RUB

Strongly Secure Authenticated Key Exchange in the Standard Model

hgi NDS

Zheng Yang

Nowadays many crucial network applications rely on the existence of a confidential channel established by authenticated key exchange (AKE) protocols over public networks. With the rapid development of cyber technology, novel attacks to cryptosystem emerge in an endless stream. This has also led to the development of AKE solutions to provide increasingly stronger security guarantees. In this thesis we focus on provision of practical constructions for AKE protocols which are provably secure in a strong sense without resorting to random oracles.

We first we present three new efficient compilers to generically turn passively secure key exchange protocols (KE) into authenticated key exchange protocols (AKE) where security also holds in the presence of active adversaries. Our compilers are not only a useful tool for the design of new AKE systems with many additional security properties in a modular and less error-prone fashion, but they also help to relax the assumptions on existing, practical key exchange mechanisms which are not known to be provably secure AKE protocols. Security of our compilers is shown in a strong modified CK model where the adversary is allowed to reveal either long-term secret key or state information of the protocol participants and launch theoretically and practically important PKI-related attacks.

On the second, we study the open problem on constructing eCK secure two party AKE protocol without random oracles and NAXOS alike trick. A generic construction satisfying those requirements is given based on well-known cryptographic primitives following the guideline of efficiency. Then a concrete protocol is proposed which is the first eCK secure protocol in the standard model under both standard assumptions and post-specified peer setting (i.e. without knowing any cryptographic information about its communication peer). Both proposed schemes can be more efficiently implemented with secure device than previous works which are eCK secure in the standard model, where the secure device might be normally used to store the long-term private key and to implement codes of protocol which need to be resilience of state leakage.

Finally, we generalize our one-round two party AKE construction to group case that yields an efficient tripartite AKE protocol based on bilinear maps and a candidate group AKE protocol (with more than three members) based on multilinear maps. Up to now they are the first solutions which can be proved secure in the g-eCK model without random oracles. Meanwhile we make first step to show how to simplify the security proof under g-eCK model.