論文の内容の要旨

論文題目　Enhancing Security of Efficient Advanced Cryptosystems via Reduction to Reliable Assumptions
（高効率な高機能暗号方式の安全性強化手法に関する研究）

氏　名　勝又　秀一

The introduction of public-key cryptography by Diffie and Hellman (IEEE TIT, 1976) has had an enormous influence on the current information society. Starting with the most fundamental primitive of public-key encryption schemes, the field of public-key cryptography has been enriched with many alluring advanced primitives. In cryptography, when we say a scheme is "secure", we implicitly have in mind the concept of provable security --- a notion introduced by Glodwasser and Micalli (STOC, 1982). Informally, we have a set of hardness assumptions which we rely on to build provably secure cryptographic primitives. As one can imagine, as the cryptographic primitives become more advanced, it is generally the case that we require a stronger hardness assumptions to construct them. However, proving a cryptographic primitive secure under a strong hardness assumption is undesirable since the security guarantee for the primitive we achieve will be weaker, and moreover, often times we would have to compensate for the security loss by making the concrete instantiation less efficient.

This Ph.D. thesis is a study of different approaches to make advanced cryptosystems more secure by constructing them from weaker, hence more reliable, hardness assumptions. We broadly prepare three measures which we can use to assess the hardness of a problem: whether it is a search problem or a decision problem, whether it is a static-problem or a non-static problem, and whether it is post-quantum or not. Following these three measures, we enhance the security guarantees (and in some cases its concrete efficiency) of advanced cryptographic primitives. The main contributions are contained in the five papers included in this thesis and cover the following primitives: identity-based encryption (IBE) schemes, verifiable random functions (VRF), predicate encryption (PE) schemes, non-zero inner product encryption (NIPE) schemes, and attribute-based signature (ABS) schemes.

Concretely, the first two papers concern IBE schemes. In the first paper, we show an alternative security proof for a state-of-the-art post-quantum IBE scheme and show that we can enhance its security without modifying the original scheme. In the second paper, we provide a general framework for proving IBE schemes by implicitly embedding non-linear polynomial functions in the public parameters and obtain two IBE schemes with better security guarantees and more compact public parameters compared to previous schemes. The third paper concerns VRFs and PE schemes. We show how to encode predicates by shallow arithmetic circuits and how to combine them with VRFs and PEs to obtain schemes with better security guarantees. The forth paper concerns NIPE schemes. We provide two different methods for obtaining NIPE schemes from various assumptions. The final paper concerns ABS schemes. We provide a generic construction of ABS schemes for unbounded circuits and instantiate it with post-quantum tools to obtain the first such scheme based on a post-quantum assumption.