論文の内容の要旨

論文題目：Provable Security of Identity Based Encryption
and Application to Design of Efficient Schemes
(IDベース暗号の証明可能安全性と効率的方式設計への応用)

氏名：楊　鵬　　　　　平成21年6月15日提出

Identity based encryption (IBE) schemes have been flourishing since the very beginning of this century. In IBE, it is widely believed that proving the security of a scheme in the sense of IND-ID-CCA2 is sufficient to claim the scheme is also secure in the senses of both SS-ID-CCA2 and NM-ID-CCA2. The justification for this belief is the relations among indistinguishability (IND), semantic security (SS) and non-malleability (NM). But these relations are proved *only* for conventional public key encryption (PKE) schemes in previous works. The fact is that between IBE and PKE, there exists a difference of special importance, i.e. only in IBE the adversaries can perform a particular attack, namely the *chosen identity attack.*

We show that security proved in the sense of IND-ID-CCA2 is validly sufficient for implying security in any other sense in IBE. This is to say the security notion, IND-ID-CCA2, captures the essence of security for all IBE schemes. To achieve this intention, we first describe formal definitions of the notions of security for IBE, and then present the relations among IND, SS and NM in IBE, along with rigorous proofs. All of these results are proposed with the consideration of the chosen identity attack.

Regarding concrete IBE schemes, there are (at least) two levels of secret information, i.e., the top-level secret, which is called the master key, and the end-level secrets, which are the users' secret keys. In order to minimize damage in case of an adversary successfully expose users' secret keys, forward security has been introduced into IBE. In a forward secure identity based encryption (FSIBE) scheme, the adversary can obtain no information about the compromised user's secret encrypted before the breaking-in time point.

In this paper, we also construct such an FSIBE scheme with master key update that the top-level secret evolves as same as users' secret keys do, so that even if at some time point the adversary compromises the master key, he can no longer generate users's secret keys corresponding to passed time points. The provable security of our proposal is CPA, strictly weaker than CCA2. This means in order to implement this scheme in real world, the security needs to be enhanced.

To achieve CCA2 security, Fujisaki-Okamoto conversions (FOpkc, FOcrypto) and REACT conversion are used *specifically* to enhance a weak IBE scheme's security. However whether they can be *generically* used for such purpose was unknown before this work. In this paper, we discuss applications of Fujisaki-Okamoto conversions and REACT conversion in IBE environment. Our results show that all the conversions are *effective*: plain REACT already achieves a good security reduction while plain FOpkc and plain FOcrypto result in bad additional running time of the simulator.

To solve this problem, we further propose a modification to plain Fujisaki-Okamoto conversions. Interestingly, our results may also show a separation between two different attack models. Finally, we choose some concrete parameters to visually explain the effect of how our modifications substantially improve security reduction comparing with the plain applications.

The last contribution of this paper addresses efficient IBE scheme design. In history, the concept of stateful PKE (SPKE), where the senders are asked to maintain some state information, was introduced to reduce computation cost of PKE. Alternatively, the classical PKE schemes are called stateless PKE. Informally speaking, SPKE is a technique of randomness reusing. In such schemes, the sender maintains a state to encrypt single or multiple messages. Thanks to this technique, compared with a PKE scheme, SPKE can surprisingly achieve much better encryption performance, e.g., regarding the ElGamal based SPKE scheme, compared with the stateless counterpart DHIES, the exponentiation computations are reduced from two times to one time for the encryption algorithm. A stateful IBE (SIBE) scheme has been discussed, but the security relies on a loose security reduction and a strong complexity assumption.

This paper presents a new SIBE scheme whose security reduction is tighter and the underlying assumption is weaker. The impact can be considered significant because our scheme allows much shorter parameters and more flexibility of choosing group. Furthermore, we study the essence of SIBE scheme by pointing out that what we need to achieve high efficiency is actually only a cryptographic primitive, and we name it stateful identity based key encapsulation mechanism (SIBKEM). We formalize this primitive, and show a composition theorem of SIBKEM and symmetric key encryption. Also, we propose a generic method of constructing such SIBKEM schemes from a well-studied primitive.

Interestingly, our methodology does not stop only in SIBE field: it also affects SPKE research. By employing our technique, one can achieve SPKE scheme based on weak assumption, and also can formalize stateful (public key) key encapsulation mechanism.