

STORK CRYPTOGRAPHY WORKSHOP

Position Paper of Darmstadt University of Technology, Germany

Authors: Harald Baier, Johannes Buchmann, Tsuyoshi Takagi

Contact: {hbaier,buchmann,ttakagi}@cdc.informatik.tu-darmstadt.de

The aim of the position paper at hand is twofold. First, we want to express our deep interest in taking part of the European cryptographic network established by the STORK project. Second, we point to relevant research topics which should be covered by future cryptological projects within the upcoming European Framework Program.

We assign our priorities to the main area 'foundations', as formulated in the call for contribution. We propose to cover the following subjects in the future research roadmap:

1. Cryptography in the age of quantum computers.
2. Extending the term 'Provably Secure Cryptosystems'.
3. Efficient implementation of cryptographic primitives in constraint environments.
4. Standardization of these extensions.

We discuss our proposals in detail in what follows.

Cryptography in the age of quantum computers

All public-key-cryptosystems of practical relevance base on the intractability of a currently hard mathematical problem. For instance, RSA relies on the difficulty of the integer factorization problem, DSA and elliptic curve cryptography base on the discrete logarithm problem, and lattice based cryptosystems use the difficulty of computing shortest vectors. However, none of the problems has been proven to be at least as difficult as some relevant lower bound. In addition, in case of the integer factorization problem and the discrete logarithm problem, polynomial-time quantum algorithms are known to solve these problems [Sho94].

It is expected that quantum algorithms can not solve all NP-complete problems [NC00]. Furthermore, it is not clear, which cryptographic primitives are amenable to quantum computer attacks. For example, no polynomial-time algorithm is known for breaking lattice based cryptosystems using the quantum computing model.

We therefore propose to investigate cryptographic primitives under the assumption that quantum computers of practical interest exist. The aim is to find mathematical problems being of exponential complexity even if quantum computers are available. The result should be a table showing key-lengths for these cryptosystems if a certain security level is required. This table is comparable to the proposal of Lenstra and Verheul [LV01] for currently used cryptographic primitives.

Our research group has a large experience with development and evaluation of different cryptographic schemes. For instance, we constructed alternative mathematical problems for cryptography like number field based cryptosystems (e.g. [BP98]). No sub-exponential time algorithm has found for some problems over number fields, e.g. the discrete logarithm problem of class groups of number field with increasing degree [BP98].

Extending the term 'Provably Secure Cryptosystems'

Even if the security of a cryptosystem is mathematically proven, it may be amenable to attacks at the implementation level. For example, Manger proposed a chosen ciphertext attack against RSA-OAEP, although this scheme has been mathematically proven to be secure against such attacks [Man01]. Thus we propose that mathematical security models have to be renewed depending on progress of attacks. As explained above, they should consider implementation details.

In addition, further new types of implementation attacks have been proposed. First, the differential fault attack is effective, if an attacker is allowed to cause a physical failure to the cryptographic device storing the secret key [BMM00,JQL99]. For instance, this attack can factor an RSA-modulus by reversing one bit value in the register. Second, side channel attacks allow an adversary to reveal the secret key in the

cryptographic device by observing some side channel information such as the computing time and the power consumption [Koc96,KJJ99]. We remark that an adversary does not have to break the physical device to obtain the secret key. Again we propose to include such attacks in new security models. Again we mention that our group has developed schemes secure against side channel attacks (e.g. [IT02], [Mö101]).

Efficient implementation of cryptographic primitives in constraint environments

In order to achieve a high security level the secret key of a cryptosystem is usually stored on a tamper-free device like a smartcard. Smartcards provide a lot of interesting security applications like personal identification. For instance, the German Digital Signature Act forces everyone to use a smartcard for qualified digital signatures. Many German manufactures have made efforts to implement public-key cryptosystems on smartcards. As smartcards have less computational resources a special coprocessor is used to enhance the speed of a signature generation. However, coprocessors are expensive. It is therefore an important research subject to find public-key cryptosystems, which may be implemented efficiently even in constraint environments.

In the recent past, our group has proposed several efficient algorithms based on number theory, e.g. [BB01], [Tak98].

Standardization of these extensions

Finally, in order to guarantee interoperability, we propose to enforce standardization of the new efforts. The standards will cover provably secure cryptosystems in the extended sense, which may be implemented efficiently in hardware with low resources. This will yield a basis for bringing digital signatures to the market.

We are developing the FlexiProvider that supports the standard algorithms (see www.flexiprovider.de). The FlexiProvider is a provider for the Java Cryptography Architecture. The goal of the FlexiProvider project is to supply fast and secure implementations of cryptographic algorithms which are easy to use even for developers who are not well-footed in the field of cryptography. In addition, using the FlexiProvider allows an easy change of the underlying cryptographic primitive.

Literature

- [BB00] H.Baier, J.Buchmann, "Efficient Construction of Cryptographically Strong Elliptic Curves", INDOCRYPT 2000, LNCS 1977, pp.191–202, 2000.
- [BMM00] I.Biehl, B.Meyer, and V.Müller, "Differential Fault Attacks on Elliptic Curve Cryptosystems", CRYPTO 2000, LNCS 1880, pp.131–146, 2000.
- [BP98] J.Buchmann and S.Paulus, "A One Way Function based on Ideal Arithmetic in Number Field", Crypto'97, LNCS 1294, pp.384–394, 1997.
- [IT02] T.Izu, T.Takagi, "A Fast Parallel Elliptic Multiplication Resistant against Side Channel Attack", PKC 2002, LNCS 2274, pp.280–296, 2002.
- [JLQ99] M.Joye, A.Lenstra, and J.–J.Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults", J. of Cryptology 12 (4), pp.241–245, 1999.
- [Koc96] C.Kocher, "Timing attacks on Implementations of Diffie–Hellman, RSA, DSS, and other systems", CRYPTO 96, LNCS 1109, pp.104–113, 1996.
- [KJJ99] C.Kocher, J.Jaffe and B.Jun, "Differential power analysis", CRYPTO 99, LNCS 1666, pp.388–397, 1999.
- [LV01] A.Lenstra, and E.Verheul, "Selecting Cryptographic Key Sizes", J. of Cryptology, 14, pp.255–293, 2001.
- [Man01] J. Manger, "A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS#1 v2.0," CRYPTO 2001, LNCS 2139, pp.230–238, 2001.
- [Mö101] B.Möller; "Securing Elliptic Curve Point Multiplication against Side–Channel Attacks", ISC 2001, LNCS 2200, pp.324–334, 2001.
- [NC00] M.Nielsen, and I.Chuang, "Quantum Computation and Quantum Information", Cambridge Press, 2000.
- [Sho94] "P.Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring", In Proceedings, 35th Annual Symposium on Foundations of Computer Science, IEEE press, pp.124–134, 1994.
- [Tak98] T.Takagi, "Fast RSA–Type Cryptosystem Modulo $\mathbb{Z}/k\mathbb{Z}$," Advances in Cryptology – CRYPTO '98, LNCS 1462, pp.318–326, 1998.