論文の内容の要旨
Abstract

論文題目　Security Evaluation of Public-Key Cryptography against Side-Channel Attacks and Quantum Attacks
（公開鍵暗号に対するサイドチャネル攻撃および量子攻撃の安全性評価）

氏　　名　　大西　健斗

Public-key cryptography is an indispensable technology for the information society, and the security of public-key cryptosystems must be guaranteed to use them. The standard definitions of security are based on computational problems, which take a long time to solve. However, both side-channel and quantum attacks threaten security. Side-channel attacks may recover sensitive information using data leaked physically, depending on an actual implementation. The standard definitions of security do not consider the actual implementations, and cryptosystems will be insecure even if the security is guaranteed. Thus, security against side-channel attacks must be considered based on the actual implementations. In addition to side-channel attacks, threats of quantum computers also exist. Quantum computers have more computational power than the currently used computers. Ideal quantum computers break the currently used public-key cryptosystems such as the RSA scheme. The National Institute of Standards and Technology (NIST) promotes the standardization of post-quantum cryptography against quantum attacks. We must also consider the threats of quantum attacks to the currently used public-key cryptosystems because it takes a long time to migrate to new cryptosystems. In this thesis, we evaluate the security of public-key cryptosystems against side-channel and quantum attacks. We present four new contributions.

First, we improve the recovery method for the CRT-RSA secret keys from the correct sliding window leakage. The CRT-RSA scheme is a currently used public-key cryptosystem. A way to recover the CRT-RSA secret keys from the correct square-and-multiply sequences was discussed in a previous study. Two methods are used to recover the CRT-RSA secret keys. In the first method, the CRT-RSA secret keys are recovered partially, after which all bits are recovered. In the second method, the CRT-RSA secret keys are recovered directly from square-and-multiply sequences. To improve the previous methods, we study a technique for recovering bits of the CRT-RSA secret keys in more depth. We propose a new method for recovering additional bits with high accuracy. We then propose a new recovery method for the CRT-RSA secret keys by combining the previous two methods and using additional recovered bits.

Second, we consider the security of the CRT-RSA schemes in a more realistic situation. We propose a new method for recovering the CRT-RSA secret keys from noisy square-and-multiply sequences.

Moreover, by calculating the number of errors corrected in polynomial time, we give the theoretical bound of errors that the CRT-RSA secret keys are recovered.

Third, we evaluate the exact security of Ring-LWE and Module-LWE based schemes against side-channel attacks on a Number Theoretic Transform (NTT). Ring-LWE and Module-LWE based schemes are next-generation public-key cryptosystems and are efficiently implemented using a number theoretic transform (NTT). These schemes are applied as candidates for the NIST standardization project. Lyubashevsky et al.'s cryptosystem (LPR cryptosystem) is the basis of these schemes. We then evaluate the security of the LPR cryptosystem against side-channel attacks on the NTT. We adopt the erasure model on the multiplication in the NTT and propose an algorithm for recovering the LPR secret keys. Moreover, we evaluate the security of the LPR cryptosystem under the erasure model. Our method recovers the LPR secret keys when the erasure rate is less than 0.78 at the current computational power.

Finally, we evaluate the security of the RSA scheme against quantum attacks. Quantum attacks break the RSA scheme by Shor's algorithm. A controlled modular adder is an essential operation for Shor's algorithm, and the depth of a controlled modular adder should be minimized. Van Meter and Itoh proposed an efficient construction of a controlled modular adder. We propose a more efficient construction than their original one, and we evaluate the security of the RSA scheme based on our controlled modular adder. We then evaluate the security based on IBM's plan for the development of quantum computers. Our estimation shows that quantum computers will break the 2048-bit RSA scheme 28.2 years later, which is 1.4 years earlier than Van Meter and Itoh's construction.