Mathematical Science for Information Security

Tsuyoshi TAKAGI

Degree: PhD(Technische Universität Darmstadt)
Research Interests: Cryptography

Cryptography has become one of the most important fields in information technology. Using cryptographic techniques, it is possible to construct many security protocols, which have become the fundamental technology for secure communications, such as SSL and IPsec. These security protocols provide us with several security applications, such as secure payment systems, secure IP networks, and secure mobile networks. Two concepts that play important roles in these practical paradigms are public-key cryptosystems and digital signatures. Without them, the technologies mentioned above would not be possible.. The security provided through application of these concepts is based on certain difficult mathematical problems, e.g., a factoring problem, a discrete logarithm problem over elliptic curves, and lattice theory. In any given case, if the underlying problem is solved, the entire system based on this problem becomes unsecure. One main topic of research is the security of these problems and the implication of this security for cryptographic protocols. To realize these security applications in practice, we have to implement the corresponding security concept on a secure device (like a smartcard). If this implementation is careless, an attacker can easily extract the secret information from the device. For this reason, secure implementation on security devices is another important topic of research.

(1) Provable Security

Security models are needed for the purpose of correctly judging the security level of cryptographic protocols. One standard such model employs semantic security against a chosen ciphertext attack. A provably secure cryptosystem is a cryptosystem whose security can be mathematically verified in a security model. Provable security is theoretically and also practically meaningful, because we have a guarantee that there can be no successful attack in a security model. We are currently engaged in investigating the security of present and future cryptographic protocols.

(2) Efficient Algorithms

We now stand at the beginning of the ubiquitous computing era. Given the present state of technology in the world, we can expect to realize lucrative applications by effectively synthesizing ubiquitous smart devices with cryptography. However, these smart devices (such as smartcards and RFIDs) generally have very limited computational capacity, and therefore we must work toward optimizing the memory and efficiency of the security system. Our research group is presently engaged in the development of new efficient cryptographic algorithms for this purpose.

(3) Security Applications

Cryptographic protocols can provide new application paradigms that cannot be realized without cryptography. For example, using cryptographic protocols, we are able to create electronic payment systems, electronic election systems, electronic auction systems, etc. Some of these systems have already been used in practical applications, and they are rapidly becoming the fundamental infrastructure of our electronic society. In our group, we are constructing more flexible and attractive security applications based on cryptographic protocols.

Recent Achievement

The most essential number-theoretic problem in cryptography is the discrete logarithm problem (DLP) over a finite field. On April 24th, 2012, our research group, together with Fujitsu Laboratories and NICT, jointly achieved a world cryptography record for solving the DLP over a finite field $GF(3^{582})$ of 923 bits. The entire computational time of our implementation required approximately 148.2 days using 252 CPU cores. Our computational results will contribute to the secure use of pairing-based cryptosystems with η_T pairing.