論文の内容の要旨

論文題目

Security Analysis and Proof Methodology of Public Key Cryptographic Schemes

(公開鍵暗号技術における安全性解析と証明技法に関する研究)

氏　　名　　川合　豊

In the research field of cryptography, in order to claim the security of the proposed scheme, security proofs are essentially important. However, owing to complications on evolutions of new protocols security proofs of these protocols have been difficult. So, the aim of this dissertation is to give rigorous security proofs in several public key cryptographic schemes and to propose new security methodology by using reduction technique and meta-reduction technique. In order to establish the framework in which correct security proofs are given against powerful adversaries, we make research two different stages.

Aiming at rigorous security analysis for complex cryptographic scheme, we give several security analyses for anonymous authentication and extended encryption. Specifically, we focus on secret handshake scheme and proxy re-encryption scheme.

First, we show the flaw of "secret handshake scheme with multiple groups (SHSMG)". Secret handshake scheme allows members of the same group to authenticate each other secretly, that is, two members who belong to the same group can learn their counterparts in the same group, while non-member of the group cannot determine whether the counterpart is a member of the group or not. Yamashita and Tanaka

extended a single group setting to a multiple groups setting where two members output accept iff both member's affiliations of the multiple groups are identical. First, we show the attack to their scheme in the meaning of detector resistance. Second, we introduce a new concept of secret handshake scheme “monotone condition secret handshake with multiple groups” in order to extend the condition of accept.

Second, we discuss the anonymity for secret handshake schemes. When a more strict anonymity is required even for a group authority (GA), previous anonymity is unfavorable in some situations. Since the above previous anonymities are extreme, the previous secret handshake schemes are not applicable to several systems. So, we propose several new anonymity requirements. Additionally, we propose a secret handshake scheme which satisfies our proposed anonymity requirements using group signature with message recovery technique.

Next, we present the first generic construction of chosen-ciphertext (CCA) secure uni-directional proxy re-encryption (PRE) scheme. PRE is an interesting extension to traditional public key encryption (PKE). In addition to the normal operations of a PKE, with a dedicated re-encryption key (generated by a receiver A), a proxy can turn a class of ciphertexts to user A into those to another user B. A remarkable property of PRE is that the proxy, who can do the transform, is totally ignorant of the plaintext. In particular, full CCA security of our proposed scheme is proven even against powerful adversaries which are given a more advantageous attack environment than in all previous works, and furthermore, it does not require random oracles. For achieving such strong security, we establish a totally novel methodology for designing PRE which is based on a specific class of threshold encryption. Via our generic construction, we present first construction which is CCA secure in the standard model.

Aiming at easy security proof methodology, we present new technique that we can check whether a security proof of a scheme (in this thesis, a public key encryption and a digital signature) is possible or not. Specifically, we proposed new impossibility proof technique (so-called meta-reduction technique) and analysis for public key encryption and digital signature schemes.

First, we introduce new meta-reduction technique in order to show several impossibility results. We use the proposed concepts to rigorously classify the impossibility range for general cases. Finally, we show the application to security analysis using new meta-reduction technique for a specific digital signature scheme. We introduce Variant Rabin signature scheme and classify its security into secure/insecure/no-information ranges using newly developed techniques.

Second, we discuss the strong attack model security for PKE and digital signature.

The main motivation of this chapter is to find an essential mechanism of secure schemes under strong attack model. So, we prove several impossibility results by using the meta-reduction. We classify two types of PKE: First model is (Gen, Enc, Dec) which we call the setup-free model, Second model is (Setup, Gen, Enc, Dec) which we call the setup model. We prove that it is impossible to reduce indistinguishability under strong chosen ciphertext attack (IND-SCCA) security to any other weaker security notion under black-box analysis in the standard model. Second, when a PKE is a setup model, we show that it is impossible that the security of SCCA is proven if the reduction is setup-preserving black-box reductions. Finally, we discuss the essential mechanism to construct IND-SCCA secure public key encryption scheme in the standard model.

Finally, we discuss security of public-key cryptographic primitives in the case that the public key is fixed. In the standard argument, security of cryptographic primitives is evaluated by estimating the average probability of being successfully attacked where keys are treated as random variables. In contrast to this, in practice, a user is mostly interested in the security under his specific public key which has been already fixed. However, it is obvious that such security cannot be mathematically guaranteed due to the fact that for any given public key, there always potentially exists an adversary which breaks its security. Therefore, the best what we can do is just to use a public key such that its effective adversary is not likely to be constructed in the real life, and thus, it is desired to provide a method for evaluating this possibility. The motivation of this work is to investigate (in)feasibility of predicting whether for a given fixed public key, its successful adversary will actually appear in the real life or not. As our main result, we prove that for any digital signature scheme or public key encryption scheme, it is impossible to reduce any fixed key adversary in any weaker security notion than the de facto ones to fixed key adversaries in the de facto security notion in a black-box manner.