論文の内容の要旨

論文題目　Public-Key Cryptosystems Resilient to Computationally Hard-to-Invert Leakage
（計算量的逆変換困難漏洩耐性を持つ公開鍵系暗号技術）

氏　　名　石坂　理人

Cryptographic technologies are essential to make our daily lives more secure and/or more convenient. For instance, in an environment where any sent message can be eavesdropped, by using public-key encryption (PKE) or symmetric-key encryption (SKE), we can send any message without giving no information about the message to the eavesdroppers. And, in an environment where any sent message can be maliciously modified, by using digital signature or message authentication code (MAC), we can send any message in a way such that any modification of the message is detected. Especially, public-key cryptosystems such as PKE and digital signature are convenient because the key-change in advance is no necessary.

The current cryptographic schemes are required to be theoretically secure or provably secure. A reason behind the fact is that there are at least a few examples of cryptographic schemes such that although they are assessed to be secure from specialists' empirical points of view, standardized and widely used, later they were shown to be theoretically insecure. When we do the proof of security, we formally construct a security model, and then reduce the hardness breaking the security model to the hardness solving a mathematical problem which are believed to be hard to solve. For instance, the most desirable security notion of digital signature is

one named strongly existentially unforgeability against chosen message attack, or sEUF-CMA in short. Intuitively, this formalization states that any adversary, who is given a signature-verification-key (public-key) in advance, is successful in forging a signature only with an extremely small probability (i.e., negligible probability), even if he can adaptively use signing oracle which takes a message and returns a signature on the message.

In the real world, cryptographic devices are always threatened by secret-information leakage caused by malicious entities. The most serious threat is Side-Channel Attack (SCA) which utilizes physical information observed from the device such as power consumption, electromagnetic radiation, acoustic emanation and temperature to identify the secret-key of the device. The standard security models, including sEUF-CMA of digital signature mentioned above, do not consider such information leakage at all. Thus, as soon as 1 bit information from such an information is leaked, they lose their security guarantees.

Leakage-Resilience guarantees that even if some partial related information of the secret-information are leaked, the security is maintained. In security models considering leakage-resilience, we model the information leakage by an efficiently computable function f. The function should be restricted, and various security models which differ in such a restriction have been proposed. Especially, a security model named Hard-to-Invert Leakage Model (HL Model) which requires f to be computationally hard-to-invert is considered to be theoretically/practically meaningful.

We present solutions to the following three open problems concerning the hard-to-invert leakage-resilience.

The first one is regarding Identity-Based Encryption (IBE) with HL-resilience. The IBE scheme proposed by Yuen et al. at EUROCRYPT'12 has been known as the only one claimed to be correctly proven to be secure in a security model with HL-resilience. Firstly, to show that their security proof is defective, we present some concrete counterexamples of adversaries which can be the evidence of the deficiency. Moreover, we propose an original IBE construction and prove that it is secure in a security model considering HL-resilience. As a result, our IBE scheme is the first one whose HL-resilience is correctly proven.

The second one is regarding Digital Signature with HL-resilience. We propose a generic construction of digital signature, and show that it is strongly unforgeable, i.e., sEUF-CMA secure, and resilient to polynomially hard-to-invert leakage. Then, we show that it can be instantiated under a standard assumption, namely the decisional linear (DLIN) assumption. Currently, there are some signature schemes proven to be secure in a model considering HL-resilience. We emphasize that our instantiation of signature scheme is not only the first one resilient to polynomially hard-to-invert leakage under standard assumptions, but also the first one proven to be secure in a strong unforgeability model considering HL-resilience.

The third one is regarding Attribute-Based Signature (ABS) and Identity-Based Signature (IBS) with HL-resilience. Currently, a lot of ABS/IBS schemes secure in a model with no leakage-resilience have been known. However, no scheme proven to be resilient to some leakage under standard assumptions has been known. We propose generic constructions of ABS/IBS schemes and prove that they are secure in HL model. Then, we show that they can be instantiated under the DLIN assumption. It should be noted that our schemes are the first ones with HL-resilience under standard assumptions, and more generally, the first ones with leakage-resilience under standard assumptions.