ABSTRACT

Digital signature is one of the most important cryptographic primitives with publicly verifiable property and provides authenticity and data integrity. In many real applications, public verifiability property is not preferable. For instance, privacy protecting mechanisms, e-commerce systems and anonymous online communications require the signer to be anonymous, but at the same time the signer must be accountable for the signature. These properties are exhibited in group signature. In applications like user identification system, mobile communication, insurance, banking etc. the verifiable data is sensitive and requires only the designated party to verify the data. Nominative signature finds applications there. When a common message is signed by a number of signers like bitcoin. In that case, it is desirable to have a single compact signature instead of many signatures to reduce storage and communication. Multisignature is useful in such applications.

This thesis presents efficient constructions for a forward secure *group signature*, two designs for *nominative signature* and a *multisignature.* All our constructions are built on top of intractability of standard lattice problems that are hard to solve even in presence of quantum machines. Lattice based cryptosystems have many potential advantages over conventional cryptosystem like asymptotic efficiency, parallel and homomorphic computation, conceptual simplicity, security against quantum adversaries and worst case assumptions.

Our proposed group signature scheme is the *first* lattice based forward secure dynamic group signature scheme, achieving the selective security in the random oracle model. Group signature permits the group manager to issue distinct certificate and secret key to each member of the group. A group member can sign anonymously on behalf of the group and can be traced out only by the group manager. The forward secure property ensures that the signatures issued in the past period remains secure even if the secret key is compromised. The dynamic property refers that the group manager does not fix the keys for the users at the setup phase and if a member is leaving the group, the setup phase does not require to be restarted. The existing lattice based group signature constructions either achieve dynamic property or forward security. In contrast, our design enjoys forward security and dynamic property simultaneously at the cost of increased signature and certificate size. Our construction is proven to withstand mis-identification attack, framing attack and preserves anonymity under the short integer solution and learning with errors assumptions.

We developed *two* constructions of nominative signature schemes from standard assumptions of lattice. Nominative signature allows a nominator and a nominee to sign messages in collaboration so that the signature cannot be produced without the consent of both the parties. The nominee sends a *proof* of validity or invalidity of the signature to a public verifier. This proof convinces the verifier the validity or invalidity of the signature while the signature is verifiable only by the nominee. Our first construction uses decomposition-extension technique and a zero knowledge proof of knowledge using the Fiat-Shamir transform or Unruh transform. The second construction integrates collision resistant preimage sampleable function with symmetric key primitives like collision resistant pseudorandom function and zero knowledge proof system for arithmetic circuits that is made non-interactive using Fiat-Shamir or Unruh transform. We achieve unforgeability, invisibility, impersonation, non-repudiation and non-transferability for both the constructions under the short integer solution and learning with errors assumptions in the random oracle model. The Fiat-Shamir transform enables our constructions to achieve non-repudiation in the random oracle model while the Unruh transform facilitates the same in the quantum random oracle model.

Further, we introduce a lattice based efficient multisignature scheme realizing both signature compression and public key aggregation with a single round of signature generation. In a multisignature, each signer in a group signs a common message and sends it to a designated combiner. The designated combiner combines the received signature to a single signature and issues a multisignature whose size does not grow with the number of signers. Instead, the size of the multisignature is asymptotically equivalent to that of a single signature. We further extend our multisignature to an accountable subgroup multisignature that exhibits the same efficiency and security as that of our multisignature scheme. Our constructions are built in the standard lattice instead of ideal lattice and are proven to be secure in the random oracle model under standard assumptions from lattice.

Keywords: lattice, short integer solution, learning with errors, group signature, dynamic, forward secure, random oracle model, mis-identification, framing, anonymity, nominative signature, preimage sampleable function, pseudorandom function, zero knowledge proof, unforgeability, invisibility, impersonation, non-repudiation, multisignature, accountable subgroup multisignature.