MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 41/1989

# Kryptographie

24.9. bis 30.9.1989

The 1st Oberwolfach conference on cryptography was organized by A.M. Odlyzko (Murray Hill), C.P. Schnorr (Frankfurt) and A. Shamir (Rehovot). There were 32 participants coming from 10 countries, 16 participants came from North America and Israel.

The 29 lectures covered a broad range of actual cryptographic research. Some lectures dealt with traditional subjects such as secret sharing schemes and random number generators using shift registers. Many lectures were given on various types of secret communication such as oblivious transfer, zero-knowledge protocols, bit commitment schemes, multiparty protocols, fault tolerant computation and playing arbitrary games using envelopes. Some lectures presented remarkable new algorithms for factoring large integers and for computing discrete logarithms by sieving in algebraic number fields. A great topic was the construction of pseudo-random generators via hard-core predicates, given any one-way function. This result became possible by a joint effort of a whole group of researchers. Exciting progress has been reported on the bit security of the discrete logarithm. Algorithms were presented for factoring large integers using lattices, for finding integer relations via lattice basis reduction and for identification based on linear codes. Practical solutions were given for efficient signatures by smart cards and for the generation of uniformly distributed prime numbers. Number theoretic solutions were proposed for signatures and key exchange based on quadratic number fields and elliptic curves.

There were vivid discussions during the lectures and active work was going on between the lectures. It was quite a stimulating and active conference.

Abstracts

*G. Simmons:*

## How to set up shared secret and/or shared control schemes without the assistance of a mutually trusted party

(joint work with Ingemar Ingemarsson)

In all shared secret schemes devised until now a trusted party was necessary to construct the private pieces of information (shares, shadows etc.) which when brought together in any authorized concurrence would permit the secret to be reconstructed. In the absence of a trusted party, no one can know the secret and hence it has appeared to be impossible to construct the private pieces of information. We describe a protocol with which a group of participants who don't trust each other and don't trust anyone else either can set up by themselves any shared control scheme that could be set up by a mutually trusted party if one existed. In addition they are able to do this without having to accept any greater risk of their interests being abused than they would have had to accept if a trusted party did set up the scheme.

*E.F. Brickell:*

## On Ideal Secret Sharing Schemes

(joint work with D.M. Davenport)

In a secret sharing scheme, a dealer has a secret. There is a finite set **P** of participants and a monotone set $\Gamma$ of subsets of **P**. A secret sharing scheme with $\Gamma$ as the access structure is a method which the dealer can use to distribute shares to each participant so that a subset of the participants can determine the secret if and only if that subset is in $\Gamma$. The scheme is perfect if a subset of the participants that is not in $\Gamma$ cannot determine any information about the secret. The share of a participant is the information sent by the dealer in private to the participant. A perfect secret sharing scheme is ideal if the set of possible shares is the same as the set of possible secrets. Shamir and Blakley constructed ideal

secret sharing schemes for the case when $\Gamma = \{ P \subset \mathbf{P} : |P| \geq k \}$ for some fixed k. In this paper, we construct ideal secret sharing schemes for more general access structures. We also show that an ideal secret sharing scheme can be viewed as a matroid and that any matroid that is representable over a near field can be used to construct an ideal secret sharing scheme.

*R.A. Rueppel:*

## Stream Ciphers

Stream ciphers encrypt each data unit with a time-varying transformation $E_{Z_i}$ under the control of the keystream. The main problem in stream cipher design is to construct running-key generators (either synchronous or self-synchronizing) that efficiently produce sequences which are indistinguishable from coin tossing sequences.

Four approaches to the solution of this design problem are distinguished: (1) information-theoretic, (2) complexity-theoretic, (3) system-theoretic, (4) provable security, (without unproved hypothesis). The four approaches (and their limitations) are discussed and illustrated by examples.

*H. Niederreiter:*

## Probabilistic results on the linear complexity profile of random sequences

The linear complexity profile measures the extent to which the initial segments of a keystream sequence can be simulated by linear feedback shift register sequences. To provide a benchmark for the assessment of keystream sequences, a probabilistic theory of the linear complexity profile of random sequences is needed. We present a method based on combinatorics and probability theory for establishing probabilistic results for sequences of elements of a finite field. This yields not only a simpler approach to earlier results of the speaker, but also information on sequences of finite length which is of relevance for practical

stream cipher applications. We also extend earlier work of the speaker on frequency distributions to joint frequency distributions.

*S. Micali:*

## Card games are universal

(joint work with Joe Kilian)

We call a game with partial information a card game if its "requirements" can be met by using a stock of cards equal on one side and by "shuffling". Poker is a card game. Card games, at first, appear to be a proper subset of games with partial information.

Consider, for instance, the following game: New Poker. Its requirements are the same as in Poker, except that the players should also know whether or not from the union of their hands it could be extracted a royal flush. It would appear that there is no way to manufacture cards so that the players may find out this bit of information without revealing each other much more information, or even their entire hand. In short, it would appear that they have to rely on an external trusted party - person or machine - to figure that out, or on cryptography, or some other external help.

We show that New Poker can actually be played by the players themselves by only using cards and shuffling. That is, New Poker also is a card game.

More generally, we show that any game with partial information is a card game.

*G. Brassard:*

## Bounded round perfect zeroknowledge

(joint work with Claude Crépeau and Moti Yung)

A perfect zero-knowledge interactive protocol can be used by one party to convince another party of the validity of a statement without disclosing additional

information. Such protocols take place by the exchange of messages back and forth between the parties. An important measure of efficiency for these protocols is the number of rounds in the interaction. In previously known perfect zero-knowledge protocols for statements concerning NP-complete problems, at least k rounds of interaction were necessary in order to prevent one party from having a probability of undetected cheating greater than $2^{-k}$ . This large number of rounds can be a serious handicap for many practical applications.

In this talk, I discussed the notion of bounded-round perfect zero-knowledge. What goes wrong when classic protocols are run "in parallel" in the obvious way? How can this problem be fixed in general? Under the assumption that one-way group homomorphisms exist, I described the first perfect zero-knowledge protocol that offers arbitrarily high security for any statement in NP with a constant number of rounds. In particular, this construction works if it is possible to find a prime $p$ with known factorization of $p-1$, together with a generator $\alpha$ for $\mathbb{Z}_p^*$, such that it is infeasible to compute discrete logarithms modulo $p$ base $\alpha$ even for someone who knows the factors of $p-1$. The assumption is not needed to prove that the first party's secret (the Prover's) is unconditionally protected, but it is necessary to prevent him from cheating. Therefore, the protocol is not an interactive proof in the sense of GMR, but rather an interactive argument (a computationally-sound proof), which is unavoidable for a perfect zero-knowledge protocol unless the polynomial hierarchy collapses.

*S. Micali:*

## Non-interactive zero-knowledge proofs via oblivious transfer

(joint work with Kilian and Ostrovsky)

We show that an Hamiltonian graph G can be probabilistically proved to be Hamiltonian by means of an interactive protocol between a Prover and a Verifier without revealing at all what an Hamiltonian circuit in G may look like.

Such proof makes use of only 2 envelopes as a way to hide data, temporarily or forever. Such a "Zero-Knowledge" proof may be performed by replacing envelopes by digital messages sent from the Prover to the Verifier (but not vice versa)

after the two of them have executed an "oblivious transfer" protocol a number of times that is logarithmic in the probability of error that is judged tolerable.

*C. Crépeau:*

## Oblivious transfer protocols based on natural sources of randomness

A 1/2-Oblivious Transfer (1/2-OT) protocol is a way for a party S to transfer one bit $b_c$ from a pair $(b_0, b_1)$ to another party R that controls the value of c. This must be done in a way such that S will not find out which of the two bits is transfered, while R will not find out anything about the other bit $b_{\neg c}$. The reason to focus on this problem is that it is very powerful, meaning that it can be used as a primitive to achieve very complex and useful similar cryptographic protocols. For instance the Oblivious Circuit Evaluation problem can be solved solely on the assumption that 1/2-OT can be achieved.

This work gives a precise formalization of the notion of cryptographic protocols as well as appropriate definitions for the concepts of reduction among cryptographic protocols and for their security. The other part of this work is to explicitly reduce some of the known cryptographic protocols to one another and eventually consider potential implementation of such protocols in the real world.

One can show easily that 1/2-OT cannot be achieved using message exchange only: some extra assumption has to be used in order to accomplish this protocol. For instance, traditionally this protocol is achieved under some computational assumption. In this piece of work we consider a model where the parties involved in a protocol have access to unlimited computing power. Still we show that under this extreme assumption, it is possible to realize the 1/2-OT protocol as long as the laws of quantum mechanics are right. A uniform source of thermal noise can alternatively be used.

This work is essentially the author's PhD thesis to be defended at MIT in the near future.

*B. den Boer:*

## An implementation of Oblivious Transfer ensuring secrecy almost unconditionally and an unconditional secure Bitcommitment scheme based on factoring

Oblivious Transfer is regarded as a building block for cryptographic protocols. In the literature two implementations are given, one based on quantum mechanics and one based on the difficulty of factoring which protects authenticity. We will give an oblivious transfer which protects secrecy almost unconditionally. Our implementation is based on the Quadratic Residuosity Assumption using a modulus made by the receiver of the bitmessages. This implementation deals equally easy with three "flavors" of oblivious transfer. From this particular implementation we do not need the law of the big numbers to build a bitcommitmentscheme. Instead we directly arrive at an earlier proposed almost unconditionally secure bitcommitmentscheme, based on factoring. At the cost of efficiency we present an idea to make this bitcommitmentscheme completely unconditionally secure, still based on factoring.

*J.M. Pollard:*

## An efficient method of factorization

We describe a factoring method for integers of special form $x^3 + k$, k small; it is related to an algorithm for computing discrete logarithms by Coppersmith, Odlyzko and Schroeppel. For example, take $k = 2$ . We look for pairs of small coprime integers a and b such that

(i) the integer $a + bx$ is smooth,

(ii) the algebraic integer $a + bz$ is smooth in the number field $\mathbb{Q}((-2)^{1/3})$,

which possesses unique factorization - equivalently that its norm $a^3-2b^3$ shall be smooth in the usual sense.

We used the method to repeat the factorization of the Fermat number $F_7$ on a microcomputer (by writing $2F_7 = x^3+2$, $x = 2^{43}$). An improved method has been used recently by A.K. Lenstra and M. Manasse to factor much larger numbers, such as the 126 digit number $n = 7^{149}+1$ (we have $7n = x^5+7$).



*A.M. Odlyzko:*

## Discrete logarithms in prime fields and factorization

Several algorithms are known for computing discrete logarithms in fields GF(p), p a prime, in time $\exp((1+o(1))\sqrt{\log p \log\log p})$. Brian La Macchio and the speaker have implemented the most practical one of these algorithms and used it to compute discrete logarithms modulo a particular 192-bit prime that is used in a Diffie-Hellman type cryptosystem that is currently widely used. An investigation showed that discrete logarithms in prime fields are only slightly more difficult than it is to factor integers of size about p by using the quadratic sieve, and so to be safe, very large primes have to be used. A long part of the project was devoted to investigating the efficiency of various algorithms for solving sparse systems of linear equations over finite fields.

Recently, the Pollard method for factoring Curringham numbers was extended to general integers. Although it is too early to be sure whether the new method is practical, it might yield factorization algorithms that run in time $\exp(c(\log n)^{1/3}(\log\log n)^{2/3})$, and similarly efficient discrete logarithm algorithms for prime fields.

*J. Buchmann:*

## Quadratic fields and cryptography

(joint work with Hugh C. Williams)

The abstract Diffie-Hellman scheme can be described as follows. Let S be a finite set, let $f: S \times \mathbb{Z}_{>0} \to S$ be a function which for every $s \in S$ and $a,b \in \mathbb{Z}_{>0}$ satisfies $f(f(s,a),b) = f(f(s,b),a)$. This function can be used to implement the Diffie-Hellman scheme as follows: Both parties A and B agree on S, f, $s \in S$. A chooses $a \in \mathbb{Z}_{>0}$, transmits f(s,a), B chooses $b \in \mathbb{Z}_{>0}$, transmits f(s,b). Then both parties can find f(f(s,a),b) = f(f(s,b),a).

Using a quadratic order $\mathcal{O}$ of discriminant D one can find secure and efficient implementations of this scheme. If $D < 0$ then we take $S = Cl$ which is the class

group of $\mathcal{O}$. Here we can utilize $f(s,a) = s^a$ for $s \in \mathcal{Cl}$, $a \in \mathbb{Z}_{>0}$. If $D > 0$ then $\mathcal{Cl}$ is expected to be very small with high probability so $\mathcal{Cl}$ is of no use in Cryptography. In this case, however, the set $\mathcal{R}$ of all the reduced principal ideals of $\mathcal{O}$ is roughly of size $\sqrt{D}$ but $\mathcal{R}$ is not a group.

We still succeed to define S and f using $\mathcal{R}$. For both systems we can give proofs for security and efficiency.

*B. Vallée:*

## The use of lattices in cryptography and integer factorization

We show that, even if the factorization of an integer n is unknown, we can solve in polynomial-time polynomial inequations $x^l \equiv y$ modulo n, provided that we have a sufficiently good approximation of the solution.

1) In the particular case of $l = 2$, we can study the set of elements whose squares are less than $O(n^{2/3})$. We obtain a precise description of the gaps between such elements and we build a polynomial-time algorithm which generates such elements in a near uniform way. We use it to derive a class of integer factorization algorithms, the fastest of which provides the best rigorously established probabilistic complexity bound for integer factorization algorithms.

2) In the general case of any l, we can reconstruct truncated roots of polynomials of degree l (mod n) in polynomial-time. This algorithm has numerous practical applications: breaking higher-degree versions of Okomato's recent cryptosystem, and predictability of RSA truncated pseudo-random generators.

Our main tool is lattices that we use after a linearisation of the problem.

*H.R.P. Ferguson:*

## (Non)-Linear Lattice Relation Finding Algorithms

1) Two linear lattice relation finding algorithms PSOS (Ferguson, Notices A.M.S., Bowdoin, 1989-8; Ferguson-Bailey, Math. of Comp., 1989) and HJLS (Ferguson-Forcade, Bull. A.M.S., 1979; Bergman, Berkeley, 1980; Ferguson, Jour. of Algorithms, 1989; Håstad-Just-Lagarias-Schnorr, Journ. of Computing, 1989) have been implemented by D. Bailey, Nasa-Ames, for Cray 2&YMP environment and by G. Cook, Livermore, for a Lambda Lisp-Macsyma symbolic environment. While HJLS tends to be faster and find shorter vectors than PSOS when it finds them, PSOS has lower computational swell, is more stable numerically in producing lower bounds on relations, and finds relations more often. HJLS is known to find relations in polynomial time in the dimension and logarithm of the size of the relation. No such theoretical results are known for PSOS.

2) Both lattice relation finding algorithms and the simpler lattice reduction algorithms can be written in terms of the group $GL(n,\mathbb{Z})$ acting on real matrices. $GL(n,\mathbb{Z})$ consists of invertible degree one polynomial mappings from $\mathbb{Z}^n$ to $\mathbb{Z}^n$. I introduce non-linear lattice relation finding algorithms based on the infinite dimensional group $GP(n,\mathbb{Z})$ of polynomial mappings with polynomial inversers. Of special importance is $GS(n,\mathbb{Z})$, the subgroup generated by the shear transformations $x_i \to x_i + p_i(x_1, \ldots, x_{i-1})$ for multivariable polynomials $p_i$, $1 \le i \le n$. A tame generator conjecture asserts that GL and GS generate GP. The three linear steps of PSOS, for example, sign, permute, and reduce are augmented by a fourth non-linear step shear. A $\mathbb{Z}$-algebraic relation then appears as a polynomial coordinate transformation. A consequent algorithm for factoring multivariable polynomials is given which allows one to work in n-space as compared to a linear relation finding algorithm in $\binom{n+d}{d}$-space for a total degree d factor. Implementation depends upon i) a supply of $\mathbb{Z}$-algebraic independents $e^{\cos(\pi k/p)}$, p prime, suitable k's, ii) if Q divides P in $\mathbb{Z}[x_1, \ldots, x_n]$, then $|Q| \le 2^{\deg(P)-n/2}|P|$, $L_2$ norm (M. Waldschmidt, 1974), iii) if P has a zero $(\xi_1, \ldots, \xi_n)$ of Q such that n-1 of the $\xi$'s are $\mathbb{Z}$-algebraically independent then Q divides P (M. Robinson, SRC, 1989).

*O. Goldreich:*

## A uniform complexity treatment of encryption and zero-knowledge

We provide a treatment of encryption and zero-knowledge in terms of uniform complexity measures. This treatment is justified by our belief that all parties in a cryptographic setting should be modelled by probabilistic polynomial-time machines and that they have access only to objects generated by probabilistic polynomial-time procedures. The advantage in our approach is that it allows to construct secure encryption schemes and zero-knowledge proof systems (for all **NP**) using only uniform complexity assumptions.

We show that uniform variants of the two definitions of security, presented in the pioneering work of Goldwasser and Micali, are in fact equivalent. Such a result was known before only for the non-uniform formalization [MRS].

Non-uniformity is implicit in all previous treatments of zero-knowledge in the sense that a zero-knowledge proof is required to "leak no knowledge" on *all* instances. For practical purposes, it suffices to require that it *is infeasible to find* instances on which a zero-knowledge proof "leaks knowledge". We show how to construct such zero-knowledge proof systems for every language in **NP**, using only a uniform complexity assumption. Properties of uniformly zero-knowledge proofs are investigated and their utility is demonstrated.

The main contribution of this work is in the rigorous demonstration that encryption and zero-knowledge can be treated in terms of uniform complexity and that such a treatment suffices for the practical applications considered in previous works (e.g. [GMW2]).

*J. Stern:*

## Using error correcting codes in cryptography

Let H be an n-k × n - matrix over the two element field. H can be viewed as the faulty check matrix of a linear binary error correcting code consisting of words x such that H.x = 0 .

The weight of a word y of length n is the number of its one bits. It is denoted by |y|. It is usually believed that the problem of finding non-zero words of small weight in a binary code is difficult. On the other hand, the distance of the code (i.e. the minimal nonzero weight of a word of code) can be estimated for random codes as it meets the well known Gilbert Varshamov bound.

Building on these remarks we propose the following protocol for identification: Common to all users is a (randomly chosen) matrix H; furthermore each user has

- a private key s which is a word of length n with a prescribed number $\Phi$ of ones
- a public key i = H.s

In order to identify himself to a verifier B, a user A acts as follows:

1) A picks a random word y and a random permutation $\sigma$ of {1, ..., n} then commits himself (through cryptographic hashing) to $(\sigma, Hy)$ $(\sigma y)$ $(\sigma y \oplus s)$

2) B sends b = 0, 1 or 2

3) A discloses $(\sigma, y)$ if b = 0, $(\sigma, y \oplus s)$ if b = 1 and $(\sigma y, \sigma(y \oplus s))$ if b = 2.

Repetition of this protocol yields an efficient method of identification.

*K.S. McCurley:*

## Some remarks on discrete logarithm cryptosystems

There is no compelling evidence for the difficulty of factoring and computing discrete logarithms other than our own ignorance, and we may someday discover otherwise. For this reason it is desirable to design cryptosystems with the property that if someone can break them, then they must solve several problems thought to be hard rather than just one.

In a 1988 paper in J. of Cryptology, I described a Diffie-Hellman scheme with the property that breaking it requires the ability to factor a modulus n and solve the original Diffie-Hellman problem modulo its prime factors. Another way to combine the difficulty of discrete logarithms and factoring is to choose primes q, r, and p such that qr | (p-1), and use an element of order q in the group $(\mathbb{Z}/p\mathbb{Z})^*$. In this case I am not able to prove that the ability to solve the Diffie-Hellman problem requires the ability to factor qr, but it is easy to prove that the ability

to solve the discrete logarithm problem does require it. A recently announced identification scheme of Schnorr can easily be modified to use this approach for some advantage.

In the analysis of the modified Schnorr scheme, the following problem arises. If you are able to observe the output of a random number generator that gives random integers between 1 and q, then how hard is it to determine q? We show that if an oracle for recognizing q is given, then q can be calculated with probability $1-2^{-k}$ in time $O((qk)^{1/2} + k)$.

*A. Shamir:*

## The discrete log is very discreet

Consider the function $f_{g,n}(x) = g^x \pmod n$ where $n = pq$, $|p| = |q|$, $p \equiv q \equiv 3 \pmod 4$, and where g is a quadratic residue modulo n. In this talk we show that under the sole assumption that factoring such n is difficult, no polynomial time algorithm can compute any of the bits of x given $f(x)$ (except possibly the leftmost $\varepsilon$-fraction of the bits), and no polynomial time algorithm can compute any boolean predicate of the rightmost half of the bits of x given $f(x)$.

*L. Levin:*

## A hard-core predicate for all one-way functions

(joint work with Oded Goldreich)

Function inverting is a challenging task. Consider F(x) that checks whether x is an absolutely complete mathematical proof and outputs its length and the last proven theorem. F is easy to compute, but inverting it amounts to finding a proof of a given size for any given theorem which has one! Still, the problem (known as "P =? NP") of actually proving that some functions are one-way, i.e. easy to compute, hard to invert, remains open.

A reason for F being one-way may be in a particular simple predicate b(x) that is determined by but hard to compute from F(x). Moreover, this bit (predicate) may even be hard to guess with any noticeable correlation (then F must be one-way on most inputs). Such a bit is called a hard-core of F, as it concentrates its one-wayness. (Hypothetical) hard-cores play an important role in foundations of (pseudo)randomness, information, cryptography, and other areas. Blum, Micali and Yao found hard-cores for functions of a special form (assuming there are one-way ones among them). We show that almost every linear predicate is a hard-core for every one-way function.

*M. Luby (Part I), J. Hastad (Part II)*

## Pseudo-random generation from any one-way function

(joint work with Russell Impagliazzo and Leonid Levin)

One of the basic primitives in cryptography and other areas of computer science is a pseudo-random generator. For example, a pseudo-random generator can be used to build secure private key encryption protocols, a zero knowledge proof system for any NP problem, and simulation of Monte-Carlo algorithms using a small random seed.

On the other hand there are many natural problems that are conjectured to be one-way functions. Thus it is desirable to convert what seems to arise naturally (one-way functions) into a valuable commodity (a pseudo-random generator).

We show that the existence of any one-way function is necessary and sufficient for the existence of a pseudo-random generator.

*O. Goldreich:*

## A Note on Computational Indistinguishability

We show that the following two conditions are equivalent:

1) The existence of pseudorandom generators.

2) The existence of a pair of efficiently constructible distributions which are computationally indistinguishable but statistically very different.

*A. Yao:*

## Two Questions in Combinatorial Cryptography

We discuss results on two topics. Firstly, what is the optimal space-time tradeoff for inverting random one-way functions. Secondly, we propose a computationally secure secret-sharing model for general access structures. In particular, we show that, in the latter model, the minimum size of any secure secret-sharing scheme is greater than the circuit complexity and less than the monotone circuit complexity for the membership language associated with the given access structure, assuming the existence of trapdoor functions.

*S. Goldwasser:*

## Multiparty Computation with Faulty Majority

(joint work with Donald Beaver)

We address the problem of performing a multi-party computation when more than half of the processors are cooperating Byzantine faults. We show how to distributively compute any boolean function defined on n inputs such that the privacy of non-faulty processor inputs is maintained, and the faulty processors obtain the function value "if and only if" the non-faulty processors obtain the

function value. If the non-faulty processors do not obtain the correct function value, they detect cheating with high probability. Our solution relies on a new type of verifiable secret sharing in which the secret is revealed via a slow-revealing-process (rather than all at once) where each participant in the verifiable secret sharing discovers the secret "at the same time" as all other participants. Our solution assumes the existence of an oblivious transfer protocol, and that broadcast channels are available. No requirements on processors having equal computing power or equal knowledge of algorithms are made.

*U. Maurer:*

## Fast Generation of Secure RSA-Moduli and Cryptographic Primes with Almost Maximal Diversity

A new method for generating primes is described that differs from the previous approaches in that it yields provable primes (rather than only pseudo-primes), with almost uniform distribution over the primes in a given interval, and in that it is faster than any of the known methods for generating even only pseudo-primes. Moreover, our approach can be adapted, without loss of performance, to the case relevant in cryptography, where the primes must satisfy certain security constraints.

*B. Chor*

## A zero-one law for Boolean privacy

(joint work with Eyal Kushilevitz)

A Boolean function $f: A_1 \times A_2 \times \ldots \times A_n \to \{0, 1\}$ is t-private if there exists a protocol for computing f so that no coalition of size $\leq t$ can infer any additional information from the execution, other than the value of the function. We show that f is $\lceil \frac{n}{2} \rceil$-private if and only if it can be represented as

$$f(x_1, x_2, \ldots, x_n) = f_1(x_1) \oplus f_2(x_2) \oplus \ldots \oplus f_n(x_n)$$

where the $f_i$ are arbitrary Boolean functions. It follows that if f is $\lceil \frac{n}{2} \rceil$-private, then it is also n-private. Combining this with a result of Ben-Or, Goldwasser, and Wigderson, we derive an interesting "zero-one" law for private distributed computation of Boolean functions: Every Boolean function defined over a finite domain is either n-private, or it is $\lfloor \frac{n-1}{2} \rfloor$-private but not $\lceil \frac{n}{2} \rceil$-private.

We also investigate a weaker notion of privacy, where (a) coalitions are allowed to infer a limited amount of additional information, and (b) there is a probability of error in the final output of the protocol. We show that the same characterization of $\lceil \frac{n}{2} \rceil$-private Boolean functions holds, even under these weaker requirements. In particular, this implies that for Boolean functions, the strong and the weak notions of privacy are equivalent.

*D. Chaum:*

## Some open problems and remarks

1) Undeniable Signatures: If the previously published protocol is performed over the multiplicative group modulo an RSA composite then all previous undeniable signatures become RSA signatures, after the multiplicative inverse of the secret key modulo the order of the group is given. A way to show that a pair generate the multiplicative group is needed.

2) An efficient signature scheme based on the RSA assumption is given. It combines Lamport-style signatures with the results of Shamir. It is more efficient that that of Goldwasser et al. at STOC in Boston '83 because the product of the roots is used instead of the separate residues.

3) Transferability of offline digital cash is achieved simply by making the challenge a public function of the payee's valueless signature and passing forward all information recieved by each payer to the next payee.

4) A quick sketch of the spymasters double agent problem was given.

*N. Koblitz:*

## Use of algebraic curves in public key cryptography

The advantage of cryptosystems based on the discrete log problem in the jacobian group $J_C(GF(p^n))$ of a hyperelliptic curve C defined over a finite field (a generalization of elliptic curve cryptosystems) is that no one knows a subexponential algorithm for any case of such a group. To avoid successful attack by the general-purpose Silver-Pohlig-Hellman algorithm, one chooses C and $p^n$ so that $|J_C(GF(p^n))|$ is "almost prime". A necessary condition for almost primality is that the corresponding zeta-polynomial $Z_C(T) \in \mathbb{Z}[T]$ be irreducible over $\mathbb{Q}$, in which case one then has the Mersenne-type problem of finding n such that the norm of the algebraic integer $\alpha^n - 1$ is "almost prime" (where $\alpha$ is a root of $Z_C(T)$).

We investigate irreducibility of $Z_C(T)$ for C of a special form: $y^2 + y = x^d$, $d = 2g + 1$. We have a theorem giving a sufficient condition for irreducibility in terms of class numbers. For example, if $d \equiv 3 \pmod 4$ and if p generates the subgroup of quadratic residues in $(\mathbb{Z}/d\mathbb{Z})^*$, then our condition is that $g \not\equiv q \pmod{12}$ and g.c.d.(g,h) = 1, where h is the class number of $\mathbb{Q}(\sqrt{d})$. Numerical examples are given.

*C.P. Schnorr:*

## Efficient identification and signatures for smart cards

We present an efficient interactive identification scheme and a related signature scheme with the following novel features.

(1) Signature generation consists of a very efficient on-line part and the exponentiation of a random number which is done in a preprocessing stage.

(2) We propose an efficient algorithm to simulate the exponentiation of random numbers. This algorithm is based on the principles of local and internal randomization.

(3) The scheme can be based on any finite cyclic group G and a generator $\alpha$ such that the discrete logarithm $\log_\alpha$ is sufficiently hard.

In particular we consider the following groups G:

- For a prime modulus p and a prime factor q of p-1 let G be the group $\{ a \in \mathbb{Z}_p^* \mid a^{(p-1)/q} \equiv 1 \bmod p \}$
- For a finite field K and a, b $\in$ K let G be the elliptic curve $E_{a,b}$.

Signatures in the new scheme are very short, e.g. less than half the length of RSA-signatures. Signature generation requires about 12 multiplications in the group G.

Berichterstatter: *Michael Kaib* (Frankfurt)

Tagungsteilnehmer

Prof. Dr. Th. Beth
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Haid-und-Neu-Str. 7

7500 Karlsruhe 1

Prof. Dr. J. Buchmann
Fachbereich 10 - Informatik
Universität des Saarlandes
Im Stadtwald 15

6600 Saarbrücken 11

buchmann@sbsvox.uucp.

Prof. Dr. A. Beutelspacher
Mathematisches Institut
der Universität Giessen
Arndtstr. 2

6300 Gießen

Dr. D. Chaum
Centre for Mathematics and Computer
Science
Kruislaan 413

NL-1098 SJ Amsterdam

Prof. Dr. B. den Boer
Stichting Mathematisch Centrum
Centrum voor Wiskunde en
Informatica
Kruislaan 413

NL-1098 SJ Amsterdam

Prof. Dr. B. Chor
Computer Science Department
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

benny@techsel.bitnet

Prof. Dr. G. Brassard
Dept. of Computer Science
University of Montreal
C.P. 6128, Succ. A

Montreal , P.Q. H3C 3J7
CANADA

Dr. C. Crepeau
Dept. of Mathematics
Massachusetts Institute of
Technology

Cambridge , MA 02139
USA

crepeau@theory.lcs.mit.edu
crepeau@lri.lri.fr
(617) 253-5845

Prof. Dr. E. F. Brickell
Applied Mathematics Division
Sandia National Laboratories

Albuquerque , NM 87185
USA

Prof. Dr. H. R. P. Ferguson
Institute for Defense Analyses
Supercomputing Research Center
17100 Science Drive

Bowie , MD 20715-4300
USA

helamanf@super.org
301-805-7355

Prof. Dr. J. Hastad
Dept. of Numerical Analysis and
Computing Science
Royal Institute of Technology
Lindstedtsvägen 25

S-100 44 Stockholm

Dr. W. Fumy
SIEMENS AG
E STE 36
Postfach 3220

8520 Erlangen

M. Kaib
Mathematisches Seminar
Fachbereich Mathematik
der Universität Frankfurt
Postfach 11 19 32

6000 Frankfurt 1

unido!rbiffm!kaib@uunet.uu.net

Prof. Dr. O. Goldreich
Computer Science Department
TECHNION
Israel Institute of Technology

Haifa 32000
ISRAEL

oded@techsel.technion.AC.IL

Prof. Dr. N. Koblitz
Dept. of Mathematics
University of Washington
C138 Padelford Hall, GN-50

Seattle , WA 98195
USA

koblitz@entropy.ms.washington.edy

Prof. Dr. S. Goldwasser
Dept. of Mathematics
Massachusetts Institute of
Technology

Cambridge , MA 02139
USA

shafi@theory.lcs.mit.edu

Prof. Dr. L. A. Levin
Dept. of Computer Science
Boston University

Boston , MA 02215
USA

Dr. C. Günther
Forschungszentrum
Asea Brown Boveri

CH-5405 Baden

günther@research.abb.arcom.ch
+ 41 56 76 82 04

Prof. Dr. M. Luby
International Computer Science
Institute
1947 Center Street
Suite 600

Berkeley , CA 94704-1105
USA

luby@icsi.berkeley.edu

U. Maurer
Inst. f. Signal- und Informations-
verarbeitung
ETH Zürich
Gloriastr. 35

CH-8092 Zürich

umaurer@nimbus.ethz.ch

Prof. Dr. J. M. Pollard
Tidmarsh Cottage
Manor Farm Lane

GB- Tidmarsh, Reading Berksh. RG8 8EX

Prof. Dr. K. S. McCurley
IBM Almaden Resarch Center
650 Harry Road

San Jose , CA 95120-6099
USA

mccurley@sandia.gov
(505) 844-5188

Prof. Dr. R. A. Rueppel
Crypto AG
Zugerstr. 42

CH-6312 Steinhausen

Prof. Dr. S. Micali
Laboratory for Computer Science
Massachusetts Institute of
Technology
545 Technology Square

Cambridge, MA 02139
USA

Prof. Dr. C.P. Schnorr
Mathematisches Seminar
Fachbereich Mathematik
der Universität Frankfurt
Postfach 11 19 32

6000 Frankfurt 1

unido!rbiffm!schnorr@uunet.uu.net
gargoyle.uchicago.edu!schnorr

Prof. Dr. H. Niederreiter
Kommission für Mathematik der
österreichischen Akademie der
Wissenschaften
Dr. Ignaz-Seipel-Platz 2

A-1010 Wien

Prof. Dr. A. Shamir
Dept. of Mathematics
The Weizmann Institute of Science
P. O. Box 26

Rehovot 76 100
ISRAEL

Prof. Dr. A.M. Odlyzko
AT & T
Bell Laboratories
600 Mountain Avenue

Murray Hill , NJ 07974-2070
USA

Prof. Dr. G. J. Simmons
National Security Studies
Sandia National Laboratories
P. O. Box 5800

Albuquerque , NM 87185
USA

Prof. Dr. J. Stern
U. E. R. de Mathematiques
T. 45-55, 5etage
Universite de Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

stern@FRULM 63.bitnet
stern@dmi.ems.fr

Prof. Dr. B. Vallee
Dept. de Mathematiques
Universite de Caen

F-14032 Caen Cedex

Prof. Dr. A. C.-C. Yao
Department of Computer Science
Princeton University

Princeton , NJ 08544
USA

Gefördert durch
DFG Deutsche Forschungsgemeinschaft