Dagstuhl-Seminar 9739 — Cryptography

(22.Sept.1997–26.Sept.1997)

A.Odlyzko, C.P.Schnorr, A.Shamir, J.Stern

The scientific filed of cryptography has been developing very rapidely in recent years. There is a growing number of conferences in cryptography in addition to the annual Crypto and Eurocrypt meetings. However, most of these meetings have a broad focus, and at Crypto and Eurocrypt, in particular, the audience is becoming less scientific as applications of cryptography increase, and as the number of attendees who are not experts increases.

This seminar has given an opportunity for key cryptologists to meet, to interact, to focus on the scientific foundation of cryptography, to identify the current central problems and to work on them. Enough time has been left during the seminar for informal interactions.

The lectures presented at the seminar have covered main directions of current cryptology, emphasizing those areas that are most amenable to mathematical reasoning. Talks have been given on

- new encyrption and signature schemes,
- security of cryptosystems and practical attacks,
- cryptographic aspects in communication networks,
- interactive proof systems,
- secret sharing,
- cryptography and number theory,
- stream and block ciphers

Additionally, some lectures have covered important issues of general interest like key escrow and copyright aspects.

This seminar has continued the tradition of a series of previous workshops at the Centre International des Recherches Mathematiques, Luminy France, the Mathematische Forschungsinstitut Oberwolfach and the IBFI Schloss Dagstuhl (Dagstuhl-Seminar 9339, 27.Sept.–01.Oct.93).

A Concrete Treatment of Symmetric Encryption

M.Bellare, A.Desai, E.Jokipii, **P.Rogaway**

We study notions and schemes for symmetric encryption in a concrete security framework. We give four different notions of security against chosen plaintext attack and analyze the concrete complexity of reductions among them, providing both upper and lower bounds, and obtaining tight reductions. In this way we classify notions (even though polynomially reducible to each other) as stronger or weaker in terms of concrete security. Next we provide concrete security analyses of methods to encrypt using a block cipher, including the most popular encryption method CBC. We establish tight bounds (meaning matching upper bounds and attacks) on the success of adversaries as a function of their resources.

Does Parallel Repetition Lower the Error in Computationally Sound Protocols?

M.Bellare, R.Impagliazzo, M.Naor

Given a protocol with error (probability that an adversary succeeds) a constant, it is natural to try to lower it by repeating the protocol in parallel several times.

Whether or not parallel repetition lowers the error has been a fundamental question in the theory of protocols, with applications in many different areas. It is well known that parallel repetition reduces the error at an exponential rate in interactive proofs and Arthur-Merlin games. It seems to have been taken for granted that the same is true in arguments, or other proofs where the soundness only holds with respect to computationally bounded parties.

We show that this is not the case. Surprisingly, parallel repetition can actually fail in this setting. We present four-round protocols whose error does not decrease under parallel repetition. This holds for any (polynomial) number of repetitions. These protocols exploit non-malleable encryption and can be based on any trapdoor permutation. On the other hand we show that for three-round protocols the error does go down exponentially fast.

The question of parallel error reduction is particularly important when the protocol is used in cryptographic settings like identification, and the error represent the probability that an intruder succeeds. Another important setting is witness hiding protocols.

Full paper available via: `http://www-cse.ucsd.edu/users/mihir`.

On the Limits of Incoercibility

J.Benaloh

Several recent papers have exploited an assumption of "unereasability" of certain kinds of data. This talk examines the unereasability assumption in greater depth and attempts to explore the extent to which this assumption can be justified.

Visual Cryptography with Polarization

E.Biham, A.Itzkovitz

Visual cryptography was introduced by Naor and Shamir as a way to allow fast visual decryption of graphic objects. No decryption device is required; instead decryption is done by fitting slides together. Several schemes were suggested which allow users to share secret pictures (and text) in an information theoretically secure way, so that deciphering is easy if all the shares are given, but it is impossible if one of them is missing. The drawbacks of all the existing methods are the exponentially small contrast of the deciphered picture as the number of shares increases, and the reduction in quality due to pixels' being represented by many smaller (black and white) pixels.

In this talk we suggest new visual cryptographic schemes based on light polarization which are better than the optimal existing schemes. Then we present an ultimate scheme which does not subdivide pixels, and in which the contrast is independent of the number of shares.

Proxy Cryptography

M.Blaze, M.Strauss

We introduce proxy cryptography, in which a proxy function, in conjunction with a public proxy key, converts ciphertext for one key (k_1) into ciphertext for another (k_2). Proxy keys, once generated may be made public and proxy functions applied in untrusted environments. Various kinds of proxy functions might exist; symmetric proxy schemes assume that the holder of k_2 unconditionally trusts the holder of k_1, while asymmetric schemes do not. It is not clear whether proxy functions exist for previously proposed public key cryptosystems such as RSA or ElGamal. We present several new public-key cryptosystems with symmetric proxy functions: an encryption scheme, which is at least as secure as Diffie-Hellman, an identification scheme, which is as secure as discrete log, and a signature scheme derived from the authentication scheme via a hash function. We pose open questions, including whether there exist asymmetric proxy schemes.

Hardcore Bits for Proofs of Knowledge

S.Brands

For various well-known proofs of knowledge, we address the problem of how much information a cheating polynomial-time verifier can learn about individual bits of the prover's secret key. Specifically, under the widely believed assumption that the Schnorr identification protocol is witness hiding, no polynomial-time verifier can distinguish the $O(\log k)$ most significant bits of the prover's secret key from equally many flips of an unbiased coin, where k is the security parameter that determines the key length. For a minor variation of Schnorr's protocol,

not only the $O(\log k)$ most significant bits are hidden but also $O(\log k)$ bits that are close to the least significant bits. Similarly, the $O(\log k)$ least significant bits of the secret key of the prover in the Guillou-Quisquater identification protocol are unapproximable. All our results hold in the strongest conceivable attack scenario, in that verifiers may engage in arbitrarily many protocol executions and choose new challenges in an adaptive fashion based on information learned in previous protocol executions.

Trust & Security: A New Look at the Byzantine Generals Problem

M.Burmester, Y.Desmedt, G.Kabatianski

Secure communication in an open network in the presence of a malicious adversary is a central issue for secure distributed computation. We address the case when the authentication is based on symmetric cryptography.

Our analysis uses the structure of the trust-graph with vertices the processors, and edges corresponding to the shared secret keys. We assume that there is a bound u on the number of faulty (malicious) processors, and that there are at least $2u + 1$ vertex-disjoint paths connecting any two non-adjacent vertices. The adversary controls the faulty processors through which it can create bogus vertices and edges.

The main problem encountered when trying to achieve secure communication in such a scenario is to deal with bogus paths for which some of the vertices are faulty or bogus, and/or some of the edges are bogus.

We consider three cases. The case when the sender and receiver know the trust-graph, the case when only the sender knows the trust-graph, and finally the case when neither the sender nor the receiver know the trust-graph. For all three cases we have secure communication protocols. The protocols are efficient in the first two cases. In the last case our protocol is not efficient.

We are currently working on this problem. We are also considering extensions to public key systems.

Generalizing Proactive Secret Sharing

Y.Desmedt, S.Jajodia

Proactive secret sharing deals with refreshing secret shares, *i.e.*, redistributing the shares of a secret to the *original* access structure. In this paper we focus on the general problem of redistributing shares of a secret key. Shares of a secret have been distributed such that access sets specified in the access structure Γ (*e.g.*, t-out-of-l) can access (or use) the secret. The problem is how to redistribute the secret, without recovering it, in such a way that those specified in the new access structure Γ' will be able to recover the secret.

We also adapt our scheme such that it can be used in the context of threshold cryptography and discuss its applications to secure databases.

A first draft is available at:
`ftp://ftp.cs.uwm.edu/pub/tech_reports/desmedt-redistribution.ps`
or as
Department of Information and Software
Systems Engineering Technical Report ISSE-TR-97-01,
George Mason University, July 1997 at:
`ftp://isse.gmu.edu/pub/techrep/97_01_jajodia.ps.gz`

Extremely Nonlinear Boolean Functions and S-Boxes: Ten Open Problems

H.Dobbertin

An S-box S is optimal resistant against the linear attack if the maximal absolute value of its Walsh coefficient is minimal. If S is a n-bit to n-bit substitution then S is optimal resistant against the differential attack if each equation $S(x+a)+S(x)=b$, a non-zero, has either none or precisely two solutions. We present ten open problems related to the construction and existence of optimal resistant S-boxes.

Secure Communications Over Echo Lines

M.Franklin, **R.Wright**

Motivated by radio communication, we explore networks for which the only communication primitive is to send the *same* message to all neighbors: *echo* lines. Our goal is to design fault tolerant protocols for secure message transmission over such networks. We consider a powerful *Byzantine* adversary that controls some faulty parties but cannot violate the echo constraint. Our results demonstrate a sizable gap between the connectivity required for *perfect* security and for *probabilistic* security. Our results also have implications to the simple channel model and to general secure multiparty computation.

A link to the paper will be available at
`http://www.research.att.com/~rwright`.
The direct link to the postscript will be:
`http://www.research.att.com/~rwright/fw97.ps`.

On the Limits of Non-Approximability of Lattice Problems

O.Goldreich, S.Goldwasser

We show simple constant-round interactive proof systems for problems capturing the approximability, to within a factor of $\sqrt{n}$, of optimization problems in integer lattices; specifically, the closest vector problem (CVP), and the shortest vector problem (SVP). These interactive proofs are for the "coNP direction"; that is,

we give an interactive protocol showing that a vector is "far" from the lattice (for CVP), and an interactive protocol showing that the shortest-lattice-vector is "long" (for SVP). Furthermore, these interactive proof systems are Honest-Verifier Perfect Zero-Knowledge.

We conclude that approximating CVP (resp., SVP) within a factor of $\sqrt{n}$ is in $NP \cap coAM$. Thus, it seems unlikely that approximating these problems to within a $\sqrt{n}$ factor is NP-hard.

Previously, for the CVP (resp., SVP) problem, Lagarias et al showed that the gap problem corresponding to approximating CVP within $n^{1.5}$ (resp., approximating SVP within n) is in $NP \cap coNP$. On the other hand, Arora et al showed that the gap problem corresponding to approximating CVP within $2^{\log^{0.999} n}$ is quasi-NP-hard.

Self-Delegation with Controlled Propagation — or — What If You Lose Your Laptop

O.Goldreich, **B.Pfitzmann**, R.L.Rivest

We introduce delegation schemes wherein a user may delegate rights to *himself*, i.e., to other public keys he owns, but may not safely delegate those rights to *others*, i.e., to their public keys. In our motivating application, a user has a primary (long-term) key that receives rights, such as access privileges, that may not be delegated to others, yet the user may reasonably wish to delegate these rights to new secondary (short-term) keys he creates to use on his laptop when traveling, to avoid having to store his primary secret key on the vulnerable laptop.

We propose several cryptographic schemes, both generic and practical, that allow such self-delegation while providing strong motivation for the user not to delegate rights that he only obtained for personal use to other parties.

Universal Stream Ciphers

J.Golić

A general stream cipher with memory (SCM) mode in which each ciphertext symbol depends both on the current and on the previous plaintext symbols is pointed out. It is shown how to convert any keystream generator into the SCM mode and the security of both the modes is discussed. It is proposed how to construct secure self-synchronizing stream ciphers, keyed hash functions, hash functions, and block ciphers from any secure stream cipher in the SCM mode. Rather new and unusual designs can thus be obtained, such as the designs of block ciphers and hash functions based on clock-controlled shift registers only.

Public Passwords and Their Use For Strong Password Authentication

S.Halevi, H.Krawczyk

his note presents the notion of a *public password* and its applications to achieve strong authentication using human-constrained passwords. The idea is that, similarly to the case of public key cryptography, a user will carry two passwords. One (the *private* password) is like a standard password that is easy to remember and requires secrecy protection. The other (the *public* password) requires integrity protection but not secrecy. Thus, it does not need to be memorized and can be safely written down and carried with the user (on paper, a plastic card, etc.). Although it is not required to be remembered, the public password can still be short enough as to allow a user to recognize it if displayed, or even to type it into a terminal when needed.

To demonstrate the usefulness of this new, simple, notion, we show how it can be used in a few protocols for password-based authentication and key exchange that defeat the usual attacks on password systems, including off-line dictionary attacks. In our protocols, the public password typically consists of a hashed value of some public key in the system. Thus, it is used essentially as a "carried certificate" for that public key.

One of the protocols which we present includes a novel use of a Carter-Wegman type authentication code. This protocol is unique in that its security can be proven based only on standard cryptographic assumptions. Another novel protocol uses the password as an RSA exponent while the inverse exponent for verification is not published but rather stored in the authentication server.

An Efficient Micropayment System Based on Probabilistic Polling

S.Jarecki, A.Odlyzko

Existing software proposals for electronic payments can be divided into "on-line" schemes that require participation of a trusted party (the bank) in every transaction and are secure against overspending, and the "off-line" schemes that do not require a third party and guarantee only that overspending is detected when vendors submit their transaction records to the bank (usually at the end of the day).

We propose a new hybrid scheme that combines the advantages of both of the above traditional design strategies. It allows for control of overspending at a cost of only a modest increase in communication compared to the off-line schemes. Our protocol is based on probabilistic polling. During each transaction, with some small probability, the vendor forwards information about this transaction to the bank. This enables the bank to maintain an accurate approximation of a customer's spending. The frequency of polling messages is related to the monetary value of transactions and the amount of overspending the bank is willing to risk.

The probabilistic polling model creates a natural spectrum bridging the existing on-line and off-line electronic commerce models. For transactions of high monetary value, the cost of polling approaches that of the on-line schemes, but for micropayments, the cost of polling is a small increase over the traffic incurred by the off-line systems.

Another Measure for Resistance Against Differential/ Linear Attack

M.Kanda, **T.Matsumoto**, Y.Takashima

To design block ciphers, it is strongly desired easy-to-calculate measures that can compare their resistance against differential/linear attack. For N-round DES-like ciphers, maximum differential (linear, resp.) characteristic probability DCP^N_{max} (LCP^N_{max}, resp.) is conventionally used. However, evaluating these measures is computationally expensive and becomes hard if the size of blocks and the number of rounds increase. In this talk, we propose to use new measures $UDCP^N_{max}$ and $ULCP^N_{max}$ and prove that $DCP^N_{max} \leq UDCP^N_{max}$ and $LCP^N_{max} \leq ULCP^N_{max}$. When each round function has the same probability DCP^1_{max} (LCP^1_{max}, resp.), $UDCP^N_{max}$ ($ULCP^N_{max}$, resp.) is defined as follows:

$$UDCP^N_{max} = \begin{cases} (DCP^1_{max})^{\lfloor N/2 \rfloor} & \text{for general cases,} \\ (DCP^1_{max})^{\lfloor 2N/3 \rfloor} & \text{when each round function is bijective.} \end{cases}$$

$$ULCP^N_{max} = \begin{cases} (LCP^1_{max})^{\lfloor N/2 \rfloor} & \text{for general cases,} \\ (LCP^1_{max})^{\lfloor 2N/3 \rfloor} & \text{when each round function is bijective.} \end{cases}$$

We demonstrate numerical examples of these measures. New measures $UDCP^N_{max}$ and $ULCP^N_{max}$ can ease conditions for constructing round functions, and thus bring us another design principle of block ciphers.

Chameleon Hashing and Signatures

H.Krawczyk, **T.Rabin**

We introduce *chameleon signatures* that provide with an undeniable commitment of the signer to the contents of the signed document (as regular digital signatures do) but, at the same time, do not allow the recipient of the signature to disclose the contents of the signed information to any third party without the signer's consent. These signatures are closely related to Chaum and van Antwerpen's "undeniable signatures", but they allow for simpler and more efficient realizations than the latter. In particular, they are essentially non-interactive and do not involve the design and complexity of zero-knowledge proofs on which traditional undeniable signatures are based. Instead, chameleon signatures are generated under the standard method of hash-then-sign. Yet, the

hash functions which are used are *chameleon hash functions*. These hash functions are characterized by the non-standard property of being collision-resistant for the signer but collision tractable for the recipient.

We present simple constructions of chameleon hashing and chameleon signatures. The former can be constructed based on standard cryptographic assumptions (such as the hardness of factoring or discrete logarithms) and have efficient realizations based on these assumptions. For the signature part we can use any digital signature (such as RSA or DSS) and prove the unforgeability property of the resultant chameleon signatures solely based on the unforgeability of the underlying digital signature in use.

As a further contribution to the efficiency and practicality of undeniable signatures, we introduce the notion of Undeniable Certificates which in many applications may bring the (amortized) cost of undeniable signatures very close to that of a regular digital signature.

The full version of this paper is available at
`http://www.research.ibm.com/security/chameleon.ps`.

Replication Is Not Needed: Single Database, Computationally-Private Information Retrieval

E.Kushilevitz, **R.Ostrovsky**

We establish the following, quite unexpected, result: replication of data for the computational Private Information Retrieval problem is not necessary. More specifically, based on the quadratic residuosity assumption, we present a *single database*, computationally-private information-retrieval scheme with $O(n^\epsilon)$ communication complexity for any $\epsilon > 0$.

Security Lower Bounds for Pseudo-Random Presignatures

J.Merkle, **C.P.Schnorr**

Let G be a finite cyclic group of order q with generator g. We call a pair $(r, g^r) \in \mathbf{Z}_q \times G$ a *presignature*. The production of random presignatures is the main work for the generation of discrete–log signatures. Schnorr (1991) proposed an efficient generator, De Rooij (1991, 1997) pointed out cryptographic weaknesses. We study *generic attacks* in the spirit of Nechaev (1994), they access the group elements only for group operations and equality tests. We let the prefabricated presignatures (r, g^r) be either public or *semi-public*, i.e. r private and g^r public. We establish security lower bounds against generic attacks including constant, birthday and meet-in-the-middle attacks. In many cases our lower bounds are exact, they match the workload of existing attacks.

On the Generation of Good Elliptic Curves

V.Müller, **S.Paulus**

Elliptic curve cryptosystems become more and more interesting. The trust in the security of suitably chosen elliptic curves has considerably grown in the last years.

We call an elliptic curve "good", if it withstands the knwon attacks computing the discrete logarithm on it. These attacks are of two kinds: group theoretic attacks, wich apply to every finite abelian group (like Babystep Giantstep, Pollard Rho, Pohlig Hellman and Index Calculus) and number theoretic attacks which are special to elliptic curves (like Weil pairing attacks, Galois group and lifting attacks). One can deduce a set of constraints to describe a good elliptic curve.

We compare the two principal approaches to compute good curves, namely the random approach (take coefficients at random, compute the order ofthe curve and check the constraints) and the complex multiplication approach (compute explicitly a curve with the constraints checked in advance). In turns out that both methods have their disadvantages, but that the random approach wins on the long run. More specifically, the complex multiplication approach computes in acceptable time only those few curves which may be susceptible to the lifting attack. Since computing the order of a curve can nowadays be done in a few minutes, this method is the best choice for producing a good curve.

A New Public Key Cryptosystem Based on Higher Residues

D.Naccache, **J.Stern**

This paper describes a new public-key cryptosystem based on the hardness of computing higher residues modulo a composite RSA integer. We introduce two versions of our scheme, one deterministic and the other probabilistic. The deterministic version is practically oriented: encryption amounts to a single exponentiation w.r.t. a modulus with at least 640 bits and a 160-bit exponent. Decryption can be suitably optimized so as to become less demanding than a couple RSA decryptions. Although slower than RSA, the new scheme is still reasonably competitive and has several specific applications. The probabilistic version exhibits an homomorphic encryption scheme whose expansion rate is much better than previously proposed such systems. Furthermore, we prove its semantic security, based on the hardness of computing higher residues for suitable moduli.

How to Copyright a Function?

D.Naccache, J.Stern

We show how to produce different copies of the same function containing user-specific identifiers.

These functions are designed in such a way that information-leakers are either forced to reveal a non-functional code or get traced. The new technique allows natural and easy monitoring of function specifications distributed within an untrusted community.

Would such a technique have been used, the illegitimate disclosures of RC4, A3GSM, Gave, GOST's S-Boxes, etc. would have probably been avoided.

On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited

M.Naor, O.Reingold

Pseudo-random permutations, which were introduced by Luby and Rackoff (SIAM J. on Computing 1988), formalize the well established cryptographic notion of block ciphers. Luby and Rackoff showed a method for constructing a pseudo-random permutation from a pseudo-random function. The method is based on composing four (or three for weakened security) so called Feistel (or DES like) permutations each of which requires the evaluation of a pseudo-random function. We reduce somewhat the complexity of the construction and simplify its proof of security by showing that two Feistel permutations are sufficient together with initial and final pair-wise independent permutations.

The revised construction and proof provide a framework in which similar constructions may be brought up and their security can be easily proved. We demonstrate this by presenting some additional adjustments of the construction that achieve the following:

1. Reduce the success probability of the adversary.
2. Provide a construction of pseudo-random permutations with large input size using pseudo-random functions with small input size.
3. Provide a construction of a pseudo-random permutation using a single pseudo-random function.

We also discuss the application of the framework to the security of remotely keyed encryption.

Paris Metro Pricing

A.Odlyzko

Paris Metro Pricing (PMP) is a simple approach for combined pricing of the Internet and congestion control. The basic approach is to divide a data network into several logically separate channels, each of which would treat packets on a best-effort basis, just as the current Internet does. The only difference between the channels would be in the prices charged for using them. Networks with higher prices would attract less traffic, and thereby provide better service. Price would be the primary tool of traffic management. The advantage of this scheme is that it would allow dispensing with the complexity of end-to-end bandwidth reservations.

PMP is an example of a simple economic solution to a seemingly technological problem. Economic considerations are likely to become increasingly prominent in determining which systems, cryptographic or otherwise, are deployed.

The paper presenting PMP is available at the author's home page `http://www.research.att.com/~amo`.

Asymmetric Cryptography with Multivariate Polynomials over Finite Fields

J.Patarin, L.Goubin

The asymmetric cryptosystems based on multivariate polynomials over a finite field are, according to us, very dangerous and... very exciting.

Very dangerous, because some have been broken in a spectacular way. Moreover, for many of these algorithms, the security is not known to be linked to a clearly defined problem that is considered hard.

Very exciting, because some of these algorithms have incredible properties: very short asymmetric signatures (128 bits long, or even 64 bits), very fast secret key computations, and/or very little RAM for the computation on a smartcard. Last but not least, some of these algorithms are also candidate trapdoor permutations.

At Dagstuhl, we have presented two (so far unbroken) algorithms: HFE (Hidden Field Equations) and 2R (Two Rounds). HFE has very efficient public key computations, and 2R has very efficient secret key computations. Both HFE and 2R can be used for asymmetric encryption, signature, or authentication, and they can generate asymmetric signatures of only 64 bits. Moreover, in the design of 2R, we use only some small S-boxes, and some linear transformations. So, is it easier than expected to design asymmetric cryptosystems ?

Note: One may be surprised by the fact that – in 2R – we have only two rounds (to compare with 16 rounds in DES). However, in our scheme 2R:

1. In each round that uses S-boxes, *all* the input bits are transformed (and not only half of them).
2. The affine transformations are *secret*.
3. In the affine transformation, each output bit is a linear transformation of *all* the input bits (and not only of one input bit, such as in the P transformations of DES).
4. The secret key is large.
5. The S-boxes may be secret.

Strengthened Security for Blind Signatures

D.Pointcheval

This talk addresses blind signature schemes in the random oracle model. Last year, with Jacques Stern, we defined appropriate notions of security for those schemes in the context of electronic cash, namely the $(\ell, \ell + 1)$-forgery which translates the fact that the attacker can spend $\ell + 1$ coins after only ℓ withdrawals. Furthermore, we proposed such provably secure schemes in the random oracle model. Unfortunately, even if our proof prevents $(\ell, \ell+1)$-forgeries, this is only if the number ℓ of withdrawn coins is bounded by a constant. In my thesis, I proposed an improvement of the proof, for the same schemes, which guarantees the security even after poly-logarithmically many withdrawals. This proof can be applied to many witness-indistinguishable based schemes (relatively to factorization, the RSA problem or the discrete logarithm problem).

Here, I propose a generic transformation which makes any such scheme secure, even after polynomially many withdrawals. More precisely, if there exists an $(\ell, \ell + 1)$-forgery for some polynomial ℓ against the transformation, then one can derive a $(\lambda, \lambda + 1)$-forgery against the basic scheme, for λ logarithmically bounded, which has been proven impossible unless the underlying problem, such as factorization or the discrete logarithm problem, is easy to solve. Moreover, this transformation keeps the scheme efficient and so can be used in a secure and efficient anonymous off-line electronic cash system.

Trapdoors, Block Ciphers and Public-Key Encryption

B.Preneel, V.Rijmen

This talk presents several methods to construct trapdoor block ciphers. A trapdoor cipher contains some hidden structure; knowledge of this structure allows an attacker to obtain information on the key or to decrypt certain ciphertexts. Without this trapdoor information the block cipher seems to be secure. It is demonstrated that for certain block ciphers, trapdoors can be built-in that make

the cipher susceptible to linear cryptanalysis; however, finding these trapdoors can be made very hard, even if one knows the general form of the trapdoor. In priciple such a trapdoor can be used to design a public key encryption scheme based on a conventional block cipher.

Partial Exhaustive Search

J.-J.Quisquater

After some historical notes, we will explain how to use a Wiener's exhaustive search machine (using FPGA) when there is not enough time to break a key in the context of encryption or decryption. We will describe 3 contexts where partial exhaustive search is useful: a first example is from a database problem (when people are using forms with a new key for each person), a problem with faulty smart cards when the fault is actively induced during use and a chosen plaintext attack is possible, and finally, we will explain how to break a proposal of key replacement in the context of pay TV. The next part of the talk will be denoted how to modify the Wiener's machine in order to be efficient. We will conclude with the question: Any other example?

Anonymous Web Transactions

M.Reiter, A.Rubin

In this talk we describe a system called Crowds that protects users' anonymity on the world-wide-web. Crowds, named for the notion of "blending into a crowd", operates by grouping users into a large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. Web servers are unable to learn the true source of a request because it is equally likely to have originated from any member of the crowd, and collaborating crowd members cannot distinguish the originator of a request from a member who is merely forwarding the request on behalf of another. We describe the design, implementation, security, performance, and scalability of our system. Our security analysis introduces "degrees of anonymity" as an important tool for describing and proving anonymity properties.

New Publicly Verifiable Secret Sharing Schemes

B.Schoenmakers

A secret sharing scheme at least comprises a *distribution* protocol, in which the secret is distributed by a dealer among several share-holders, and a *recovery* protocol, in which the secret is recovered by pooling the shares of a (qualified) subset of the share-holders. The object of Verifiable Secret Sharing (VSS) is to prevent cheating by the dealer and/or share-holders.

In Publicly Verifiable Secret Sharing (PVSS) schemes, as introduced by Stadler at Eurocrypt'96, it is an explicit goal that anybody can verify that the shares

have been distributed correctly. PVSS can be viewed as an extension of non-interactive VSS, where the level of interaction between the participants is limited to the absolute minimum.

In this talk we present some new PVSS schemes. We distinguish the cases where the secret can be an arbitrary value (even a single bit) and where the secret is a large, random value. In the latter case the resulting scheme is more efficient. Compared to Stadler's solution we achieve improvements both in efficiency and in the type of number-theoretic assumption. More specifically, we show how to reduce the work by a factor of k, where k is a security parameter, and how to avoid the notion of "double discrete logarithms." We discuss some interesting applications of these basic PVSS schemes. Also, we identify a few additional properties which some applications of PVSS rely on, and we show that these properties may again call for more complicated solutions.

How to Photofinish a Cryptosystem

A.Shamir

In this talk I introduce a new paradigm for carrying out massively parallel computations. Instead of using electronic computers (or the other emerging paradigms of DNA computing or quantum computing), I propose using photographic plates or films to represent a single bit in a large number of parallel computations in bit-slice architecture. By computing negatives, overlays, and double exposing, it is possible to compute in parallel up to 2^{40} results.

This scheme is particularly useful in cryptanalysis, and we demonstrate its aplli-cability to the task of breaking exportable DES-like schemes.

Auto Escrowable Auto Certifiable Cryptosystems

A.Young, **M.Yung**

We describe how to solve the "software key escrow" problem such that the solution is a "drop-in" replacement to a public key infrastructure (a public key system with a certification authority). To this end we develop the notion of "Auto Escrowable Auto Certifiable Cryptosystems". We also present an efficient implementation of the notion which was reduced to practice (programmed).
