様式３

論　文　内　容　の　要　旨

氏　名　（　伊　藤　竜　馬　）	
論文題名	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）

論文内容の要旨

This dissertation presented a study on statistical cryptanalysis of stream ciphers, and focused particularly on RC4. First of all, we investigated 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 applied 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 attempted to improve them. Finally, we proposed 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 focused on Glimpse Correlations between the keystream and the internal state. The existing Glimpse Correlations provided only cases with positive biases, and held generally on any round. Then, we have refined 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 investigations, we have provided six events with several new biases, and proved these events theoretically.

In Chapter 5, we investigated 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 used this feature. As a result of our investigations, we have provided 22 events with key correlations of the internal state variables, and proved the events theoretically. Our theoretical proofs have made clear how TKIP induces biases in the internal state of generic RC4. We then discussed 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 have observed 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 investigated 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 investigations, we have proved new events with the iterated RC4 key correlations theoretically. Furthermore, we applied these events to the existing plaintext recovery attacks on WPA-TKIP. As a result of our experiments, we have achieved 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.

In Chapter 7, we concluded our results and provided a direction to construct secure stream ciphers generally based on our statistical cryptanalysis of RC4 stream cipher.

様式 7

論文審査の結果の要旨及び担当者

氏　名	（　伊藤　竜馬　）	
	(職)	氏　名
論文審査担当者	主査　教　授	宮地　充子
	副査　教　授	馬場口　登
	副査　教　授	滝根　哲哉
	副査　教　授	丸田　章博
	副査　教　授	三瓶　政一
	副査　教　授	井上　恭
	副査　教　授	鷲尾　隆(産業科学研究所)
	副査　教　授	駒谷　和範(産業科学研究所)
	副査　教　授	Serge Vaudenay (Ecole Polytechnique Federale de Lausanne)
	副査　准教授	河内　亮周

論文審査の結果の要旨

本論文は，データの秘匿および完全性実現に利用される共通鍵暗号の一種であるストリーム暗号の安全性解析を行った．特に，無線 LAN セキュリティプロトコルの WPA などで利用されていたストリーム暗号の 1 つである RC4 の統計的解析を行い，未知の脆弱性を発見するとともに，その存在を証明している．ストリーム暗号の方式は多数存在するが，RC4 の設計方針は現在利用されている各種ストリーム暗号の基本になっており，RC4 の安全性解析は今後のストリーム暗号の安全性解析という観点でも非常に重要である．以下に本論文の結果をまとめる．

第一の研究成果は RC4 から生成されるキーストリームと内部状態の間における Glimpse と呼ばれる相関性に関する解析である．具体的には，これまで発見されていなかった 6 種類の相関性を詳細に解析することで，6 個の定理を証明している．特に，2 バイト連続するキーストリームが $Z_{r+1}=Z_r$ の時，r ラウンドにおける内部状態 $S_r[r+1]$ が 0 となる確率が著しく低いことを示している．

第二の研究成果は RC4 の入力となる秘密鍵と内部状態の間における相関性の解析である．具体的には，WPA-TKIP 利用時の RC4 において秘密鍵の先頭 3 バイトが公開情報であることを利用していることに着目し，公開情報を用いた線形式と内部状態の間にこれまで発見されていなかった数百を超える相関性の存在を発見している．さらに，安全性解析をおこない， 22 個の相関性については定理として証明を与えている．特に，WPA-TKIP 利用時の RC4 において内部状態 $S_0[1]$ が最上位バイトの秘密鍵 K[0] の値となる確率が 0 であることを示している．

さらに，WPA-TKIP 利用時の RC4 において，公開情報から 3 バイトの秘密鍵をどのように設定すれば相関性の発生を抑制できるかについて解析し，より安全な秘密鍵の設定方法を提案している．

第三の研究成果は RC4 の入力となる秘密鍵とキーストリームの間における相関性に関する研究である．具体的には，既存研究で解析済みの相関性に着目し，これまで発見されていなかった相関性へと拡張することで，3 個の相関性を発見し，定理として証明を行っている．さらに，既存の相関性に加え，本章で新たに発見した相関性を用いることで，既存の平文回復攻撃を最適化した結果について示している．

最後に，これまでの研究成果を統合し，ストリーム暗号の安全なシステム設計方法を明確にしている．ストリーム暗号の脆弱性はシステム設計方法に依存することが多く，本論文は安全な情報利活用の観点で非常に重要である．

以上のように，本論文では代表的なストリーム暗号の 1 つである RC4 を解析対象とし，統計的脆弱性の詳細な解析，既存の平文回復攻撃の最適化，そして WPA-TKIP の安全な利用に向けた設計方法を示すとともに，一般的なストリーム暗号の解析手法，安全な設計方法を与えたという点で工学の発展に大きく貢献している．

よって，本論文は博士論文として価値あるものと認める．