Exact Security of Digital Signatures based on the Discrete-Logarithm Problem

Résumé du projet de recherche (Langue 1)

The basic task in cryptography is to enable to parties to communicate "securely" over an insecure channel, in a way that guarantees confidentiality, integrity and authenticity of their communication (among other possible security goals). The design of cryptographic protocols in order to achieve these goals is a delicate, error-prone and difficult task. The idea of provable security was introduced thirty years ago in the pioneering work of Goldwasser and Micali (for which they received the Turing award in 2013). Their approach relies on the principle that the security of cryptographic schemes is proven secure based on mathematically precise assumptions. This paradigm has been extremely successful and many cryptographic tasks have been put under rigorous treatment and realized under a number of well-studied complexity-theoretic intractability assumptions. However, after almost three decades of active research, all known results for the security of the discrete-logarithm based signatures like Schnorr signatures are given in the random oracle model and impose the loss of a factor nearly q (the number of queries the forger makes to the random oracle) in either execution time or success probability of reductions that convert a forger into an algorithm that extracts discrete logarithms. Paillier and Vergnaud proved in that any algebraic random-oracle-based reduction (i.e. that can only apply group operations on group elements from computing the discrete logarithm to forging Schnorr signatures must lose a factor at least $q^{1/2}$ (and this result was improved to $O(q)$). This shows that a security reduction in the random oracle model, if algebraic, will never be tight.

Résumé du projet de recherche (Langue 2)

There exists discrete-logarithm based signatures with tight security reduction to stronger decisional assumptions but schemes with such reduction to the discrete logarithm problem remain elusive. This is in contrast with factoring-based signatures, where a construction of Katz and Wang showed that by adding only a single random bit to a signed message, one can achieve a tight reduction. Designing a discrete-logarithm based signature scheme with a tight reduction in the random oracle model to the discrete logarithm problem (and not under weaker related ones) or proving than no such scheme exists is a challenging open problem that is the primary goal of this PhD thesis. Besides, in order to protect message authentication codes from birthday paradox attacks, a folklore technique is to add to each message some kind of randomization. It was shown that such public randomization allows one to achieve sometimes optimal exact security. Randomized message pre-processing was also used as a mode of operation for cryptographic hash functions intended for use with digital signatures (in order to base their on properties of the hash function weaker than the collision resistance). These works give rise to many interesting open problems. Among them, this PhD thesis will try to resolve whether it is possible to design simple and efficient variants of randomization that improve the security of digital signatures when used with iterated hash functions (to prevent known attacks).

Informations complémentaires (Langue 1)