NTT, Ruhr-Universität Bochum, and Kobe University Develop a New Cryptanalytic Technique to Improve the Design of Lightweight Ciphers for Internet of Things

1. Research result

NTT, jointly with Ruhr-Universität Bochum and with Kobe University, has developed a new cryptanalytic technique (the nonlinear invariant attack) that helps improve the design and security of lightweight symmetric-key ciphers, which are considered to play an active part in the IoT (Internet of Things) era.

Most of the previous cryptanalysis techniques assume unrealistic scenarios where adversaries have opportunities to obtain encrypted data of plaintext they deliberately choose, in terabytes. In contrast, the new cryptanalytic technique, when applied to several existing (lightweight) ciphers, recovers part of the plaintext from encrypted data in amounts smaller than one kilobyte, under the condition that either the plaintext contains repetition or the same plaintext gets encrypted multiple times. The new technique can be used to greatly improve the design of lightweight ciphers and to re-evaluate the security of other existing symmetric-key ciphers.

The paper reporting this research result [1] received the distinction of being "Invited to the Journal of Cryptology," meaning that it was one of the top three papers accepted at Asiacrypt 2016 (held in Hanoi, Vietnam, December 4–8), a prestigious conference organized by the International Association of Cryptologic Research.

2. Key facts

Linear cryptanalysis was published in 1993 and applied to the Data Encryption Standard (DES), which was essentially the world standard at that time, demonstrating the first cracking of DES by a computer. Linear cryptanalysis was applied to numerous cryptographic primitives as a generic cryptanalytic technique, and cryptographic primitives newly developed after the publication of linear cryptanalysis were required to provide evidence of resistance to linear cryptanalysis. Linear cryptanalysis, as the name suggests, linearly approximates nonlinear behavior of cryptographic primitives. It has been a long-standing open problem whether it is possible to devise a similar type of cryptanalysis using nonlinear (quadratic or higher) approximation rather than linear approximation. A previous attempt in 1995 used nonlinear approximation to analyze input and output parts of a cryptographic primitive, but no previous attempts succeeded in cryptanalyzing an entire cryptographic primitive. Our new cryptanalytic technique, the nonlinear invariant attack, provides an answer to the open problem for the first time.

The previously mentioned paper describes how the nonlinear invariant attack is applied to SCREAM, iSCREAM, and Midori64. SCREAM and iSCREAM are symmetric-key schemes submitted to CAESAR, a competition to evaluate authenticated encryption (symmetric-key ciphers equipped with an integrity check). Midori64 is a symmetric-key cipher published at Asiacrypt 2015. The key idea of the attack is to identify a quadratic (hence, nonlinear) invariant quantity associated with the nonlinear component of the cipher called sbox and then to observe that the sum of the quadratic function (nonlinear approximation) applied to each sbox output also remains unchanged through the linear part of the cipher where a binary orthogonal matrix is used. When the attack is

applied to SCREAM and iSCREAM, 32 bits of plaintext are instantly recovered from 33 blocks (one block is 128 bits) of encrypted data, under the condition that the secret key is one of the 2^{96} special keys (called "weak keys") out of the entire 2^{128} key space. When applied to Midori64 in most modes of operations used in practice, for example in the CTR (counter) mode, 32 bits of plaintext are instantly recovered from 33 blocks (one block is 64 bits) of encrypted data for 2^{64} special keys out of the entire 2^{128} key space.

3. Future plans

NTT Secure Platform Laboratories is continuing to re-evaluate the security of other existing ciphers by applying the nonlinear invariant attack and is also pursuing cryptanalytic techniques for developing secure cryptographic algorithms.

Reference

[1] Y. Todo, G. Leander, and Y. Sasaki, "Nonlinear Invariant Attack—Practical Attack on Full SCREAM, iSCREAM, and Midori64," Proc. of Asiacrypt 2016, Part II, pp. 3–33, Hanoi, Vietnam, Dec. 2016.

For Inquiries
NTT Service Innovation Laboratory Group
http://www.ntt.co.jp/news2016/1612e/161201a.html