[2] + k) \oplus \mu\}_{1\le j\le S}| & \text{when } r = 3, \\ |\{j \mid C_{j,r} = (K[0] - K[1] + k) \oplus \mu\}_{1\le j\le S}| & \text{when } r = 17, 33, 49, \\ |\{j \mid C_{j,r} = (K[0] - K[2] + k) \oplus \mu\}_{1\le j\le S}| & \text{when } r = 18, 34, 50, 66, 82, \\ |\{j \mid C_{j,r} = (-K[0] + k) \oplus \mu\}_{1\le j\le S}| & \text{when } r = 256, \\ |\{j \mid C_{j,r} = k \oplus \mu\}_{1\le j\le S}| & \text{otherwise,} \end{cases}$$

represents the induced distribution of the keystream bytes Z_r obtained from $\{C_{j,r}\}_{1\le j\le S}$ and μ.

Step 3. Calculate the probability λ_μ that that the candidate plaintext byte μ is correctly encrypted into the ciphertext bytes $\{C_{j,r}\}_{1\le j\le S}$ as

$$\lambda_\mu = \frac{S!}{N^{(\mu)}_{0\text{x}00}! \cdots N^{(\mu)}_{0\text{xFF}}!} \prod_{k\in\{0\text{x}00,\ \dots,\ 0\text{xFF}\}} p_{r,k}^{N^{(\mu)}_k},$$

where λ_μ follows the multinomial distribution with parameter S and $(p_{r,0\text{x}00}, \dots, p_{r,0\text{xFF}})$ (see Definition 2.6).

Step 4. Determine the maximum-likelihood plaintext byte value P^*_r by calculating λ_μ for all $0\text{x}00 \le \mu \le 0\text{xFF}$ and then distinguishing μ such that λ_μ is the maximum value.

The details of our proposed attack are described as Algorithm 9.

We have performed experiments in order to compare the number of ciphertexts for recovering 12 bytes of a plaintext $\{P_1, P_3, P_{17}, P_{18}, P_{33}, P_{34}, P_{49}, P_{50}, P_{66}, P_{82}, P_{256}, P_{257}\}$ by our proposed attack and the existing attacks (the IOWM attack, the ABPPS attack, and the PPS attack). Our experimental results are described as Table 6.2. We summarize the list of the number of ciphertexts with the success probability of 100% in each case. From the table, we can achieve significant improvement for recovering five bytes of a plaintext on WPA-TKIP by our proposed attack. In fact, the number of samples for recovering P_3, P_{18}, P_{34}, P_{50}, and P_{66} on WPA-TKIP can be reduced to $2^{20}/2^{27}$, $2^{24}/2^{28}$, $2^{25}/2^{26}$, $2^{26}/2^{28}$, and $2^{28}/2^{29}$, respectively.

6.4.3 Optimization of Plaintext Recovery on WPA-TKIP

This subsection discusses how to optimize the plaintext recovery of the first 257 bytes on WPA-TKIP. We assumed that the plaintext recovery of the first 257 bytes on WPA-TKIP can be optimized by combining the best approach for each round from our proposed attack in Section 6.4.2 and the existing attacks (the IOWM attack, the ABPPS attack, the SMMPS attack, and the PPS attack).

We have performed experiments in order to compare the probabilities of success for recovering the first 257 bytes of a plaintext by our proposed attack, the PPS attack, and the optimized

Algorithm 9 Our proposed plaintext recovery attack

```
Input: ${C_j}_{1 \le j \le S}$: $S$ ciphertexts by encrypting the same plaintext $P$,
    $r$: the number of rounds,
    $p_{r,k}$: the accurate distribution of the keystream $Z_r$ at round $r$.
Output: $P_r^*$: estimate for plaintext byte $P_r$.
$N_{0x00} \leftarrow 0, \ldots, N_{0xFF} \leftarrow 0$
for $j$ from 1 to $S$ do
    if $r \in \{1, 257\}$ then
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}-(-K[0]-K[1])} + 1$
    else if $r = 3$ then
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}-(K[0]+K[1]+K[2])} + 1$
    else if $r \in \{17, 33, 49\}$ then
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}-(K[0]-K[1])} + 1$
    else if $r \in \{18, 34, 50, 66, 82\}$ then
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}-(K[0]-K[2])} + 1$
    else if $r = 256$ then
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}-(-K[0])} + 1$
    else
        $N_{C_{j,r}} \leftarrow N_{C_{j,r}} + 1$
    end if
end for
for $\mu$ from 0x00 to 0xFF do
    for $k$ from 0x00 to 0xFF do
        $N_k^{(\mu)} \leftarrow N_{k \oplus \mu}$
    end for
    $\lambda_\mu \leftarrow \sum_{k=0x00}^{0xFF} N_k^{(\mu)} \log p_{r,k}$
end for
$P_r^* \leftarrow \arg\max_{\mu \in \{0xFF, \ldots, 0xFF\}} \lambda_\mu$
```

Table 6.2: Experimental comparison of the number of ciphertexts for recovering 12 bytes of a plaintext on WPA-TKIP by our proposed attack and the existing attacks. The probability of success in each case is 100%.

r	# of ciphertexts	
	Our proposed attack	The existing attacks
1	2^{17}	2^{16}
3	2^{20}	2^{27}
17	2^{23}	2^{23}
18	2^{24}	2^{28}
33	2^{24}	2^{23}
34	2^{25}	2^{26}
49	2^{26}	2^{24}
50	2^{26}	2^{28}
66	2^{28}	2^{29}
82	2^{29}	2^{29}
256	2^{19}	2^{19}
257	2^{22}	2^{22}

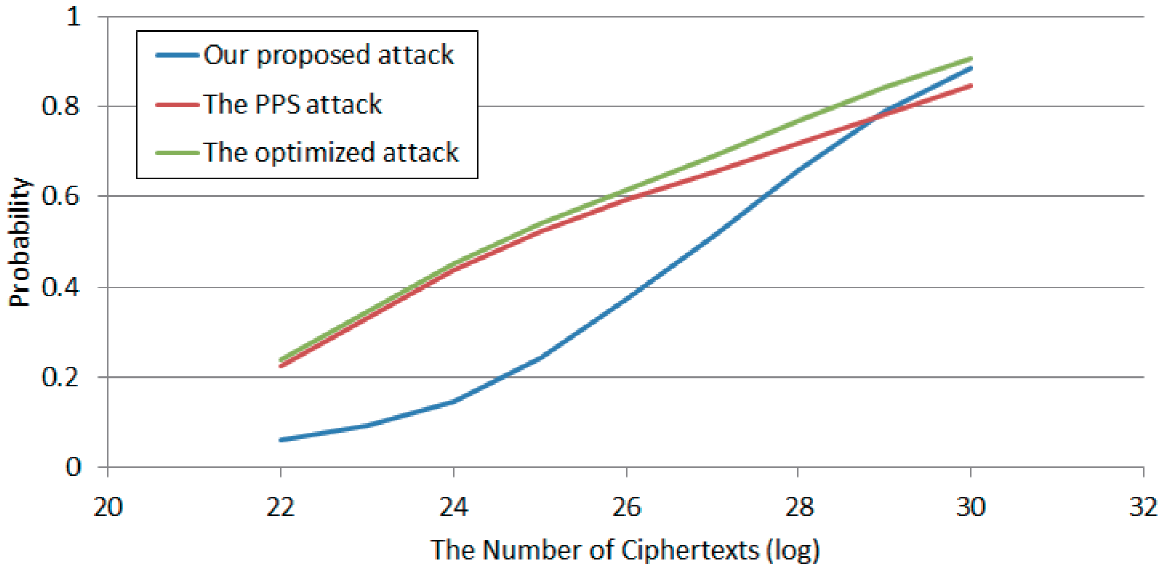

Figure 6.10: Success probabilities for recovering the first 257 bytes of a plaintext by our proposed attack, the PPS attack, and the optimized attack from $2^{22}, 2^{23}, \dots, 2^{30}$ ciphertexts in each cases.

attack from $2^{22}, 2^{23}, \dots, 2^{30}$ ciphertexts in each cases. Figure 6.10 shows our experimental results. The horizontal and vertical lines represent the number of ciphertexts with a logarithmic scale and the probabilities of success in each attack, respectively. The blue, red, and green lines represent the experimental results in our proposed attack, the PPS attack, and the optimized attack, respectively. From the figure, we see that the optimized attack can recover the first 257 bytes of a plaintext on WPA-TKIP with the highest probability of success in the attacks. As a result, we can achieve to recover the first 257 bytes of a plaintext on WPA-TKIP from approximately 2^{30} ciphertexts with the success probability of approximately 90.8%, whose probability is approximately 6.0% higher than the success probability of the PPS attack.

6.5 Chapter Conclusion

This chapter has focused on key correlations of the keystream bytes, and has investigated correlations between $(K[0], K[r \bmod \ell])$ pairs and Z_r based on the previous works in [SVV10, Sar14]. Then, we have provided theoretical proofs of newly observed key correlations of the keystream bytes. Combining our key correlations with the previous ones, they can be integrated as *iterated RC4 key correlations*, i.e., $Z_r = K[0] - K[r \bmod \ell] - r$ for any arbitrary round r.

Furthermore, this chapter has discussed the extend IOWM attack, the extend ABPPS attack, and the optimized plaintext recovery attack on WPA-TKIP. The first attack has achieved significant improvement for recovering eight bytes of a plaintext $\{P_{17}, P_{18}, P_{33}, P_{34}, P_{49}, P_{50}, P_{66}, P_{82}\}$ using our iterated RC4 key correlations in the same way as the SMMPS attack. the second attack has achieved significant improvement for recovering five bytes of a plaintext $\{P_3, P_{18}, P_{34}, P_{50}, P_{66}\}$ using key correlations of the keystream bytes (including ours and the previous ones [GMM+14]). The third attack has optimized the plaintext recovery of the first 257 bytes by combining the best approach for each round. As a result, the optimized attack has achieved to recover the first 257 bytes of a plaintext on WPA-TKIP from approximately 2^{30} ciphertexts with the success probability of approximately 90.8%, whose probability is approximately 6.0% higher than the success probability of the PPS attack.

Chapter 7

Conclusion and Future Works

We conclude this dissertation in this chapter. This dissertation has presented *a study on statistical cryptanalysis of stream ciphers*, and focused particularly on RC4 in Chapters 4–6.

Section 7.1 revisits the individual chapters by summarizing our results on statistical cryptanalysis of RC4 stream cipher. Section 7.2 discusses future works for statistical cryptanalysis of stream ciphers. This dissertation ends in Section 7.3.

7.1 Summary of Our Results

We firmly believe that our study has improved the awareness about the threat of information security to many people and has proposed the analysis methods of all existing and future stream ciphers toward the realization of secure communications. Our results in this dissertation can be summarized as follows:

Refined Glimpse Correlations

We have presented the *Refined Glimpse Correlations*. The existing Glimpse Correlations include the Glimpse Theorem by Jenkins in [Jen96] and the Long-term Glimpse by Maitra and Sen Gupta in [MG13], which are correlations between the keystream bytes and the internal state variables. They provided only cases with positive biases, and dealt with correlations on each round all together. Then, we have investigated to find dual cases of the existing Glimpse Correlations and cases with precise biases on specific rounds. As a result of our investigations, we have refined the existing Glimpse Correlations by demonstrating the existence of events with two dual cases, a new positive bias, and three precise biases on the first and second round, and have presented their theoretical proofs.

Key Correlations of the Internal State Variables

We have presented the *Key Correlations of the Internal State Variables.* The existing key correlations in WPA-TKIP included only cases of the keystream bytes by Sen Gupta et al. in

[GMM+14], which are called key correlations of the keystream bytes. Then, we have investigated to find cases of the unknown internal state variables in WPA-TKIP and cases with different biases between generic RC4 and WPA-TKIP. As a result of our investigations, we have demonstrated hundreds of key correlations of the internal state variables experimentally, and have presented theoretical proofs for 22 cases. Furthermore, our investigations have clarified how TKIP induces biases of the internal state of generic RC4 by demonstrating several cases with different biases between generic RC4 and WPA-TKIP.

Toward Secure RC4 Key Setting in WPA-TKIP

We have discussed the *Toward Secure RC4 Key Setting in WPA-TKIP* in such a way that it can retain the security level of generic RC4. The existing work by Sen Gupta et al. in [GMM+14] and our investigations in Chapter 5 have clarified how TKIP induces key correlations of the keystream bytes and the internal state variables of generic RC4. Then, we have investigated to find the refined three bytes of the RC4 key derived from the known IV. As a result of our investigations, we have reduced the number of key correlations induced by the refined RC4 key setting by approximately 70% in comparison with the original setting in WPA-TKIP.

Iterated Key Correlations of the Keystream Bytes

We have presented the *Iterated Key Correlations of the Keystream Bytes*. The existing key correlations by Sepehrdad et al. in [SVV10] were limited to ℓ rounds, and no correlations between $K[r \bmod \ell]$ and Z_r for $r \geq \ell$ have been investigated, although $K[r \bmod \ell]$ may be *iterated* to use to produce Z_r for $r \geq \ell$. Then, we have investigated to find correlations between $K[r \bmod \ell]$ and Z_r for $r \geq \ell$. As a result of our investigations, we have demonstrated the *iterated* key correlations between $(K[0], K[r \bmod \ell])$ pairs and Z_r for the first 256 rounds, and have presented theoretical proofs for them.

Improvement for Plaintext Recovery on WPA-TKIP

We have discussed three attacks toward the *Improvement for Plaintext Recovery on WPA-TKIP* using key correlations of the keystream bytes, which include the iterated key correlations and the existing ones in [GMM+14]. The first attack has extended the existing attack by Isobe et al. in [IOWM14], and has achieved significant improvement for recovering eight bytes of a plaintext in the same way as the existing attack by Sen Gupta et al. in [GMM+14]. The second attack has extended the existing attack by AlFardan et al. in [ABP+13], and has achieved significant improvement for recovering five bytes of a plaintext. The third attack has optimized the plaintext recovery of the first 257 bytes by combining the best approach from among a plurality of attacks for each round. As a result, we have demonstrated significant optimization for recovering the first 257 bytes of a plaintext from approximately 2^{30} ciphertexts with the success probability of approximately 90.8%, whose probability is approximately 6.0% higher than the success probability of the existing attacks.

7.2 Future Works

Further Improvement for Plaintext Recovery on WPA-TKIP

We discuss the *Further Improvement for Plaintext Recovery on WPA-TKIP* in the following direction. AlFardan et al. and Paterson et al. proposed plaintext recovery algorithms on generic RC4 and WPA-TKIP using not only short-term biases but also long-term biases in [ABP$^+$13] and [PPS14], respectively. We then would contribute to an improvement for the plaintext recovery attack on WPA-TKIP by extending the long-term bias attacks in [ABP$^+$13, PPS14] using key correlations of the keystream bytes as we discussed in Chapter 6.

Improvements for Key Recovery on Generic RC4, WEP, and WPA-TKIP

We discuss the *Improvements for Key Recovery on Generic RC4, WEP, and WPA-TKIP* in the following directions. Klein proposed a key recovery algorithm on WEP using a practical application of the Glimpse Theorem in [Kle08] (see Section 3.3.4). No study, however, has been reported on any key recovery algorithm using the other Glimpse Correlations, which include the Long-term Glimpse in [MG13] and our refined Glimpse Correlations. We then would contribute to an improvement for recovering full bytes of an RC4 key on WEP using a practical application of the Glimpse Correlations in the same way as the existing attack in [Kle08]. Furthermore, Sepehrdad et al. discovered new key correlations of the keystream bytes experimentally, and applied their key correlations to the theoretical key recovery attack on generic RC4 in [SVV10] (see Section 3.3.2). We then would contribute to an improvement for recovering full bytes of an RC4 key on generic RC4 and WPA-TKIP by using the iterated key correlations of the keystream bytes in the same way as the existing attack in [SVV10].

Improvement for State Recovery on Generic RC4 and WPA-TKIP

We discuss the *Improvement for State Recovery on Generic RC4 and WPA-TKIP* in the following direction. Knudsen et al. proposed a basic recursive algorithm to recover the internal state by guessing the unknown internal state variables $\{S_r[i_{r+1}], S_r[j_{r+1}], j_{r+1}, t_{r+1}\}$ in [KMP$^+$98] (see Section 3.4). Furthermore, we demonstrated hundreds of key correlations of the unknown internal state variables in generic RC4 and WPA-TKIP in Chapter 5. We then would contribute to an improvement for recovering the internal state in generic RC4 and WPA-TKIP by efficiently guessing the unknown internal state variables using our key correlations.

Toward Secure Stream Ciphers

We discuss the *Toward Secure Stream Ciphers* in the following direction. Recently, the IV is often used for initialization of the internal state in representative stream ciphers, which include HC-128 [Wu08], Rabbit [BVZ08], Salsa20/12, [Ber08b], ChaCha20 [Ber08a, Ber08c], SOSEMANUK [BBC$^+$08], Grain v1 [HJMM08], MICKEY [BD08], and Trivium [Can08]. The IV values are known for adversaries, and therefore the usage of the IV values may inhibit the secure operation of the stream ciphers as well as the IV setting in WPA-TKIP (see Chapter 5). We proposed secure RC4 key setting in WPA-TKIP in such a way that it can retain the security level of generic RC4 in Section 5.4. We then would contribute to securely operating stream ciphers by investigating secure IV setting in the stream ciphers in the same way as the discussion in Section 5.4.

7.3 Concluding Remarks

As mentioned in Chapter 1, stream ciphers can encrypt/decrypt faster than block ciphers. Therefore, stream ciphers continue to be important in order to suppress reduction in data communication speed over networks from increase in data communication quantity.

Looking back on our study, it became clear that there exist many statistical weaknesses in RC4 stream cipher. In other words, it is not appropriate to use RC4 as a cryptographic scheme. Despite this situation, RC4 is still widely used in essential security protocols for secure communications over networks such as SSL/TLS, WEP, WPA-TKIP. Particularly, according to a survey report by Information-technology Promotion Agency (IPA) in 2016 [IPA], there exist only 12.2 % of 5000 clients (questionnaire respondents) who intentionally avoid using RC4 for secure communications over the Wi-Fi networks. This fact demonstrates that most of the clients have low level of awareness about threats of information security. We believe that this dissertation will be a warning to many clients using the Internet and Wi-Fi networks, and that their awareness about threats of information security will be improved.

Our motivation in this dissertation was to contribute to security evaluations of all stream ciphers through cryptanalysis of RC4. As mentioned in Section 7.2, the IV is often used for initialization of the internal state in representative stream ciphers. Several works on cryptanalysis using IV have been reported so far [EJT07, FKM08, JM04, Mai16], however, there are few stream ciphers which has sufficiently analyzed the IV setting when designing a cryptographic scheme. Once a cryptographic scheme is designed and put into practical use, it is not easy to change its specification. Therefore, we need to analyze including the IV setting when designing a cryptographic scheme in order to ensure the highest security level. We believe that this dissertation will provide an opportunity to sufficiently analyze the IV setting for designers and will contribute toward the realization of secure communications.

List of Publications

Journals

1. Ryoma Ito and Atsuko Miyaji. Refined Glimpse Correlations of RC4. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(1):3–13, January 2016. (**Ref.** [IM16a])

2. Ryoma Ito and Atsuko Miyaji. Refined RC4 Key Correlations of Internal States in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(6):1132–1144, June 2016. (**Ref.** [IM16b])

3. Ryoma Ito and Atsuko Miyaji. Refined Construction of RC4 Key Setting in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E100-A(1):138–148, January 2017. (**Ref.** [IM17])

International Conferences

1. Ryoma Ito and Atsuko Miyaji. New Integrated Long-Term Glimpse of RC4. In Kyung-Hyune Rhee and Jeong Hyun Yi, editors, *Information Security Application - WISA 2014*, volume 8909 of *Lecture Notes in Computer Science*, pages 137–149. Springer Berlin Heidelberg, 2015. (**Ref.** [IM14a])

2. Ryoma Ito and Atsuko Miyaji. New Linear Correlations Related to State Information of RC4 PRGA Using IV in WPA. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 557–576. Springer Berlin Heidelberg, 2015. (**Ref.** [IM15c])

3. Ryoma Ito and Atsuko Miyaji. How TKIP Induces Biases of Internal States of RC4. In Emest Foo and Douglas Stebila, editors, *Information Security and Privacy - ACISP 2015*, volume 9144 of *Lecture Notes in Computer Science*, pages 329–342. Springer International Publishing, 2015. (**Ref.** [IM15a])

4. Ryoma Ito and Atsuko Miyaji. New Iterated RC4 Key Correlations. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy - ACISP 2018*, volume 10946 of *Lecture Notes in Computer Science*, pages 154–171. Springer International Publishing, 2018. (**Ref.** [IM18a])

Domestic Conferences

1. Ryoma Ito and Atsuko Miyaji. New Negative Biases in Long-Term Glimpse of RC4. In *IEICE Japan Technical Report - ISEC 2014*, ISEC 2014–3, pages 13–19, 2014–5. (**Ref.** [IM14b])

2. Ryoma Ito and Atsuko Miyaji. New Linear Correlations on State Information of RC4 in WPA. In *The 32th Symposium on Cryptography and Information Security - SCIS 2015*, 2E2–3, 2015–1. (**Ref.** [IM15b])

3. Ryoma Ito and Atsuko Miyaji. On New Iterated Key Correlations of RC4. In *The 35th Symposium on Cryptography and Information Security - SCIS 2018*, 2B3–1, 2018–1. (**Ref.** [IM18b])

4. Ryoma Ito and Atsuko Miyaji. Plaintext Recovery Attacks against WPA-TKIP Using Iterated RC4 Key Correlations. In *IEICE Japan Technical Report - ISEC 2018*, ISEC 2018–48, pages 379–386, 2018–7. (**Ref.** [IM18c])

References

[ABP$^+$13] Nadhem J. AlFardan, Daniel J. Bernstein, Keneth G. Paterson, Bertram Poettering, and Jacob C. N. Schuldt. On the Security of RC4 in TLS. In *USENIX Security Symposium 2013*, 2013.

[AIK$^+$01] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms—Design and Analysis. In *International Workshop on Selected Areas in Cryptography – SAC 2001*, pages 39–56. Springer Berlin Heidelberg, 2001.

[Ano94] Anonymous. Thank You Bob Anderson: RC4 Source Code, September 1994. http://cypherpunks.venona.com/date/1994/09/msg00304.html.

[BBC$^+$08] Cme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cdric Lauradoux, Marine Minier, Thomas Pornin, and Herv Sibert. SOSEMANUK, A Fast Software-Oriented Stream Cipher. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 98–118. Springer Berlin Heidelberg, 2008.

[BD08] Steve Babbage and Matthew Dodd. The MICKEY Stream Ciphers. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 191–209. Springer Berlin Heidelberg, 2008.

[Ber08a] Daniel J. Bernstein. ChaCha, A Variant of Salsa20. In *Workshop Record of SASC*, volume 8, 2008.

[Ber08b] Daniel J. Bernstein. The Salsa20 Family of Stream Ciphers. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 84–97. Springer Berlin Heidelberg, 2008.

[Ber08c] Daniel J. Bernstein. The Salsa20 Family of Stream Ciphers. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 84–97. Springer Berlin Heidelberg, 2008.

[BMPdM18] Remi Bricout, Sean Murphy, Kenneth G. Paterson, and Thyla Van der Merwe. Analysing and Exploiting the Mantin Biases in RC4. *Designs, Codes and Cryptography*, 86(4):743–770, 2018.

[BTCS$^+$15] Ray Beaulieu, Stefan Treatman-Clark, Douglas Shors, Bryan Weeks, Jason Smith, and Louis Wingers. The SIMON and SPECK Lightweight Block Ciphers. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, pages 1–6. IEEE, 2015.

[BVZ08] Martin Boesgaard, Mette Vesterager, and Erik Zenner. The Rabbit Stream Cipher. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 69–83. Springer Berlin Heidelberg, 2008.

[Can08] Christophe De Canniere. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 244–266. Springer Berlin Heidelberg, 2008.

[DA98] Tim Dierks and Christopher Allen. The TLS Protocol Version 1.0. *Internet Engineering Task Force - IETF, Request for Comments*, 2246, January 1998.

[Dev11] Jay L. Devore. *Probability and Statistics for Engineering and the Sciences.* Cengage learning, 2011.

[DMPS11] Apurba Das, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. Some Combinatorial Results towards State Recovery Attack on RC4. In Sushil Jajodia and Chandan Mazumdar, editors, *Information Systems Security - ICISS 2011*, volume 7093 of *Lecture Notes in Computer Science*, pages 204–214. Springer Berlin Heidelberg, 2011.

[DR99] Joan Daeman and Vincent Rijmen. AES Proposal: Rijndael. 1999.

[DR06] Tim Dierks and Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. *Internet Engineering Task Force - IETF, Request for Comments*, 4346, April 2006.

[DR08] Tim Dierks and Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. *Internet Engineering Task Force - IETF, Request for Comments*, 5246, August 2008.

[DR18] Tim Dierks and Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-28. March 2018.

[DS12] Itai Dinur and Adi Shamir. Applying Cube Attacks to Stream Ciphers in Realistic Scenarios. *Cryptography and Communications*, 4(3–4):217–232, 2012.

[DS18] Sabyasachi Dey and Santanu Sarkar. Generalization of Roos Bias in RC4 and Some Results on Key-Keystream Relations. *Journal of Mathematical Cryptology*, 12(1):43–56, 2018.

[EJT07] Hkan Englund, Thomas Johansson, and Meltem Snmez Turan. A Framework for Chosen-IV Statistical Analysis of Stream Ciphers. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *Progress in Cryptology - INDOCRYPT 2007*, volume 4859 of *Lecture Notes in Computer Science*, pages 268–281. Springer Berlin Heidelberg, 2007.

[FKK11] Alan Freier, Philip Karlton, and Paul Kocher. The Secure Sockets Layer (SSL) Protocol Version 3.0. *Internet Engineering Task Force - IETF, Request for Comments*, 6101, August 2011.

[FKM08] Simon Fischer, Shahram Khazaei, and Willi Meier. Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 236–245. Springer Berlin Heidelberg, 2008.

[FM00] Scott R. Fluhrer and David A. McGrew. Statistical Analysis of the Alleged RC4 Keystream Generator. In Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, and Bruce Schneier, editors, *Fast Software Encryption - FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 19–33. Springer Berlin Heidelberg, 2000.

[FM02] Niels Ferugson and MacFergus. *Michael: An Improved MIC for 802.11 WEP.* doc.: IEEE 802.11-02/020r0, April 2002.

[FMS01] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2001*, volume 2259 of *Lecture Notes in Computer Science*, pages 1–24. Springer Berlin Heidelberg, 2001.

[GGHN05] Guang Gong, Kishan Chand Gupta, Martin Hell, and Yassir Nawaz. Towards a General RC4-Like Keystream Generator. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *International Conference on Information Security and Cryptology - CICS 2005*, volume 3822 of *Lecture Notes in Computer Science*, pages 162–174. Springer Berlin Heidelberg, 2005.

[GMM$^+$14] Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul, and Santanu Sarkar. Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 350–369. Springer Berlin Heidelberg, 2014.

[GMPS11] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. Proof of Empirical RC4 Biases and New Key Correlations. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - SAC 2011*, volume 7118 of *Lecture Notes in Computer Science*, pages 151–168. Springer Berlin Heidelberg, 2011.

[GMPS14] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. (Non-)Random Sequences from (Non-)Random Permutations - Analysis of RC4 Stream Cipher. *Journal of Cryptology*, 27(1):67–108, 2014.

[GPdM15] Christina Garman, Keneth G. Paterson, and Thyla Van der Merwe. Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS. In *USENIX Security Symposium 2015*, pages 113–128, 2015.

[GS16] Martin Gábris and Martin Stanek. State Recovery of RC4 and Spritz Revisited. *IACR Cryptology ePrint Archive*, 2016:337, 2016.

[HJMM08] Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The Grain Family of Stream Ciphers. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 179–190. Springer Berlin Heidelberg, 2008.

[HWF02] Russ Housley, Doug Whiting, and Niels Ferguson. *Alternate Temporal Key Hash.* doc.: IEEE 802.11-02/282r2, April 2002.

[IM14a] Ryoma Ito and Atsuko Miyaji. New Integrated Long-Term Glimpse of RC4. In Kyung-Hyune Rhee and Jeong Hyun Yi, editors, *Information Security Application - WISA 2014*, volume 8909 of *Lecture Notes in Computer Science*, pages 137–149. Springer Berlin Heidelberg, 2014.

[IM14b] Ryoma Ito and Atsuko Miyaji. New Negative Biases in Long-Term Glimpse of RC4. In *IEICE Japan Technical Report*, ISEC 2014, ISEC 2014-3, pages 13–19, 2014.

[IM15a] Ryoma Ito and Atsuko Miyaji. How TKIP Induces Biases of Internal States of RC4. In Emest Foo and Douglas Stebila, editors, *Information Security and Privacy - ACISP 2015*, volume 9144 of *Lecture Notes in Computer Science*, pages 329–342. Springer International Publishing, 2015.

[IM15b] Ryoma Ito and Atsuko Miyaji. New Linear Correlations on State Information of RC4 in WPA. In *The 32th Symposium on Cryptography and Information Security*, SCIS 2015 (2015-1). 2E2-3, 2015.

[IM15c] Ryoma Ito and Atsuko Miyaji. New Linear Correlations Related to State Information of RC4 PRGA Using IV in WPA. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 557–576. Springer Berlin Heidelberg, 2015.

[IM16a] Ryoma Ito and Atsuko Miyaji. Refined Glimpse Correlations of RC4. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(1):3–13, January 2016.

[IM16b] Ryoma Ito and Atsuko Miyaji. Refined RC4 Key Correlations of Internal States in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E99-A(6):1132–1144, June 2016.

[IM17] Ryoma Ito and Atsuko Miyaji. Refined Construction of RC4 Key Setting in WPA. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E100-A(1):138–148, January 2017.

[IM18a] Ryoma Ito and Atsuko Miyaji. New Iterated RC4 Key Correlations. In Willy Susilo and Guomin Yang, editors, *Information Security and Privacy - ACISP 2018*, volume 10946 of *Lecture Notes in Computer Science*, pages 154–171. Springer International Publishing, 2018.

[IM18b] Ryoma Ito and Atsuko Miyaji. On New Iterated Key Correlations of RC4. In *The 35th Symposium on Cryptography and Information Security*, SCIS 2018 (2018-1). 2B3-1, 2018.

[IM18c] Ryoma Ito and Atsuko Miyaji. Plaintext Recovery Attacks against WPA-TKIP Using Iterated RC4 Key Correlations. In *IEICE Japan Technical Report*, ISEC 2018, ISEC 2018-48, pages 379–386, 2018.

[IOWM13] Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Full Plaintext Recovery Attack on Broadcast RC4. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2013.

[IOWM14] Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii. Comprehensive Analysis of Initial Keystream Biases of RC4. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E97-A(1):139–151, January 2014.

[IPA] https://www.ipa.go.jp/security/fy28/reports/ishiki/index.html.

[Iso13] Takanori Isobe. *Analysis and Design of Symmetric Cryptographic Algorithms*. PhD thesis, Graduate School of Engineering, Kobe University, Japan, 2013.

[JBIO16] Sonu Jha, Subhadeep Banik, Takanori Isobe, and Toshihiro Ohigashi. Some Proofs of Joint Distributions of Keystream Biases in RC4. In Orr Dunkelman and Somitra Kumar Sanadhya, editors, *Progress in Cryptology - INDOCRYPT 2016*, volume 8424 of *Lecture Notes in Computer Science*, pages 305–321. Springer Berlin Heidelberg, 2016.

[Jen96] R. J. Jenkins. ISAAC and RC4. http://burtleburtle.net/bob/rand/isaac\.html, 1996.

[JM04] Antoine Joux and Frdric Muller. A Chosen IV Attack against Turing. In Mitsuru Matsui and Robert J. Zuccherato, editors, *Selected Areas in Cryptography - SAC 2004*, volume 3006 of *Lecture Notes in Computer Science*, pages 194–207. Springer Berlin Heidelberg, 2004.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC press, 2007.

[Kle08] Andreas Klein. Attacks on the RC4 Stream Cipher. *Designs, Codes and Cryptography*, 48(3):269–286, April 2008.

[KMP+98] Lars R. Knudsen, Willi Meier, Bart Preneel, Vincent Rijmen, and Sven Verdoolaege. Analysis Methods for (Alleged) RC4. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 327–341. Springer Berlin Heidelberg, 1998.

[LCM+16] A. Langley, W. Chang, N. Mavrogiannopoulos, J. Strombergson, and S. Josefsson. ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS). *Internet Engineering Task Force - IETF, Request for Comments*, 7905, June 2016.

[Mai16] Subhamoy Maitra. Chosen IV Cryptanalysis on Reduced Round ChaCha and Salsa. *Discrete Applied Mathematics*, 208:88–97, 2016.

[Man01] Itsik Mantin. Analysis of the Stream Cipher RC4. Master's thesis, The Weizmann Institute of Science, Israel, 2001. http://www.wisdom.weizmann.ac.il/ itsik/RC4/rc4.html.

[Man05] Itsik Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 491–506. Springer Berlin Heidelberg, 2005.

[Mat97] Mituru Matsui. New Block Encryption Algorithm MISTY. In *International Workshop on Fast Software Encryption – FSE 1997*, pages 54–68. Springer Berlin Heidelberg, 1997.

[MG13] Subhamoy Maitra and Sourav Sen Gupta. New Long-Term Glimpse of RC4 Stream Cipher. In Aditya Bagchi and Indrakshi Ray, editors, *Information Systems Security - ICISS 2013*, volume 8303 of *Lecture Notes in Computer Science*, pages 230–238. Springer Berlin Heidelberg, 2013.

[Mir02] Ilya Mironov. (Not So) Random Shuffles of RC4. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer Berlin Heidelberg, 2002.

[MOV96] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC press, 1996.

[MP08a] Subhamoy Maitra and Goutam Paul. Analysis of RC4 and Proposal of Additional Layers for Better Security Margin. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 27–39. Springer Berlin Heidelberg, 2008.

[MP08b] Subhamoy Maitra and Goutam Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In Kaisa Nyberg, editor, *Fast Software Encryption - FSE 2008*, volume 5086 of *Lecture Notes in Computer Science*, pages 253–269. Springer Berlin Heidelberg, 2008.

[MPG11] Subhamoy Maitra, Goutam Paul, and Sourav Sen Gupta. Attack on Broadcast RC4 Revisited. In Antoine Joux, editor, *Fast Software Encryption - FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 199–217. Springer Berlin Heidelberg, 2011.

[MPS$^+$13] Subhamoy Maitra, Goutam Paul, Santanu Sarkar, Michael Lehmann, and Willi Meier. New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. In Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013*, volume 7918 of *Lecture Notes in Computer Science*, pages 222–239. Springer Berlin Heidelberg, 2013.

[MS01] Itsik Mantin and Adi Shamir. Practical Attack on Broadcast RC4. In Mitsuru Matsui, editor, *Fast Software Encryption - FSE 2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 152–164. Springer Berlin Heidelberg, 2001.

[NGG05] Yassir Nawaz, Kishan Chand Gupta, and Guang Gong. A 32-Bit RC4-Like Keystream Generator. *IACR Cryptology ePrint Archive*, 2005:175, 2005.

[OIWM13] Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatsu Morii. How to Recover Any Byte of Plaintext on RC4. In Tanja Lange, Kristin Lauter, and Petr Lisonèk, editors, *Selected Areas in Cryptography - SAC 2013*, volume 8282 of *Lecture Notes in Computer Science*, pages 155–173. Springer Berlin Heidelberg, 2013.

[OIWM15] Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe, and Masakatsu Morii. Full Plaintext Recovery Attacks on RC4 Using Multiple Biases. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E98-A(1):81–91, January 2015.

[oS77] National Bureau of Standards. Data Encryption Standard. *National Bureau of Standards, US Department of Commerce, Washington D.C.*, January 1977.

[PM07] Goutam Paul and Subhamoy Maitra. Permutation After RC4 Key Scheduling Reveals the Secret Key. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected Areas in Cryptography - SAC 2007*, volume 4876 of *Lecture Notes in Computer Science*, pages 360–377. Springer Berlin Heidelberg, 2007.

[PM09] Goutam Paul and Subhamoy Maitra. On Biases of Permutation and Keystream Bytes of RC4 towards the Secret Key. *Cryptography and Communications*, 1:225–268, 2009.

[Pop15] Andrey Popov. Prohibiting RC4 Cipher Suites. *Internet Engineering Task Force - IETF, Request for Comments*, 7465, February 2015.

[PP04] Souradyuti Paul and Bart Preneel. A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. In Bimal Roy and Willi Meier, editors, *International Workshop on Fast Software Encryption - FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 245–259. Springer Berlin Heidelberg, 2004.

[PPS14] Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt. Plaintext Recovery Attacks Against WPA/TKIP. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 325–349. Springer Berlin Heidelberg, 2014.

[PS18] Kenneth G. Paterson and Jacob C. N. Schuldt. Statistical Attacks on Cookie Masking for RC4. *Cryptography and Communications*, 10(5):777–801, 2018.

[Roo95] Andrew Roos. A Class of Weak Keys in the RC4 Stream Cipher. `http://marcel.wanda.ch/Archive/WeakKeys`, 1995.

[RS14] Ronald L. Rivest and Jacob C. N. Schuldt. Spritz - A Spongy RC4-Like Stream Cipher and Hash Function. 2014.

[Sar14] Santanu Sarkar. Proving Empirically Key-Correlations in RC4. *Information Processing Letters*, 114 (5):234–238, 2014.

[Sar15] Santanu Sarkar. Further Non-Randomness in RC4, RC4A and VMPC. *Cryptography and Communications*, 7:317–330, 2015.

[SGPM15] Santanu Sarkar, Sourav Sen Gupta, Goutam Paul, and Subhamoy Maitra. Proving TLS-Attack Related Open Biases of RC4. *Designs, Codes and Cryptography*, 77(1):231–253, 2015.

[Soc04] IEEE Computer Society. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Standard 802.11i - 2004*, 2004.

[SOM03] Yoshiaki Shiraishi, Toshihiro Ohigashi, and Masakatu Morii. An Improved Internal-State Reconstruction Method of a Stream Cipher RC4. *Proceedings of Communication, Network, and Information Security, Track*, pages 440–488, 2003.

[SSL] https://www.trustworthyinternet.org/ssl-pulse/.

[SSVV13] Pouyan Sepehrdad, Petr Susil, Serge Vaudenay, and Martin Vuagnoux. Smashing WEP in a Passive Attack. In Shiho Moriai, editor, *Fast Software Encryption - FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 155–178. Springer Berlin Heidelberg, 2013.

[SV17] Santanu Sarkar and Ayineedi Venkateswarlu. Revisiting (Nested) Roos Bias in RC4 Key Scheduling Algorithm. *Designs, Codes and Cryptography*, 82(1-2):131–148, 2017.

[SVV10] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Discovery and Exploitation of New Biases in RC4. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography - SAC 2010*, volume 6544 of *Lecture Notes in Computer Science*, pages 74–91. Springer Berlin Heidelberg, 2010.

[SVV11] Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical Attack on RC4. In Kenneth G. Paterson, editor, *Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 343–363. Springer Berlin Heidelberg, 2011.

[TAO$^+$10] Ryoichi Teramura, Yasuo Asakura, Toshihiro Ohigashi, Hidenori Kuwakado, and Masakatsu Morii. Fast WEP-Key Recovery Attack Using Only Encrypted IP Packets. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E93-A(1):164–171, January 2010.

[TWP08] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 Bit WEP in Less Than 60 Seconds. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *Information Security Application - WISA 2007*, volume 4867 of *Lecture Notes in Computer Science*, pages 188–202. Springer Berlin Heidelberg, 2008.

[VP15] Mathy Vanhoef and Frank Piessens. All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS. In *USENIX Security Symposium 2015*, pages 97–112, 2015.

[VP16] Mathy Vanhoef and Frank Piessens. Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. In *USENIX Security Symposium 2016*, 2016.

[VSP17] Mathy Vanhoef, Domien Schepers, and Frank Piessens. Discovering Logical Vulnerabilities in the Wi-Fi Handshake Using Model-based Testing. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 360–371. ACM, 2017.

[VV07] Serge Vaudenay and Martin Vuagnoux. Passive – Only Key Recovery Attack on RC4. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected Areas in Cryptography - SAC 2007*, volume 4876 of *Lecture Notes in Computer Science*, pages 344–359. Springer Berlin Heidelberg, 2007.

[WIOM17] Yuhei Watanabe, Takanori Isobe, Toshihiro Ohigashi, and Masakatsu Morii. How to Efficiently Exploit Different Types of Biases for Plaintext Recovery of RC4. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 100(3):803–810, 2017.

[Wu08] Hongjun Wu. The Stream Cipher HC-128. In Matthew Robshaw and Olivier Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 39–47. Springer Berlin Heidelberg, 2008.

[Zol04] Bartosz Zoltak. VMPC One-Way Function and Stream Cipher. In Bimal Roy and Willi Meier, editors, *International Workshop on Fast Software Encryption - FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 210–225. Springer Berlin Heidelberg, 2004.

Appendix A

Newly Observed Key Correlations of State Variables

Table A.1: New key correlations by Equation (5.2) in generic RC4 and WPA-TKIP.

X_r	Key correlations	RC4	WPA-TKIP
$S_0[i_1]$	$-Z_1 + 1$	0.007584	0.007660
$(= j_1)$	$-Z_1 - K[0] + K[1] + 1$	0.003906	0.004847
	$-Z_1 + K[0] - K[1] + 1$	0.003907	0.004843
	$-K[0] - K[1] - K[2]$	0.005361	0.005360
	$-K[0] - K[1] - 3$	0.005336	0.008437
	$-K[0] - K[1] - 2$	0.002487	0.002605
	$-K[0] - K[1] - 1$	0.003901	0.002613
	$-K[0] - K[1]$	0.002469	0.002619
	$-K[0] - K[1] + 1$	0.005350	0.002600
	$-K[0] - K[1] + 2$	0.002498	0.002601
	$-K[0] - K[1] + 3$	0.005331	0.002605
	$-K[0] - 3$	0.003915	0.002481
	$-K[0] - 2$	0.003895	0.002461
	$-K[0] - 1$	0.003823	0.005254
	$-K[0]$	0.003897	0.002458
	$-K[0] + 1$	0.003918	0.002486
	$-K[0] + 2$	0.003902	0.005340
	$-K[0] + 3$	0.003293	0.002486
	$-K[0] + K[1] - 3$	0.005334	0.005240
	$-K[0] + K[1] - 2$	0.002480	0.002341
	$-K[0] + K[1] - 1$	0.005331	0.005229
	$-K[0] + K[1]$	0.002481	0.002677
	$-K[0] + K[1] + 1$	0.005340	0.005446
	$K[1] + 1$	0.006765	0.005756

X_r	Key correlations	RC4	WPA-TKIP
	$K[1] + 2$	0.002479	0.002884
	$K[0] - K[1] - 3$	0.005337	0.007848
	$K[0] - K[1] - 2$	0.002476	0.002061
	$K[0] - K[1] - 1$	0.003922	0.007877
	$K[0] - K[1]$	0.002485	0.002404
	$K[0] - K[1] + 1$	0.005324	0.002221
	$K[0] - K[1] + 2$	0.002493	0.002658
	$K[0] - K[1] + 3$	0.005333	0.002640
	$K[0] - 3$	0.003923	0.002499
	$K[0] - 2$	0.003920	0.002493
	$K[0] - 1$	0.003915	0.002494
	$K[0]$	0.001450	0
	$K[0] + 1$	0.003912	0.002464
	$K[0] + 2$	0.003915	0.002475
	$K[0] + 3$	0.003913	0.002471
	$K[0] + K[1] - 3$	0.002486	0.002356
	$K[0] + K[1] - 2$	0.002499	0.002339
	$K[0] + K[1] - 1$	0.002491	0.002337
	$K[0] + K[1] + 1$	0.365895	0.368730
	$K[0] + K[1] + 2$	0.002470	0.002309
	$K[0] + K[1] + 3$	0.002475	0.002291
	$K[0] + K[1] + K[2] + 3$	0.001492	0.001491
	$Z_1 - K[0] - K[1] - K[2] - 2$	0.005326	0.004753
$S_1[i_2]$	$-Z_2 - K[0] + K[1]$	0.003905	0.004957
	$-Z_2 - K[0] + K[1] + 2$	0.003906	0.004839
	$-Z_2 - K[1] + K[2] - 3$	0.005314	0.005327
	$-Z_2$	0.007768	0.007791
	$-Z_2 + 2$	0.007751	0.007749
	$-Z_2 + K[1] + K[2] + 3$	0.005317	0.005328
	$-Z_2 + K[0] - K[1]$	0.003907	0.004958
	$-Z_2 + K[0] - K[1] + 2$	0.003906	0.004839
	$-K[0] - K[1] - K[2] - 2$	0.002478	0.002464
	$-K[0] - K[1] - K[2] + 1$	0.005348	0.005351
	$-K[0] - K[1] - K[2] + 2$	0.002513	0.002499
	$-K[0] - K[1] - K[2] + 3$	0.005281	0.005290
	$-K[0] - K[1] + 3$	0.005329	0.004036
	$-K[0] - K[1] + K[2] - 3$	0.005307	0.002491
	$-K[0] - K[1] + K[2] - 2$	0.002513	0.002473
	$-K[0] - K[1] + K[2] - 1$	0.005305	0.008197
	$-K[0] - K[1] + K[2]$	0.002507	0.002499

X_r	Key correlations	RC4	WPA-TKIP
	$-K[0] - K[1] + K[2] + 1$	0.005317	0.002491
	$-K[0] - K[1] + K[2] + 2$	0.002512	0.002473
	$-K[0] - K[1] + K[2] + 3$	0.005305	0.002474
	$-K[0] - K[2] - 3$	0.003905	0.004635
	$-K[0] + K[2] - 3$	0.003908	0.002489
	$-K[0] + K[2] - 2$	0.003904	0.005311
	$-K[0] + K[2] - 1$	0.003905	0.002522
	$-K[0] + K[2]$	0.003904	0.002477
	$-K[0] + K[2] + 1$	0.003906	0.005326
	$-K[0] + K[2] + 2$	0.003903	0.002489
	$-K[0] + K[2] + 3$	0.003926	0.002504
	$-K[0] + K[1] - K[2] - 3$	0.005293	0.004616
	$-K[0] + K[1] - K[2] - 2$	0.002517	0.002486
	$-K[0] + K[1] - K[2] - 1$	0.005296	0.005885
	$-K[0] + K[1] - K[2]$	0.002515	0.002482
	$-K[0] + K[1] - K[2] + 1$	0.005301	0.005279
	$-K[0] + K[1] - K[2] + 2$	0.002519	0.002510
	$-K[0] + K[1] - K[2] + 3$	0.005300	0.005289
	$-K[0] + K[1] + 1$	0.003905	0.005001
	$-K[0] + K[1] + K[2] - 3$	0.005308	0.005322
	$-K[0] + K[1] + K[2] - 2$	0.002506	0.002489
	$-K[0] + K[1] + K[2] - 1$	0.005305	0.005333
	$-K[0] + K[1] + K[2]$	0.002506	0.002488
	$-K[0] + K[1] + K[2] + 1$	0.005306	0.005326
	$-K[0] + K[1] + K[2] + 2$	0.002510	0.002492
	$-K[0] + K[1] + K[2] + 3$	0.005310	0.004261
	$-K[1] - K[2] - 3$	0.006748	0.006767
	$-K[2] - 3$	0.003903	0.004966
	$-K[2] - 2$	0.003899	0.002481
	$-K[2] - 1$	0.006127	0.007571
	$-K[2]$	0.003896	0.002477
	$-K[2] + 1$	0.003915	0.005308
	$-K[2] + 2$	0.003888	0.002487
	$-K[2] + 3$	0.003904	0.005306
	$K[2] - 3$	0.003910	0.005309
	$K[2] - 2$	0.003899	0.002486
	$K[2] - 1$	0.003910	0.005321
	$K[2]$	0.003900	0.002475
	$K[2] + 1$	0.003909	0.005331
	$K[2] + 2$	0.003906	0.002479

X_r	Key correlations	RC4	WPA-TKIP
	$K[2]+3$	0.006219	0.003886
	$K[1]+K[2]+3$	0.008157	0.008172
	$K[0]-K[1]-K[2]-2$	0.002503	0.002488
	$K[0]-K[1]-K[2]-1$	0.005309	0.005895
	$K[0]-K[1]-K[2]$	0.002518	0.002495
	$K[0]-K[1]-K[2]+1$	0.005302	0.005314
	$K[0]-K[1]-K[2]+2$	0.002517	0.002501
	$K[0]-K[1]-K[2]+3$	0.005308	0.005318
	$K[0]-K[1]+2$	0.003918	0.004707
	$K[0]-K[1]+K[2]-3$	0.005295	0.008163
	$K[0]-K[1]+K[2]-2$	0.002517	0.002497
	$K[0]-K[1]+K[2]-1$	0.005290	0.008171
	$K[0]-K[1]+K[2]$	0.002524	0.002497
	$K[0]-K[1]+K[2]+1$	0.005309	0.008171
	$K[0]-K[1]+K[2]+2$	0.002518	0.002500
	$K[0]-K[1]+K[2]+3$	0.005310	0.002838
	$K[0]+K[2]-3$	0.003908	0.002491
	$K[0]+K[2]-2$	0.003905	0.002480
	$K[0]+K[2]-1$	0.003912	0.002496
	$K[0]+K[2]$	0.003902	0.002479
	$K[0]+K[2]+1$	0.003918	0.002497
	$K[0]+K[2]+2$	0.003903	0.002475
	$K[0]+K[2]+3$	0.003914	0.002835
	$K[0]+K[1]-K[2]-3$	0.005312	0.005340
	$K[0]+K[1]-K[2]-2$	0.002493	0.002484
	$K[0]+K[1]-K[2]$	0.002511	0.002485
	$K[0]+K[1]-K[2]+1$	0.005291	0.005295
	$K[0]+K[1]-K[2]+2$	0.002517	0.002489
	$K[0]+K[1]-K[2]+3$	0.005304	0.005309
	$K[0]+K[1]+K[2]-3$	0.002500	0.002495
	$K[0]+K[1]+K[2]-2$	0.002502	0.002491
	$K[0]+K[1]+K[2]-1$	0.002507	0.002503
	$K[0]+K[1]+K[2]$	0.002505	0.002493
	$K[0]+K[1]+K[2]+3$	0.360357	0.361718
	$Z_2-K[1]-K[2]-3$	0.005323	0.005333
	$Z_2+K[1]+K[2]+3$	0.005322	0.005332
$S_2[i_3]$	$-Z_3-K[0]+K[1]+3$	0.003906	0.004878
	$-Z_3+3$	0.007825	0.007819
	$-Z_3+K[0]-K[1]+3$	0.003907	0.004877
	$-K[0]-K[1]+2$	0.005335	0.005539

X_r	Key correlations	RC4	WPA-TKIP
	$-K[0]+K[1]+3$	0.003901	0.004983
	$K[0]-K[1]+3$	0.003888	0.004690
$S_3[i_4]$	$-K[0]-K[1]-K[2]$	0.005324	0.005325
	$-K[0]-K[1]+3$	0.006721	0.005513
	$-K[0]+K[1]+2$	0.003900	0.004975
$S_{28}[i_{29}]$	$-Z_{29}-K[0]+K[1]-3$	0.003906	0.004861
$S_{29}[i_{30}]$	$-Z_{30}-K[0]+K[1]-2$	0.003906	0.004863
$S_{30}[i_{31}]$	$-Z_{31}-K[0]+K[1]-1$	0.003907	0.004863
$S_{31}[i_{32}]$	$-Z_{32}-K[0]+K[1]$	0.003906	0.004862
	$-K[0]+K[1]$	0.003911	0.004784
	$K[1]+2$	0.003924	0.004674
$S_{32}[i_{33}]$	$-Z_{33}-K[0]+K[1]+1$	0.003907	0.004860
	$-K[0]+K[1]+1$	0.003997	0.005974
	$K[1]+1$	0.003900	0.005814
$S_{33}[i_{34}]$	$-Z_{34}-K[0]+K[1]+2$	0.003906	0.004860
	$-K[0]+K[1]+2$	0.003905	0.005890
$S_{34}[i_{35}]$	$-Z_{35}-K[0]+K[1]+3$	0.003907	0.004863
	$-K[0]+K[1]+3$	0.003905	0.004607
	$K[0]+K[1]$	0.003915	0.005239
$S_{36}[i_{37}]$	$K[1]+3$	0.003906	0.005737
$S_{54}[i_{55}]$	$-K[0]+2$	0.003894	0.005066
$S_{65}[i_{66}]$	$K[0]+K[1]+K[2]+2$	0.004975	0.004952
$S_{92}[i_{93}]$	$-Z_{93}+K[0]-K[1]-3$	0.003904	0.004877
	$K[0]-K[1]-3$	0.003897	0.005208
$S_{93}[i_{94}]$	$-Z_{94}+K[0]-K[1]-2$	0.003906	0.004877
$S_{94}[i_{95}]$	$-Z_{95}+K[0]-K[1]-1$	0.003907	0.004875
	$K[0]-K[1]-1$	0.003903	0.005201
$S_{95}[i_{96}]$	$-Z_{96}+K[0]-K[1]$	0.003906	0.004878
$S_{96}[i_{97}]$	$-Z_{97}+K[0]-K[1]+1$	0.003906	0.004875
$S_{97}[i_{98}]$	$-Z_{98}+K[0]-K[1]+2$	0.003906	0.004875
$S_{98}[i_{99}]$	$-Z_{99}+K[0]-K[1]+3$	0.003906	0.004876
$S_{120}[i_{121}]$	$K[1]-3$	0.003906	0.004723
$S_{122}[i_{123}]$	$K[1]-2$	0.003906	0.004703
$S_{124}[i_{125}]$	$-Z_{125}-K[0]+K[1]-3$	0.003908	0.004874
	$-Z_{125}+K[0]+K[1]-3$	0.003906	0.004872
	$-K[0]+K[1]-3$	0.003900	0.005076
	$K[1]-1$	0.003906	0.004682
	$K[0]-K[1]-3$	0.003900	0.004927
$S_{125}[i_{126}]$	$-Z_{126}-K[0]+K[1]-2$	0.003907	0.004876

X_r	Key correlations	RC4	WPA-TKIP
	$-Z_{126} + K[0] - K[1] - 2$	0.003907	0.004876
$S_{126}[i_{127}]$	$-Z_{127} - K[0] + K[1] - 1$	0.003906	0.004874
	$-Z_{127} + K[0] - K[1] - 1$	0.003906	0.004876
	$-K[0] - K[1] - 3$	0.004765	0.005734
	$-K[0] + K[1] - 1$	0.003898	0.005069
	$K[0] - K[1] - 1$	0.003901	0.004923
$S_{127}[i_{128}]$	$-Z_{128} - K[0] + K[1]$	0.003908	0.004875
	$-Z_{128} + K[0] - K[1]$	0.003907	0.004876
$S_{128}[i_{129}]$	$-Z_{129} - K[0] + K[1] + 1$	0.003906	0.004875
	$-Z_{129} + K[0] - K[1] + 1$	0.003907	0.004875
	$K[1] + 1$	0.004672	0.005886
$S_{129}[i_{130}]$	$-Z_{130} - K[0] + K[1] + 2$	0.003906	0.004875
	$-Z_{130} + K[0] - K[1] + 2$	0.003906	0.004876
	$K[2] + 3$	0.004671	0.004678
$S_{130}[i_{131}]$	$-Z_{131} - K[0] + K[1] + 3$	0.003903	0.004876
	$-Z_{131} + K[0] - K[1] + 3$	0.003906	0.004875
$S_{156}[i_{157}]$	$-Z_{157} - K[0] + K[1] - 3$	0.003904	0.004876
$S_{157}[i_{158}]$	$-Z_{158} - K[0] + K[1] - 2$	0.003906	0.004877
$S_{158}[i_{159}]$	$-Z_{159} - K[0] + K[1] - 1$	0.003906	0.004875
$S_{159}[i_{160}]$	$-Z_{160} - K[0] + K[1]$	0.003906	0.004876
$S_{160}[i_{161}]$	$-Z_{161} - K[0] + K[1] + 1$	0.003906	0.004876
	$-K[0] + K[1] + 1$	0.003898	0.004825
$S_{161}[i_{162}]$	$-Z_{162} - K[0] + K[1] + 2$	0.003907	0.004875
$S_{162}[i_{163}]$	$-Z_{163} - K[0] + K[1] + 3$	0.003907	0.004874
	$-K[0] + K[1] + 3$	0.003901	0.004835
$S_{182}[i_{183}]$	$-K[0] + 2$	0.003902	0.004601
$S_{220}[i_{221}]$	$-Z_{221} + K[0] - K[1] - 3$	0.003907	0.004860
	$K[0] - K[1] - 3$	0.003902	0.004670
$S_{221}[i_{222}]$	$-Z_{222} + K[0] - K[1] - 2$	0.003907	0.004858
$S_{222}[i_{223}]$	$-Z_{223} + K[0] - K[1] - 1$	0.003906	0.004861
	$K[0] - K[1] - 1$	0.003904	0.004671
$S_{223}[i_{224}]$	$-Z_{224} + K[0] - K[1]$	0.003907	0.004859
$S_{224}[i_{225}]$	$-Z_{225} + K[0] - K[1] + 1$	0.003908	0.004861
$S_{225}[i_{226}]$	$-Z_{226} + K[0] - K[1] + 2$	0.003907	0.004861
$S_{226}[i_{227}]$	$-Z_{227} + K[0] - K[1] + 3$	0.003907	0.004859
$S_{252}[i_{253}]$	$-Z_{253} - K[0] + K[1] - 3$	0.003907	0.004876
	$-Z_{253} - 3$	0.007813	0.007815
	$-Z_{253} + K[0] - K[1] - 3$	0.003906	0.004875
$S_{253}[i_{254}]$	$-Z_{254} - K[0] + K[1] - 2$	0.003906	0.004875

X_r	Key correlations	RC4	WPA-TKIP
	$-Z_{254} - 2$	0.007814	0.007812
	$-Z_{254} + K[0] - K[1] - 2$	0.003906	0.004875
$S_{254}[i_{255}]$	$-Z_{255} - K[0] + K[1] - 1$	0.003905	0.004875
	$-Z_{255} - 1$	0.007816	0.007815
	$-Z_{255} + K[0] - K[1] - 1$	0.003905	0.004876
	$-K[0] - K[1] - 3$	0.004430	0.004985
$S_{255}[i_{256}]$	$-Z_{256} - K[0] + K[1]$	0.003908	0.004875
	$-Z_{256}$	0.007861	0.007810
	$-Z_{256} + K[0] - K[1]$	0.003909	0.004875
	$K[0]$	0.137294	0.138047
	$K[1]$	0.003911	0.037189
$S_r[i_{r+1}]$ $(0 \leq r \leq N)$	$-K[0] - 1$	Figure A.1	
	$-K[1] - 1$	Figure A.2	
	$-K[2] - 1$	Figure A.3	
	$K[0]$	Figure A.4	
	$K[0] + K[1] + 1$	Figure 5.1	
$S_0[j_1]$	$-Z_1 + K[0] + K[1] + 1$	0.005330	0.005280
	$-K[0] - K[1] - 3$	0.004339	0.005513
	$-K[0] - K[1] + 1$	0.005791	0.003417
	$K[1] + 1$	0.004933	0.004597
	$K[0] - K[1] - 3$	0.004403	0.005342
	$K[0] - K[1] - 1$	0.004431	0.005346
	$K[0]$	0.002889	0.001898
	$K[0] + K[1] + 1$	0.135738	0.134820
	$K[0] + K[1] + K[2] + 3$	0.002385	0.002441
	$Z_1 - K[0] - K[1] - K[2] - 2$	0.005295	0.004726
	$Z_1 - K[0] - K[1] - 1$	0.005188	0.005115
$S_1[j_2]$	$-Z_2 + K[0] + K[1] + 1$	0.005316	0.005335
	$-K[0] - K[1] + 1$	0.005318	0.005408
	$Z_2 - K[0] - K[1] - K[2] - 3$	0.005686	0.005694
	$Z_2 + K[0] + K[1] + 1$	0.005321	0.005344
j_2	$-Z_2 + K[0] + K[1] + 1$	0.005318	0.005336
	$-Z_2 + K[0] + K[1] + 3$	0.005302	0.005310
	$-K[0] - K[1] - K[2] + 2$	0.005333	0.005856
	$-K[0] - K[1] + K[2] - 2$	0.003921	0.004574
	$-K[0] - K[1] + K[2]$	0.003919	0.005573
	$-K[0] - K[1] + K[2] + 2$	0.003912	0.004545
	$-K[0] + K[1] + K[2]$	0.003921	0.005501
	$-K[1] + K[2] - 2$	0.003911	0.005479

X_r	Key correlations	RC4	WPA-TKIP
	$-K[1]+K[2]+3$	0.003899	0.005476
	$K[2]$	0.004428	0.005571
	$K[0]-K[1]+K[2]$	0.003918	0.005618
	$K[0]-K[2]-2$	0.004951	0.004974
	$K[0]+K[1]-K[2]$	0.004397	0.004923
	$K[0]+K[1]+3$	0.005309	0.003889
t_1	$-Z_1-K[0]-K[1]+1$	0.005251	0.005333
	$-K[0]-K[1]+2$	0.005310	0.003902
	$K[0]$	0.005291	0.004806
	$Z_1-K[0]-K[1]-K[2]-1$	0.006639	0.006094
t_2	$-Z_2-K[0]-K[1]-K[2]+1$	0.005301	0.005306
	$-Z_2+K[0]+K[1]+1$	0.005339	0.005341
	$K[0]+K[1]+1$	0.005317	0.005349
t_3	$K[0]+K[1]+K[2]+3$	0.005297	0.005310
t_r	$-Z_r+K[0]$	Figure A.5	
$(1 \leq r \leq N)$	$Z_r-K[0]$	Figure A.6	
	Z_r	Figure A.7	
	$Z_r+K[0]+K[1]+1$	Figure A.8	

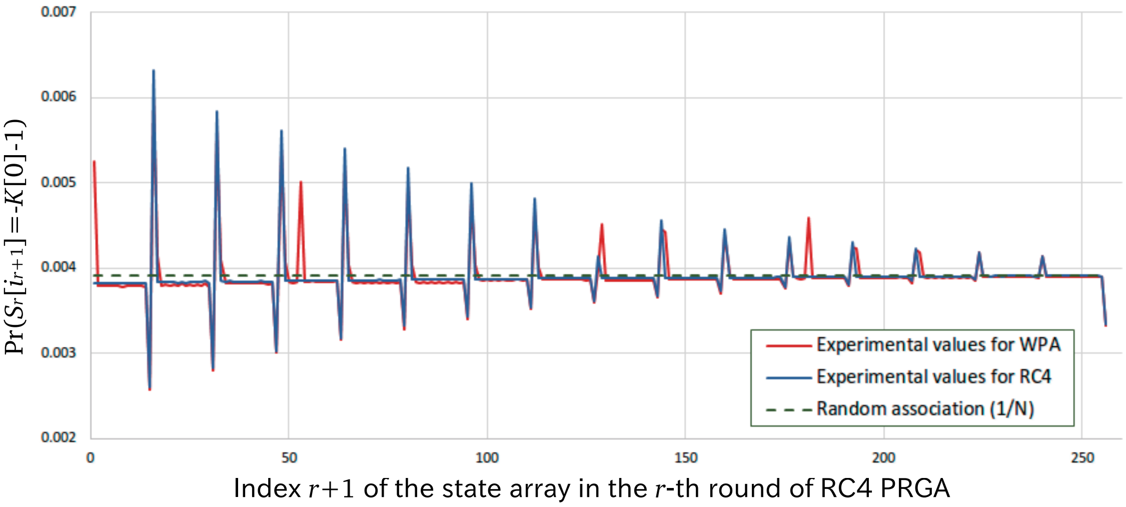

Figure A.1: Observation of the event $(S_r[i_{r+1}] = -K[0] + 1)$.

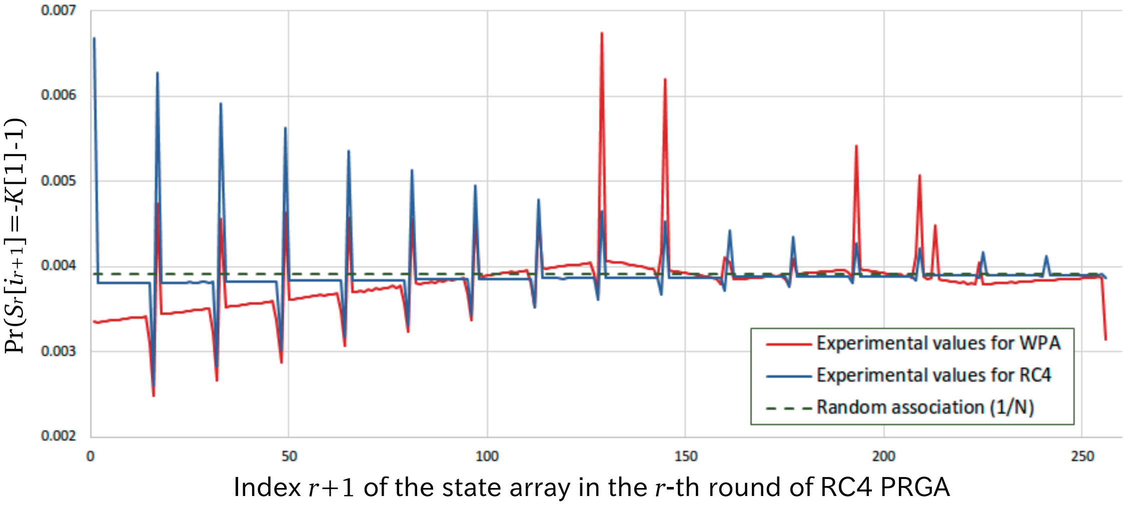

Figure A.2: Observation of the event $(S_r[i_{r+1}] = -K[1] + 1)$.

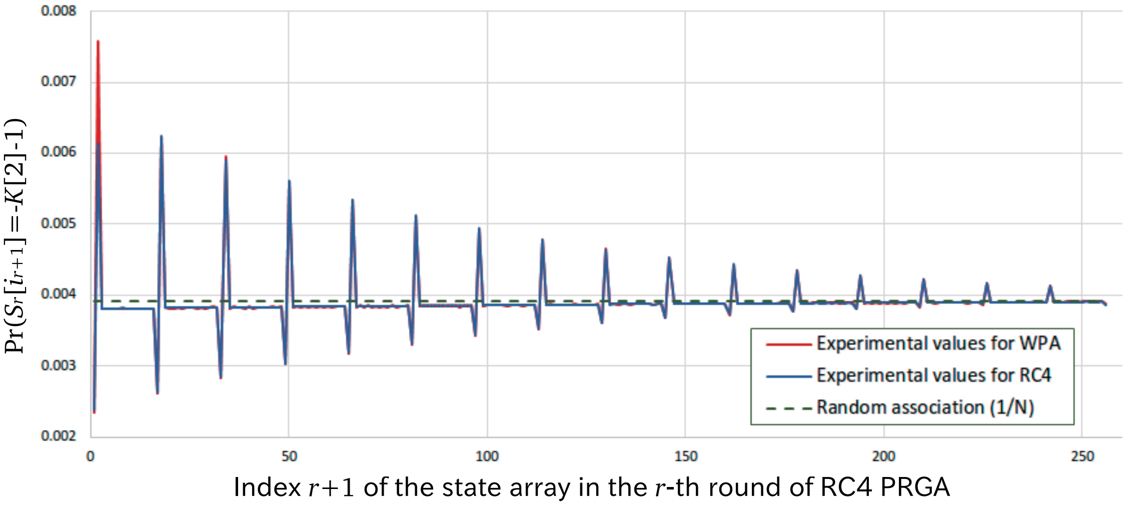

Figure A.3: Observation of the event $(S_r[i_{r+1}] = -K[2] + 1)$.

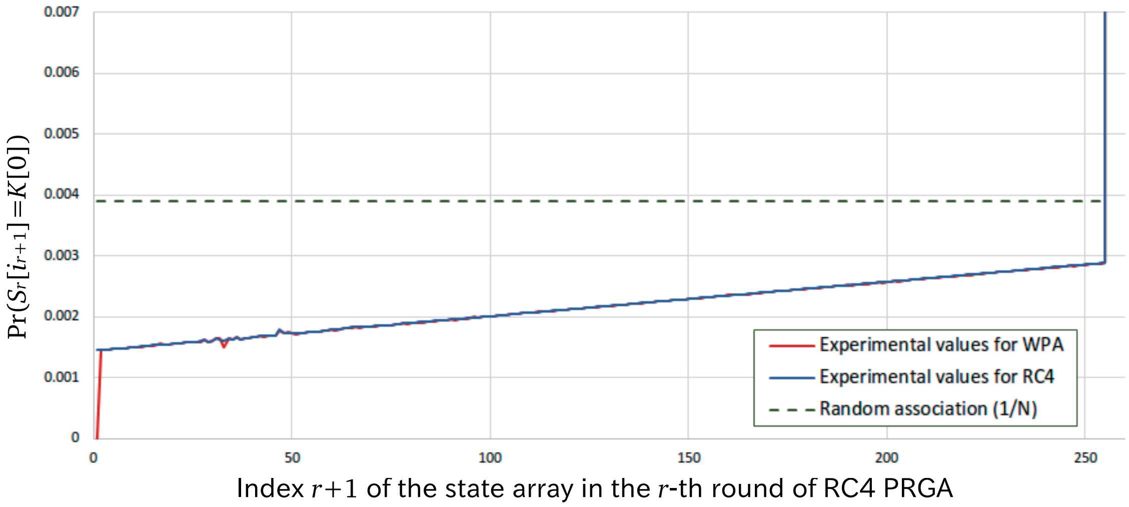

Figure A.4: Observation of the event $(S_r[i_{r+1}] = K[0])$.

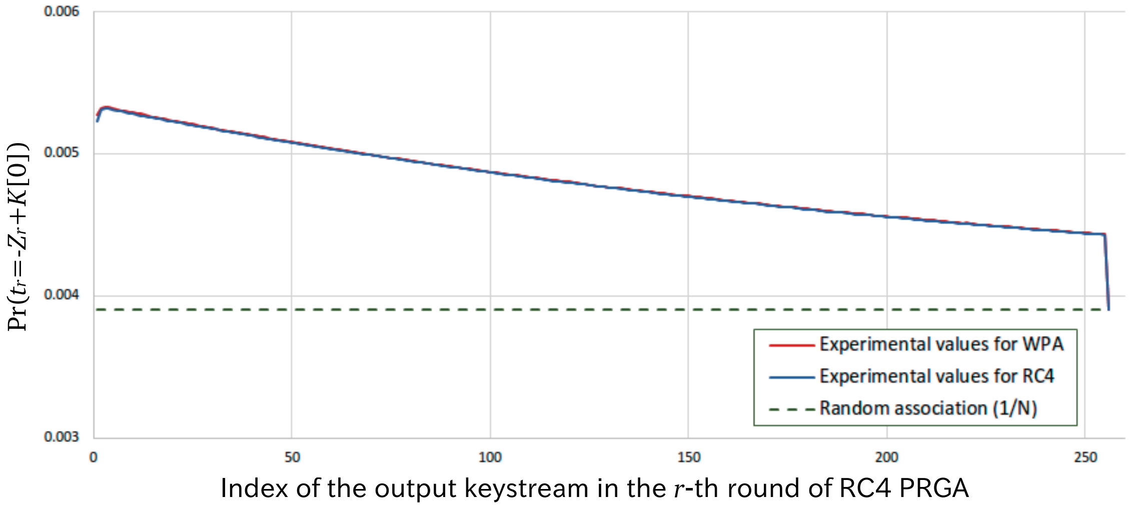

Figure A.5: Observation of the event $(t_r = -Z_r + K[0])$.

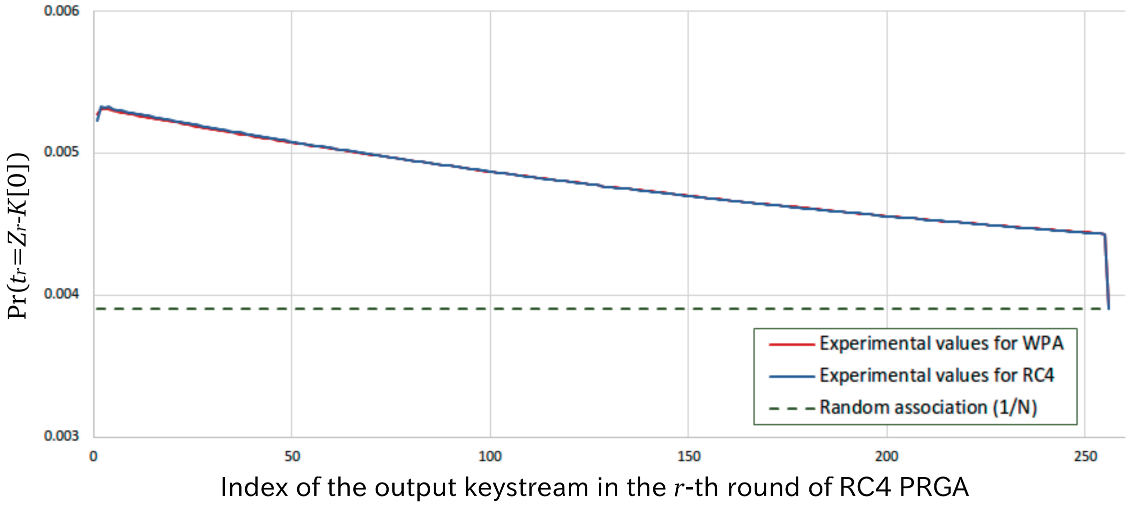

Figure A.6: Observation of the event $(t_r = Z_r - K[0])$.

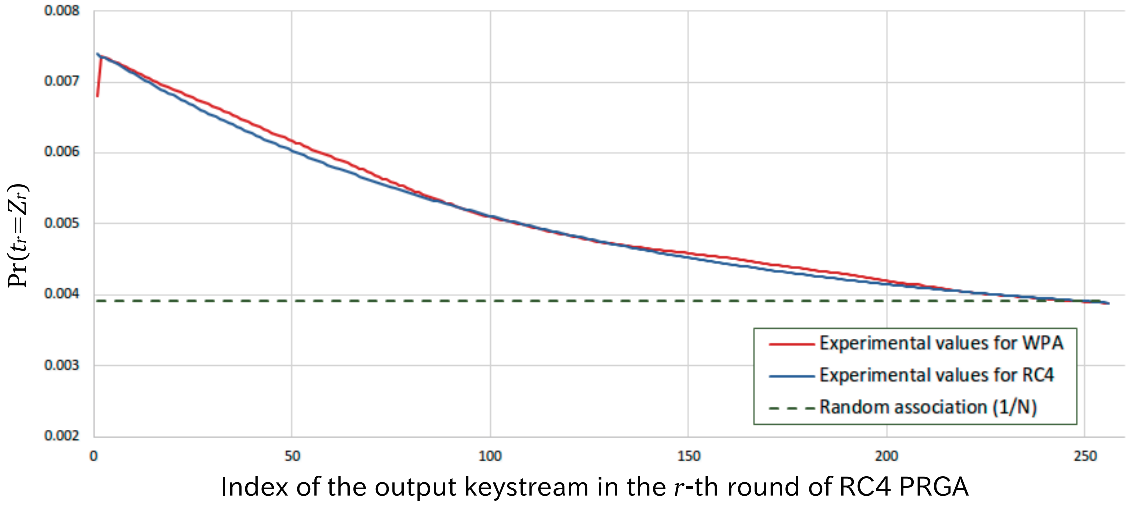

Figure A.7: Observation of the event $(t_r = Z_r)$.

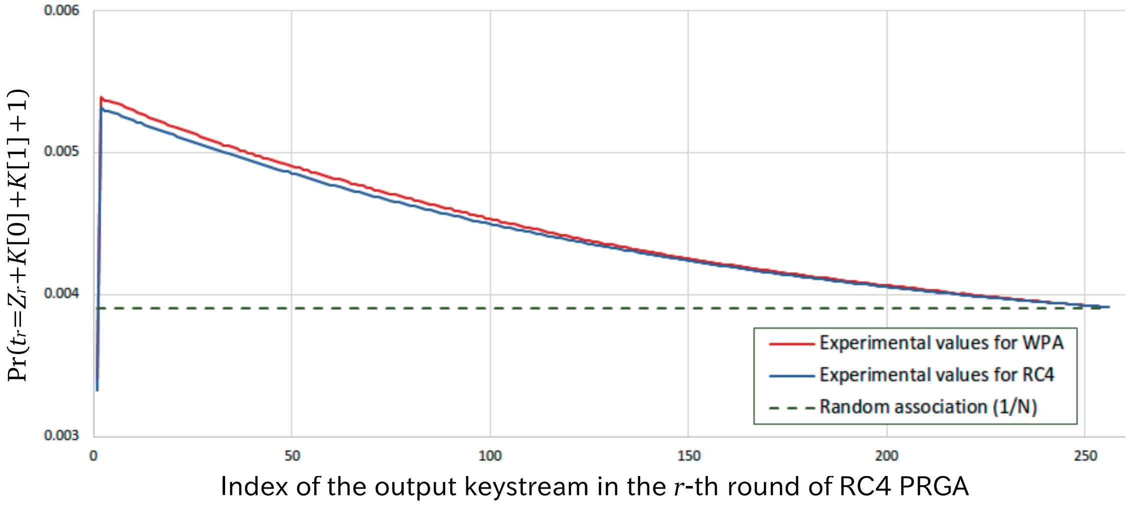

Figure A.8: Observation of the event $(t_r = Z_r + K[0] + K[1] + 1)$.

Appendix B

Number of Correlations Induced by the Refined Key Setting

Table B.1: Number of correlations induced by the refined RC4 key settings.

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
0	1	2	22	368	13	28	462	893	reference value (TKIP)
	2	4	9	208	2	9	398	626	29.899
	3	6	10	205	2	6	399	622	30.347
	4	8	7	204	2	6	398	617	30.907
	5	10	7	206	2	6	396	617	30.907
	6	12	7	206	2	6	396	617	30.907
	7	14	7	203	2	6	398	616	31.019
	8	0	22	424	5	15	952	1418	-58.791
	9	2	10	206	2	8	400	626	29.899
	10	4	7	205	2	6	395	615	31.131
	11	6	7	204	2	6	398	617	30.907
	12	8	7	205	2	6	397	617	30.907
	13	10	7	202	2	5	400	616	31.019
	14	12	7	204	2	6	309	618	30.795
	15	14	7	205	2	6	401	621	30.459
1	2	3	5	107	4	7	161	284	68.197
	3	5	3	107	4	7	160	281	68.533
	4	7	3	107	4	7	158	279	68.757
	5	9	3	107	4	7	160	281	68.533
	6	11	3	107	4	7	160	281	68.533
	7	13	3	107	4	7	159	280	68.645
	8	15	3	107	4	7	161	281	68.533
	9	1	7	226	9	19	479	740	17.133

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
1	10	3	3	106	4	7	159	279	68.757
	11	5	3	106	4	7	161	281	68.533
	12	7	3	106	4	7	160	280	68.645
	13	9	3	106	4	7	160	280	68.645
	14	11	4	106	4	7	159	280	68.645
	15	13	3	108	4	7	160	282	68.421
	0	15	15	326	12	18	476	847	5.151
2	3	4	5	105	2	5	161	278	68.869
	4	6	5	107	2	5	161	280	68.645
	5	8	5	107	2	5	160	279	68.757
	6	10	5	107	2	5	161	280	68.654
	7	12	5	107	2	5	160	279	68.757
	8	14	5	107	2	5	162	281	68.533
	9	0	11	208	2	8	399	628	29.675
	10	2	13	226	5	13	475	732	18.029
	11	4	5	106	2	5	160	279	68.757
	12	6	5	106	2	5	160	278	68.869
	13	8	5	106	2	5	160	278	68.869
	14	10	6	106	2	5	162	281	68.533
	15	12	5	107	2	5	160	279	68.757
	0	14	9	205	2	8	413	637	28.667
	1	0	23	270	14	34	458	779	12.766
3	4	5	3	102	2	5	162	274	69.317
	5	7	3	105	2	5	162	277	68.981
	6	9	3	105	2	5	160	275	69.205
	7	11	3	105	2	5	161	276	69.093
	8	13	3	105	2	5	163	278	68.869
	9	15	3	104	2	5	161	275	69.205
	10	1	3	105	4	7	160	279	68.757
	11	3	7	218	5	13	475	718	19.484
	12	5	3	104	2	5	162	276	69.093
	13	7	3	104	2	5	162	276	69.093
	14	9	3	104	2	5	163	277	68.981
	15	11	3	106	2	5	161	277	68.981
	0	13	10	202	2	6	411	631	29.339
	1	15	3	107	2	7	160	279	68.757
	2	1	9	115	4	8	162	298	66.629
4	5	6	3	104	2	5	160	274	69.317
	6	8	3	105	2	5	159	274	69.317

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
4	7	10	3	105	2	5	158	273	69.429
	8	12	3	105	2	5	162	277	68.981
	9	14	3	104	2	5	162	276	69.093
	10	0	9	205	2	6	400	622	30.347
	11	2	6	105	2	5	162	280	68.654
	12	4	7	218	5	13	475	718	19.484
	13	6	3	104	2	5	159	273	69.429
	14	8	3	104	2	5	162	276	69.093
	15	10	3	105	2	5	158	276	69.093
	0	12	7	202	2	6	288	629	29.563
	1	14	3	107	2	7	159	281	68.533
	2	0	11	209	2	9	400	631	29.399
	3	2	6	105	2	5	163	281	68.533
5	6	7	3	105	2	5	162	277	68.981
	7	9	3	106	2	5	160	276	69.093
	8	11	3	106	2	5	160	276	69.093
	9	13	4	105	2	5	161	277	68.981
	10	15	3	105	2	5	162	277	68.981
	11	1	3	106	4	7	159	279	68.757
	12	3	3	105	2	5	161	276	69.093
	13	5	7	220	5	13	478	723	19.037
	14	7	3	105	2	5	161	276	69.093
	15	9	3	106	2	5	161	277	68.981
	0	11	8	203	2	6	412	631	29.339
	1	13	3	108	2	7	161	281	68.533
	2	15	5	108	2	6	162	283	68.309
	3	1	3	107	4	7	159	280	68.465
	4	3	3	106	2	5	161	277	68.981
6	7	8	4	104	2	5	159	274	69.317
	8	10	3	106	2	5	161	277	68.981
	9	12	3	105	2	5	169	274	69.317
	10	14	3	105	2	5	161	277	68.981
	11	0	9	206	2	5	400	623	30.235
	12	2	6	106	2	5	162	281	68.533
	13	4	3	105	2	5	161	276	69.093
	14	6	7	220	5	13	472	717	19.709
	15	8	3	106	2	5	158	274	69.317
	0	10	7	202	2	6	411	628	29.675
	1	12	3	108	2	7	159	279	68.757

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
6	2	14	5	108	2	6	159	280	68.654
	3	0	11	206	2	6	397	622	30.347
	4	2	6	107	2	5	162	282	68.421
	5	4	3	106	2	5	161	277	68.981
7	8	9	3	103	2	5	162	275	69.205
	9	11	3	104	2	5	160	274	69.317
	10	13	3	104	2	5	161	275	69.205
	11	15	3	104	2	5	162	276	69.093
	12	1	3	105	4	7	161	280	68.645
	13	3	3	104	2	5	159	276	69.093
	14	5	3	104	2	5	161	275	69.205
	15	7	7	220	5	13	478	723	19.037
	0	9	7	202	2	6	415	632	29.227
	1	11	3	107	2	7	160	279	68.757
	2	13	5	107	2	6	160	280	68.465
	3	15	4	105	2	5	161	277	68.981
	4	1	3	106	4	7	162	282	68.421
	5	3	3	105	2	5	160	275	69.093
	6	5	3	106	2	5	159	275	69.093
8	9	10	3	103	2	5	160	273	69.429
	10	12	3	104	2	5	162	276	69.093
	11	14	3	104	2	5	162	276	69.093
	12	0	9	205	2	6	399	621	30.459
	13	2	6	105	2	5	160	278	68.869
	14	4	3	104	2	5	161	275	69.205
	15	6	3	105	2	5	161	276	69.093
	0	8	19	510	5	16	1234	1784	-99.776
	1	10	4	107	2	6	160	281	68.533
	2	12	5	107	2	6	160	280	68.465
	3	14	3	105	2	5	161	276	69.093
	4	0	9	206	2	6	398	621	30.459
	5	2	6	106	2	5	161	280	68.465
	6	4	3	105	2	5	161	276	69.093
	7	6	3	106	2	5	163	279	68.757
9	10	11	3	103	2	5	158	271	69.653
	11	13	3	104	2	5	161	275	69.205
	12	15	3	104	2	5	162	276	69.093
	13	1	3	105	4	7	162	281	68.533
	14	3	3	104	2	5	161	275	69.205

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
9	15	5	3	105	2	5	161	276	69.093
	0	7	7	201	2	5	412	628	29.675
	1	9	7	230	5	19	471	732	18.029
	2	11	5	107	2	6	160	280	68.465
	3	13	3	105	2	5	163	278	68.869
	4	15	3	105	2	5	162	277	68.981
	5	1	3	106	4	7	161	281	68.533
	6	3	3	105	2	5	162	277	68.981
	7	5	3	105	2	5	161	276	69.093
	8	7	3	104	2	5	161	275	69.205
10	11	12	3	104	2	5	159	273	69.429
	12	14	3	104	2	5	160	274	69.317
	13	0	9	205	2	6	398	620	30.571
	14	2	6	105	2	5	160	278	68.869
	15	4	3	105	2	5	160	275	69.205
	0	6	8	202	2	6	415	633	29.115
	1	8	3	107	2	7	159	278	68.869
	2	10	13	228	5	16	476	738	17.357
	3	12	3	105	2	5	162	277	68.981
	4	14	3	105	2	5	162	277	68.981
	5	0	9	205	2	6	399	621	30.459
	6	2	6	106	2	5	161	280	68.465
	7	4	3	105	2	5	161	276	69.093
	8	6	3	105	2	5	161	276	69.093
	9	8	3	104	2	5	161	275	69.205
11	12	13	3	103	2	5	161	274	69.317
	13	15	3	104	2	5	160	274	69.317
	14	1	3	105	4	8	161	281	68.533
	15	3	3	105	2	5	161	276	69.093
	0	5	7	202	2	6	411	628	29.675
	1	7	3	107	2	7	160	279	68.757
	2	9	5	107	2	6	162	282	68.421
	3	11	7	221	5	13	475	721	19.261
	4	13	3	105	2	5	160	276	69.093
	5	15	3	105	2	5	162	277	68.981
	6	1	3	106	4	7	162	282	68.421
	7	3	4	105	2	5	162	278	68.869
	8	5	3	105	2	5	160	275	69.205
	9	7	3	104	2	5	160	274	69.317

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
11	10	9	3	104	2	5	162	276	69.093
12	13	14	3	103	2	5	160	273	69.429
	14	0	9	205	2	6	400	622	30.347
	15	2	6	106	2	5	160	279	68.757
	0	4	7	202	2	6	412	629	29.563
	1	6	3	107	2	7	159	278	68.869
	2	8	5	107	2	5	160	280	68.645
	3	10	4	105	2	5	161	277	68.981
	4	12	7	221	5	13	476	722	19.149
	5	14	3	105	2	5	160	275	69.205
	6	0	9	206	2	6	398	621	30.459
	7	2	7	106	2	5	159	279	68,757
	8	4	3	105	2	5	162	277	68.981
	9	6	3	104	2	5	159	273	69.429
	10	8	3	104	2	5	159	273	69.429
	11	10	3	104	2	5	162	276	69.093
13	14	15	3	103	2	5	161	274	69.317
	15	1	3	106	4	7	162	282	68.421
	0	3	10	202	2	6	415	635	28.891
	1	5	3	107	2	7	160	279	68.757
	2	7	5	107	2	6	159	279	68.757
	3	9	4	105	3	5	161	278	68.869
	4	11	3	105	2	5	163	278	68.869
	5	13	5	221	5	24	481	730	18.253
	6	15	3	105	2	5	159	274	69.317
	7	1	3	106	4	7	159	279	68.757
	8	3	3	104	2	5	160	274	69.317
	9	5	3	104	2	5	162	276	69.093
	10	7	3	104	2	5	159	273	69.429
	11	9	3	104	2	5	161	275	69.205
	12	11	3	104	2	5	162	276	69.093
14	15	0	9	206	2	6	396	619	30.683
	0	2	11	201	2	7	413	634	29.003
	1	4	4	106	2	5	159	276	69.093
	2	6	5	107	2	5	161	280	68.645
	3	8	3	105	2	5	161	276	69.093
	4	10	3	105	2	5	161	276	69.093
	5	12	3	104	2	5	158	272	69.541
	6	14	7	219	5	13	478	722	19.149

x	y	z	# of Correlations						
			Z_{r+1}	$S_r[i_{r+1}]$	$S_r[j_{r+1}]$	j_{r+1}	t_{r+1}	total	reduction rate (%)
14	7	0	9	206	2	6	398	621	30.459
	8	2	6	104	2	5	162	279	68.757
	9	4	3	104	2	5	161	275	69.205
	10	6	3	104	2	5	162	276	69.093
	11	8	3	104	2	5	161	275	69.205
	12	10	3	104	2	5	160	274	69.317
	13	12	3	103	2	5	160	273	69.429
15	0	1	14	226	13	30	472	755	15.454
	1	3	3	106	2	7	159	277	68.981
	2	5	5	106	2	6	160	279	68.757
	3	7	3	105	2	5	161	276	69.093
	4	9	3	104	2	5	161	275	69.205
	5	11	3	104	2	5	160	274	69.317
	6	13	3	104	2	5	160	274	69.317
	7	15	5	220	5	13	479	724	18.925
	8	1	3	105	4	7	162	281	68.533
	9	3	3	103	2	5	160	273	69.429
	10	5	3	103	2	5	161	274	69.317
	11	7	4	103	2	5	162	276	69.093
	12	9	3	103	2	5	160	273	69.429
	13	11	3	104	2	5	160	274	69.317
	14	13	4	104	2	5	160	275	69.205

MiYaJi
Laboratory

宮地研究室

MIYAJI LAB