Title	A Study on Differential Cryptanalysis of Salsa 20 and ChaCha Stream Ciphers
Author(s)	Ghafoori, Nasratullah
Citation	大阪大学, 2024, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/101457
rights	
Note	

Form 3

Abstract of Thesis

Name （ GHAFOORI NASRATULLAH ）	
Title	A Study on Differential Cryptanalysis of Salsa 20 and ChaCha Stream Ciphers （ストリーム暗号 Salsa20 と ChaCha の差分解析に関する研究）

Abstract of Thesis

Technology has changed the way we carry out our routine activities. We use digital platforms, including communications, financial transactions, education, entertainment, healthcare, and transportation. The use of digital platforms has significantly simplified our daily lives. However, security has consistently emerged as the primary concern when integrating digital platforms into our daily activities. To address security concerns, cryptography has always played an important role in data confidentiality and integrity on travel and at rest. With the widespread adoption of cryptographic primitives, a comprehensive understanding of their security properties is crucial to ensure the integrity and confidentiality of data. Rigorous analysis of potential vulnerabilities and attack vectors is essential to maintain trust in these systems and mitigate the risk of catastrophic data loss. This thesis studies the symmetric cryptography. I focus on the security assessment of stream ciphers. Stream ciphers are symmetric encryption that operates on individual bits or bytes of data, unlike block ciphers, which process data in fixed blocks. Their speed and bitwise encryption make them applicable for specific applications such as secure communications, stream media, disk encryption, voice-over IP, instant messaging, and more. Salsa 20 and ChaCha are deployed in Operating Systems, TLS 1.3, programming libraries, networks, and others. This dissertation studies the security of Salsa20 and ChaCha and is divided into the following parts.

- The differential cryptanalysis of Salsa20 and ChaCha and the key recovery attack on reduced rounds of Salsa20 and ChaCha.
- The higher-order differential-linear cryptanalysis of ChaCha stream cipher.
- The boomerang attack on reduced rounds of ChaCha stream cipher permutation function.

As the first research, a study was conducted to study the security of the Salsa20 based on the comprehensive analysis of probabilistic neutral bits, which was a differential attack. As a result, a differential key recovery attack was reported with a time complexity of $2^{241.62}$ and data complexity of $2^{31.5}$ on Salsa 8 and an attack on ChaCha7.25 with a time complexity of $2^{254.011}$ and data complexity of $2^{51.81}$. I studied the advanced methodologies of differential cryptanalysis, particularly emphasizing higher-order differentials and higher-order differential-linear cryptanalysis, along with their application to the ChaCha stream cipher. Furthermore, I introduced the higher-order differential-linear distinguishing attack on ChaCha 5, ChaCha 5.5, and ChaCha 6 with $2^{33.21}$, $2^{63.21}$ and $2^{87.21}$ time complexity, respectively.

The third research study studied the security of the ChaCha stream cipher permutation function using boomerang cryptanalysis. The boomerang attack is a variation of differential cryptanalysis. It combines two separate differential properties from different parts of a cipher into a new differential for the entire cipher. It happens with a probability of p^2q^2, requiring both properties to be satisfied twice. I also showed that for some attack positions in ChaCha, the probability could increase to p^2, further improving the attack complexity of ChaCha. In addition, I introduced an algorithm for boomerang attacks on the ChaCha stream cipher. To illustrate the effectiveness of boomerang cryptanalysis, I attack the permutation of ChaCha 6 and ChaCha 7. I found that a boomerang attack with a total of $2^{4.04}$ and $2^{5.99}$ adaptively chosen plaintext and ciphertext is needed to distinguish ChaCha 6 and ChaCha 7 permutation function from a random permutation, respectively.

・様式７

論文審査の結果の要旨及び担当者

氏名	（GHAFOORI NASRATULLAH）		
論文審査担当者		（職）	氏名
	主査	教授	宮地 充子
	副査	教授	滝根 哲哉
	副査	教授	丸田 章博
	副査	教授	井上 恭
	副査	教授	田中 雄一
	副査	教授	落合 秀樹
	副査	教授	駒谷 和範
	副査	講師	樽谷 優弥
	副査	特別研究員	藤堂 洋介（日本電信電話株式会社 社会情報研究所）

論文審査の結果の要旨

In recent years, our society has become increasingly digitalized. Many services that were previously realized in analog way are now realized digitally. Digitization is not only to services such as ticket reservations, purchases, and tax payments, but also to activities such as bidding, commercial transactions, lectures, and ways of working. However, it is very difficult to achieve digitization in a secure manner, especially digitization of activities. This is why security has consistently been the foremost concern when integrating digital platforms into our daily lives. To mitigate these concerns, cryptography has played a vital role in ensuring data confidentiality and integrity, both during transmission and while stored. As cryptographic primitives become increasingly prevalent, a deep understanding of their security properties is essential to safeguard data. Rigorous analysis of potential vulnerabilities and attack vectors is crucial to maintaining trust in these systems and minimizing the risk of significant data breaches.

Symmetric cryptography, also known as secret-key cryptography, is fundamental to today's digital society. Among its techniques, stream ciphers are particularly efficient, offering the capability to encrypt data of any length swiftly and effectively. Due to their efficiency, stream ciphers are widely employed in securing data across various applications, including mobile phones, ATMs, online shopping and payment systems, credit cards, social media, video games, and more. These ciphers provide confidentiality in digital communication across diverse platforms. Notably, Salsa20 and ChaCha are two of the most important stream ciphers, extensively utilized in operating systems, TLS 1.3, programming libraries, and network protocols, among others.

Salsa20 and ChaCha are important stream ciphers used across various platforms, making their security analysis crucial. So far, differential and differential linear analyses have been conducted on Salsa20 and ChaCha; however, these are not sufficient to guarantee their current security. In fact, while the PNB method has been used in differential analysis, vulnerabilities specific to this method have not been examined well. Moreover, traditional differential analysis uses single-bit biases, but its application to higher-order differential analysis, which utilizes multiple-bit biases, remains insufficient. Additionally, boomerang attacks, which are used in other ciphers, have not yet been applied to Salsa20 and ChaCha. Taking these existing analysis results into account, this dissertation aims to further investigate the security of Salsa20 and ChaCha.

This dissertation consists of the following three contributions.

1. Differential Cryptanalysis of Salsa20 and ChaCha

   Current research on Salsa20 and ChaCha focuses on computing the attack position from input to output differences and identifying the number of probabilistic neutral bits (PNBs). The output difference significantly influences attack complexity. This thesis analyzes the output difference to mount attacks on Salsa8 and ChaCha7.25 by introducing new attack points (ID and OD) and uncovering new sets of PNBs. The distribution of neutrality measures across the 256 key bit positions of Salsa20/8, ChaCha7, ChaCha7.25, ChaCha5, and ChaCha7.75 is also examined. By focusing on PNB analysis instead of relying solely on ID and OD pairs, new PNB sets have been discovered. Then, differential attacks have been mounted on Salsa20/8 with a time complexity of $2^{241.62}$ and a data complexity of $2^{31.5}$, and on ChaCha7.25 with a time complexity of $2^{254.011}$ and a data complexity of $2^{51.81}$. The time complexity of the attacks on Salsa8 and ChaCha7.25 has been improved by factors of $2^{2.08}$ and $2^{1.6}$, respectively.

2. <u>Higher-Order Differential-Linear Cryptanalysis of ChaCha</u>

   Previous attacks on ChaCha have primarily focused on first-order differentials, with researchers combining this approach with linear cryptanalysis to target reduced rounds. However, the linear approximation of the final modular addition used in the key generation process has not been fully exploited. This thesis aimed to enhance the differential component to reduce overall attack complexity. By applying second-order differential analysis, ChaCha4 has been attacked by differential cryptanalysis, and then attacked by linear cryptanalysis from the 4th round to the 5th and the 6th rounds. As a result, this thesis has introduced a distinguisher for ChaCha6 with a complexity of $2^{47.21}$, improving the existing distinguisher by a factor of $2^{3.79}$. Higher-order differentials and their impact on reduced rounds of ChaCha are also explored. Furthermore, the linear approximation of the final modular addition has been considered, to launch a distinguishing attack on ChaCha. Then, specifically ChaCha5, ChaCha5.5, and ChaCha6 have been examined, whose distinguishing attack complexities were calculated as $2^{33.21}$, $2^{63.21}$, and $2^{87.21}$, respectively. This is the first distinguishing attack on ChaCha of this kind.

3. <u>The Boomerang Attack on ChaCha Permutation</u>

   While ChaCha has been extensively analyzed for resistance against traditional differential attacks, its vulnerability to other cryptanalytic methods, such as boomerang cryptanalysis, remains insufficiently explored. The technique combines two sets of differential properties to form a new composite property that covers the entire cipher, with a probability of p^2q^2. This research presents the first evaluation of the security of ChaCha's permutation function against boomerang attacks. The boomerang attack results on ChaCha6 and ChaCha7 indicate that approximately $2^{4.04}$ and $2^{5.99}$ adaptively chosen plaintext-ciphertext pairs, respectively, are required to distinguish them from a random permutation. As this is the initial application of a boomerang attack on the ChaCha permutation, no direct comparisons with existing studies are available.

As described above, this dissertation investigates the security of Salsa20 and ChaCha using advanced techniques such as differential, higher-order differential-linear, and boomerang cryptanalysis. The study introduces new distinguishers for reduced rounds of ChaCha, and conducts the first boomerang attack on ChaCha's permutation function, revealing new vulnerabilities. These contributions enhance the understanding and security of these widely used ciphers, Salsa20 and ChaCha. Thus, the impact of this research on the further digitization of society in the future is immeasurable.

Therefore, this thesis contributes significantly to the development of the field of information security and engineering and is recognized as a valuable doctoral dissertation.