論文の内容の要旨

論文題目　Efficient Constructions and Provable Security of Public-Key Encryptions

（和訳　公開鍵暗号の効率的構成法および証明可能安全性に関する研究）

氏　名　　崔　洋

（本文）Public-key encryption is playing a crucial role in modern cryptography and information security, for the confidentiality of the secrecy and privacy. This dissertation considers the efficient design and provable security of public-key encryptions. We present new algorithms and motivating applications, with rigorous proofs based on well-known cryptographic assumptions. All schemes we presented are efficient and practical.

In particular, our approach is focusing on the following areas.

1). **Generic conversions for public-key encryptions:** The confidentiality of public-key encryptions is required to satisfy the strongest security, however, most of current public-key encryptions are only fulfilling with relatively weak security. Although there were some generic conversions had been proposed for enhancing the security of the original public-key encryptions including some distinguished schemes, unfortunately, there does not exist such a scheme that could generically transform many public-key encryption schemes to the strongest security, with the theoretically minimal overhead. Optimal Asymmetric Encryption Padding (OAEP), as its name, was considered to be able to transform a specific public-key encryption to the strongest security with optimal message overhead, but finally found to have a flaw if without additional overhead. Thus, it loses the optimal result. We present here a generic conversion which is the first one to achieve the optimal message overhead while keeping the strongest security. It bases on a well-known cryptographic assumption, and its proof has a tight reduction cost compared to the previous schemes, which usually implies a better performance under the same security level.

On the other hand, a number of public-key encryptions currently used are subject to quantum algorithms if quantum computer could be built. Concerning that long-term security, it is essential to take account of post-quantum public-key encryptions as soon as possible. Among many candidates, a kind of promising public-key encryptions has recently been broken by a decryption error based attack. We present here a generic and efficient solution to thwart the underlying attack, so that the public-key encryption with decryption errors may still immune to the quantum algorithm based attack.

2). **Efficient hybrid encryption:** Since we have achieved the optimal result when solely public-key encryption scheme is used, we also intend to construct efficient schemes in other cases. One of the most important applications of public-key encryptions, is to transfer session key for the symmetric encryption to encrypt the lengthy data in a fast way. A combination of public-key encryptions and symmetric-key encryptions works in tandem, which is called hybrid encryption. We show that in hybrid encryption scenario, the efficiency could be further enhanced while keeping the security as the same. We present two schemes in hybrid public-key encryption setting, which are based on a recently presented advantageous framework in a number of aspects. One of the schemes is quite simple and nearly optimal since only one cryptographic hash function and one key derivation function are needed in addition to the original public-key encryption. Astonishingly, a distinguished scheme proposed more than 10 years ago could be actually taken as a special case of our very efficient scheme. Therefore, our result can be considered as a generalization solution, and several significant public-key encryptions are possibly adapted to our new scheme in order to guarantee the strongest security. The scheme is secure as long as a well-known mathematical assumption holds, and the security proof is built in the so-called "random oracle" model.

Although the random oracle model is a powerful tool widely use in the design and analysis of cryptography, sometimes it is not desired to assume such an ideal cryptographic hash function in practice. The other scheme we presented here, has achieved the best security in the standard model (i.e. without requiring the random oracles). We take advantage of identity-based encryption to construct a hybrid public-key encryption in the strongest sense. The resulting scheme is a lot more efficient than the previous one both in computation and communication cost.

More interestingly, the second scheme is naturally functional in the threshold cryptography, which has numerous applications in E-commerce and E-voting. Basing on our new scheme, we also present a threshold hybrid encryption and an identity-based threshold hybrid encryption in the standard model, with pretty good efficiency. The technique we used may have an independent meaning in cryptography.

3). **Lightweight public-key encryptions:** Public-key encryptions have plenty of applications in theory and in practice. We are motivated by the security requirement in wireless environment, where the problem is hard to tackle because of the restricted computation and communication sources. Although it is difficult to achieve a full-fledged public-key encryption in the best security level, we point out that some lightweight solutions are still available. We present two secure authentication protocols by using a partial public-key encryption, and prove the protocols are effective and efficient. Summarizing another work where we find successful attacks against a distinguished lightweight authentication based on a similar assumption, we conclude that our protocols are very promising for protecting wireless security in practice.

Finally, this dissertation summarizes the methodology of design and analysis of public-key encryptions. We wish that it will contribute to the research of cryptography and information security, for protecting the information technology as well as personal secrecy and privacy.