# 論文内容の要旨

## Security Notions and Generic Constructions of Chosen Ciphertext Secure Public Key Encryption Schemes
## (選択暗号文攻撃に対して安全な公開鍵暗号の安全性定義と一般的構成法)

氏名　　松　田　　隆　宏

Public key encryption (PKE) is a fundamental cryptographic primitive with which we can communicate securely over possibly insecure network without shared secret information in advance. For PKE schemes, security against chosen ciphertext attacks (CCA security) is nowadays considered as a standard security notion needed in most practical applications/situations where PKE schemes are used. Roughly, CCA security captures security against "active" adversaries that can access to an imaginary machine called decryption oracle which on input a ciphertext returns a decryption result of it, and has been shown to imply important strong security notions such as non-malleability and universal composability. Therefore, studies on constructing and understanding CCA secure PKE schemes are important research topics in the area of cryptography. In this thesis, we focus on "generic constructions" of CCA secure PKE schemes from other cryptographic primitives, and make several contributions both from practical and theoretical points of view.

Firstly, aiming at generic constructions that lead to CCA secure PKE schemes with practical efficiency, we focus on the so-called "IBE-to-PKE" transformation paradigm, where IBE stands for identity-based encryption and is a kind of PKE scheme where any string can be used as a public key. This is a methodology that transforms an IBE scheme

which only satisfies security against chosen plaintext attacks (CPA security), the least requirement as an encryption scheme, into a CCA secure PKE scheme, and is the only known generic methodology with which we can construct CCA secure PKE schemes with practical efficiency. The biggest problem of this methodology is that the constructed PKE scheme has large ciphertext size, even if we use a practical IBE scheme as a building block. We propose two approaches to overcome this problem. The first approach is to require non-malleability, slightly stronger security than CPA security, for the underlying IBE scheme, and develop a new very simple IBE-to-PKE transformation where we only use one-way function, the weakest primitive used in the area of cryptography, as an additional building block. The second approach is to develop a new efficient encapsulation scheme, which is a special kind of commitment scheme and is a primitive used in one of the previous IBE-to-PKE transformations, from a special kind of pseudorandom generator. Both approaches do not need strong cryptographic primitives as additional building blocks, and lead to CCA secure PKE schemes with smaller ciphertext size than the previous IBE-to-PKE transformations.

Secondly, we focus on the problem of whether it is possible to construct a CCA secure PKE scheme only from a CPA secure one. This is an important fundamental open problem that leads to clarifying a necessary and sufficient condition to realize a CCA secure PKE scheme. Regarding this problem, the best known positive results are the constructions of so-called bounded CCA secure schemes from any CPA secure PKE scheme, where bounded CCA security is security against adversaries that make at most the predetermined number of decryption queries, and thus is weaker than ordinary CCA security. Since we can achieve the best possible security in the bounded CCA security notions, in order to further tackle the fundamental problem, we need new security notions that capture intermediate security notions that lie between CPA and CCA security in a different sense from bounded CCA security. Motivated by this situation, in order to provide a theoretical foundation for further tackling the above problem, we focus on parallel decryption queries for the extension of bounded CCA security, and introduce a new security notion which we call “mixed CCA” security. It captures security against adversaries that make single and parallel decryption queries in a predetermined order, where each parallel query can contain unboundedly many ciphertexts. Moreover, how the decryption oracle is available before and after the challenge is also taken into account in this new security definition, which enables us to capture existing major security notions that lie between CPA and CCA security, including a complex notion like non-malleability against bounded CCA, in a unified security notion. We investigate the relations among mixed CCA security notions, and

show a necessary and sufficient condition regarding implications/separations between any two notions in mixed CCA security. We then show two black-box constructions of PKE schemes from CPA secure ones, one of which satisfies a strictly stronger security notion than the security notions achieved by the existing constructions of PKE schemes constructed only from a CPA secure one. We also discuss the consequences of our results regarding security with parallel decryption queries and give several observations.