Generic Construction of Designated Verifier Signature from Standard Cryptographic Algorithms

Jun-Rui Wang
Yuan Ze University
inin70201@gmail.com

Abstract

Designated verifier signature (DVS) is a variant of digital signature which can designate a verifier to verify signatures. The key difference between message authentication code and DVS is that there is no initial and shared key in DVS. In this thesis, we propose a new generic construction of DVS from standard cryptographic algorithms. Our DVS construction is very modular and composed of a few fundamentally cryptographic primitives (i.e., message authentication code, public key encryption and collision resistant hash). Based on the DVS construction, we can also obtain a generic construction of threshold designated verifier signature with only slight modification.

System Model

There are two parties in a DVS including a signer and an intended verifier. A signer can generate a DVS on a message for an intended verifier such that the signature can only be verified by the intended verifier's private key. A DVS scheme is composed of five algorithms described as follows:

- **DV-KeyGen(1^λ, i)**: It takes as input a security parameter λ and ID_i, then generates user's public key pk and secret key sk.
- **DV-Sign(m, pk, sk)**: It first generates a DV secret key $k \in \{0,1\}^*$, then takes as input a message m, DV secret key k, the designated verifier public key pk and signer secret key sk and generates the DV signature σ.
- **DV-Verify(pk, sk, m, σ)**: It takes as input a public key of signer pk, a secret key of verifier sk, a message m and signature σ. It outputs 1 if σ is a valid signature for m. Otherwise, returns 0.
- **DV-Signature-Simulation(m', σ, sk, pk)**: It takes as input a message m', a DV signature σ, the secret key of designated verifier sk and the public key of signer pk. It outputs another valid signature σ' for m'.

Conclusions

In this thesis, we propose a generic construction of designated verifier signature from standard cryptographic algorithm system which can extension by replacing algorithm, and an extended construction, threshold designated verifier signature system, it replaced PKE by TD, provides multi-verifier to verify signature, and we provide the security proof details respectively.