論文の内容の要旨

Security Models and Provable Security of Enhanced Signature and Signcryption Schemes
（高機能な電子署名及びサインクリプションの安全性モデルと証明可能安全性）

氏名　　シュルツ　ヤコブ

One of the great achievements of public key cryptography is the construction of digital signatures which provide publicly verifiable authenticity and non-repudiation. Digital signatures have proven to be an invaluable building block in the construction of many higher-level security protocols, and have become a standard cryptographic primitive. However, the development of more complex digital systems and the desire to secure these, have led to the need for *enhanced signatures* which provide additional functionality and security guarantees compared to the basic primitive. While basic signature schemes have been studied for several decades and their security properties are well understood, the enhanced signature schemes are far less mature. In this thesis, we examine two types of enhanced signature schemes which provide natural extensions of the basic signature primitive -- schemes providing control of verifiability and schemes allowing delegation of signing rights.

Firstly, we examine *convertible undeniable signatures* which provide a flexible solution to the problem of controlled verifiability. This type of scheme is desirable when sensitive or confidential data is being signed since the signer will be guaranteed that only the intended verifiers will be able to verify his signatures and that any outsider will not be able to link him to the signed data. We propose a new security model capturing a new essential security requirement for this type of scheme which has not been considered previously. Our new security requirement is based on a concrete attack against a recently proposed scheme. We then propose a new practical and efficient scheme which is provably secure in our improved security model. Furthermore, we examine *on-line non-transferable signatures* which, according to the definition given in this thesis, are a generalization of undeniable signatures. Unlike most undeniable signature schemes (and the related designated confirmer signature schemes), this type of scheme will be secure against attacks by a powerful on-line attacker. We propose a new general approach to the construction of on-line non-transferable signatures and provide a practical and efficient instantiation. Our approach overcomes a number of limitations of the previous work in this area.

Secondly, we examine *proxy signatures* which allow a signer to delegate (a possibly restricted set of) his signing rights to a proxy. This will enable the proxy to construct signatures on behalf of the original signer. This type of enhanced signature scheme has been proposed to be used in a wide range of practical applications, including distributed systems, mobile agent applications, grid computing, and global distribution networks. Despite this, many of the previously proposed proxy signature schemes lack a formal security analysis, and only recently, provably secure schemes have appeared. We propose a new security model for proxy signature schemes which captures a more realistic set of attacks than previous models and reflects the settings in which proxy signatures are likely to be used. Furthermore, we propose a generic construction which is provably secure in our enhanced security model. Lastly, we demonstrate how to extend our security model and construction techniques to the identity-based setting which allows the use of identities instead of ordinary public keys.

Besides the two types of enhanced signature schemes described above, we also examine *signcryption* schemes which, in addition to message authenticity, also guarantee message confidentiality. While this primitive is closely related to signature schemes, signcryption schemes are not required to provide non-repudiation like the other primitives discussed in this thesis. However, signcryption schemes provide an efficient solution to the problem of authenticated message delivery, which makes them desirable in many practical systems. We examine simple but efficient constructions of signcryption schemes providing various levels of security, and propose several optimizations leading to improved efficiency and security guarantees. Furthermore, we show how signature and encryption schemes with a few special properties can be combined in a non-black-box manner to achieve an efficient and secure signcryption scheme. Concrete instantiations of this approach yield the currently most efficient signcryption scheme which provably satisfies the highest level of security in the standard model.