Control and Cybernetics

vol. **36** (2007) No. 4

Book review:

Contemporary Cryptology

by

Dario Catalano, Ronald Cramer, Ivan Damgard, Giovanni Di Crescenzo, David Pointcheval, Tsuyoshi Takagi

The book here reviewed consists of several articles written by different authors. We provide below short characteristics of each of the articles in the book.

1. Efficient distributed computation modulo a shared secret (Dario Catalano)

The article concerns the subject of distributed computation. This is realized by the secret sharing protocols. The author presents several kinds of such protocols: additive sharing over Z or Z_q, and polynomial sharing over Z or Z_q. The mutual conversions among different secret sharing methods are presented. Then, the author considers the distributed modular reduction applying the Newton iteration method. These methods allow for approximating $1/p$, where p is a prime number, in a distributive manner. Moreover, the conventional arithmetical operations, such as adding and multiplication, are performed in a distributive manner. By combining the above ideas, the modular powering, inversion and computation $a(\mod p)$ is made through distributive computation. The joint generation of random values and the modular distributive arithmetic constitute, therefore, a sufficient background for applying the Miller-Rabin probabilistic primality tests, in order to generate the prime numbers in a distributive manner. This is the way, in which cryptographic systems might be generated in a distributive model. Consider, for example, the RSA cryptosystem. If two random primes are generated, we are able to compute their product. Then the encryption and decryption exponents are generated - the first one as a random shared secret and the other as the inverse in the modular arithmetic. In this manner the RSA system could be realized in a distributed way. In the similar manner other public key cryptosystems could be incorporated in distributive computational model.

The distributive model for the RSA cryptosystem was realized for the first time by Boneh and Franklin in 1997. Catalano's article represents a good and elementary introduction in this area. Moreover, what is also important, the efficiency, communication costs and computational bounds for the presented protocols are considered.

2. Multiparty computation, an Introduction (Ronald Cramer, Ivan Damgard)

The lecture deals with the secure multiparty computation, MPC (in the group of n players), first introduced by Yao. The problem is to compute the agreed function of their inputs in a secure way. Generally speaking, security means here that

1. the generated output is correct
2. the private inputs of the players are kept secret even if some of the players cheat.

The protocol is based on the Verifiable Secret Sharing scheme, which allows for distributing the secret value among the players even in the case when the dealer, or some players are cheating. The honest players should be able to reconstruct the secret value, even against the actions of the cheaters. The general corruption model is related to the so-called access structure, where the distinguished authorized subsets of players are able to compute the value of the corresponding function in a secure way. In MPC protocol the following notions are important: definition of the adversaries and their powers, the assumed model of communication and the definition of security. Therefore, two communication models are considered:

– Cryptographic model - when the communication channels are secure, provided the adversary has a limited computational power.
– Information-theoretic model - when security can be guaranteed, even if the adversary has the unbounded computational power.

Furthermore the passive and active corruptions are considered and two types of adversaries: static or adaptive.

Passive corruption means that the corrupted players still execute the protocol correctly, while in case of active corruption this condition is not satisfied.

The adversary is static or adaptive depending on whether the set of the corruptive players ought to be fixed before the protocol starts or not, respectively.

The formal model of security is based on the notion of the Ideal Functionality F (regarded as incorruptible computer) and the Simulator S.

The goal of the protocol is to create (with the presence of the adversary) a situation equivalent to the case where we have F available. More precisely giving to S exactly the data that the protocol is supposed to release to corrupt players, and based on this, it should be possible to simulate toward the environment all the rest that corrupted players would see in a real protocol execution. In the article, the authors generalize the security notion considered before by Canetti (the universally composable security) and prove the protocol security even in the case of the active and adaptive adversary. What is important, the analysis is made in the model of the threshold adversary as well as the general access structure.

3. Provable security for public key schemes (David Pointcheval)

The article concerns the development of the concept of the so called provable security of the given cryptographic protocol. This means that there exists a polynomial reduction of some intractable computational problem to an attack against the given protocol. However, in some cases such reduction may have only theoretical significance, since the practical values of the corresponding protocol parameters are not effectively related to the constant in the suitable polynomial reduction. The author analyses the more adequate notion of the so-called "practical security", meaning that one manages to prove that from an attack, one can describe an algorithm against the underlying problem, with almost the same success probability and within almost the same amount of time. In order to control the efficiency of the corresponding protocol, some models have been proposed in which the concrete objects are identified with the ideal ones. The example is the "random-oracle model", informally introduced by Fiat and Shamir, and formalized by Bellare and Rogaway.

In this article the author presents a good introduction into the area of provable security of cryptographic systems. After the presentation of the suitable formalism he analyses the computational problems: the discrete logarithm problem and the factorization problem. Next he investigates the digital signatures, the suitable attacks and the formal security analysis. In the last section the corresponding methodology is applied for the public key encryption systems. In the last part of the paper he refers to the scheme of Cramer and Shoup for both encryption and signature, with formal security proofs in the standard model.

4. Foundations of Modern Cryptography (Giovanni Di Crescenzo)

This article is devoted to the general introduction to some basic topics in the foundation of modern cryptography. In particular the following primitives are investigated: one-way functions, pseudo-random generators, pseudo-random functions and zero-knowledge protocols. The article starts from some preliminary notions and definitions from the complexity theory introducing the complexity classes: P, NP, BPP and their relation to the corresponding candidates (of arithmetical nature) for the one-way and trapdoor functions. Successively he defines the weak and strong one-way functions and proves that the non-triviality of one class implies the non-triviality of the other. Next he considers the collections of such functions and gives the hypothetical examples of such families.

Then the pseudo-random generators are defined and the section terminates with the theorem stating that the existence of a collection one-way permutations imply the existence of a corresponding family of pseudo-random generators. The last section deals with the zero-knowledge protocols. As an important application there is a construction of perfect zero-knowledge proof system for the Graph Non-isomorphism Problem.

5. Efficient and Secure Public Key Cryptosystems (Tsuyoshi Takagi)

The lecture is a survey of efficient and secure implementations, mainly related to RSA and Elliptic Curve based cryptosystems. In view of the applications to the commonly used systems such as SSL, IPSEC or PKI, the special treatment is concerned with the modular arithmetic. The binary representations of integers are therefore considered and the fast multiplication arithmetic (window method, Montgomery multiplication) are applied. The efficient implementations of different variants of RSA (such as RSA with CRT, multi-prime RSA or multi -exponent RSA) are considered. Then the implementation attacks such as: timing attack, fault attack, SPA/DPA or EPOC attack are presented. The discussion concerning the efficient implementation of the elliptic curve arithmetic is given afterwards (width-w NAF form, efficient coordinate system). The final part of the paper is devoted to the chosen attacks on the Elliptic Curves Cryptosystems such as side channel attacks or Goubin's power analysis attack.

I can strongly recommend the book for an interested reader. It is well written and presents a good survey of problems of modern cryptography. Especially interesting are the articles in the area of the group cryptography and the papers concerning the security of cryptographic protocols.

Jacek Pomykała

Dario Catalano, Ronald Cramer, Ivan Damgard, Giovanni Di Crescenzo, David Pointcheval, Tsuyoshi Takagi, Contemporary Cryptology. Birkhäuser Verlag, Basel-Boston-Berlin, 2005, VIII+237 pages. ISBN 3-7643-7294-X. Price (softcover) 32.00 EUR.