ストリーム暗号の安全性評価に関する研究

Security Evaluation for Stream Ciphers

准教授　大東　俊博

Associate Prof.
Toshihiro OHIGASHI

Keyword : cryptography, security evaluation, stream cipher

情報セキュリティの基礎となる暗号技術は学会等の公開の場で提案され、世界中の暗号研究者による厳しい安全性評価（解読法の検討）を受けて一定の信頼を得ます。したがって、暗号解読の研究は重要な研究の一つと言えます。

本研究室ではストリーム暗号の安全性評価に関して研究をしています。過去、無線 LAN 用の暗号化方式である WEP に対する新しい解読法を考案し、WEP が従来信じられていた安全性より格段に弱いことを示しました。さらに、インターネット用の暗号化プロトコルである SSL/TLS において RC4 暗号という方式を使った場合に解読可能であることを世界で初めて発見しました。現在は、ストリーム暗号の安全性について統計的な方法を用いて自動的に評価する方法の確立について取り組んでいます。

Stream cipher is a class of symmetric-key cryptography, which uses the same key for encryption and decryption, and it provides confidentiality and integrity to data or network. We have evaluated the security of stream ciphers, e.g. RC4 stream cipher. In our research results, we found the key recovery attack for RC4 on Wired Equivalent Privacy (WEP), the falsification attack on WPA-TKIP, and the plaintext recovery attack for RC4 on SSL/TLS. Recently, we challenge about the automatic evaluation technique for stream cipher by using statistical method.

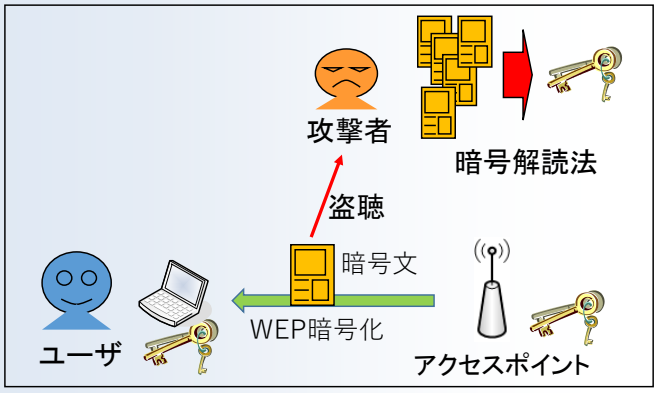

Fig. 1 Attack model for WEP

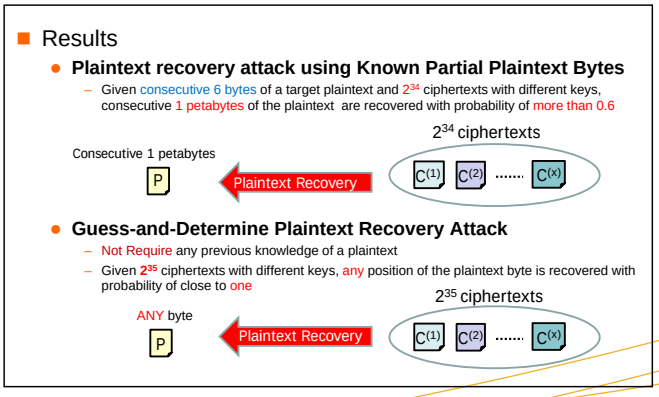

Fig. 2 Attack for SSL/TLS

◆リンクページ(Link)：http://www.ocsl.jt.u-tokai.ac.jp/

◆電子メール（address）：ohigashi@tsc.u-tokai.ac.jp