Eurocrypt'2000
Conference Report

May 15–18, 2000
Bruges

Richard Graveman
Telcordia Technologies
Morristown, NJ USA
rfg@acm.com

Welcome

This was the nineteenth annual Eurocrypt conference. Thirty-nine out of 150 papers were accepted, and there were two invited talks along with the traditional rump session. About 480 participants from 39 countries were present. Bart Preneel was Program Chair. The Proceedings were published by Springer Verlag as *Advances in Cryptology—Eurocrypt'98, Lecture Notes in Computer Science*, Volume 1807, Bart Preneel, editor.

Session 1: Factoring and Discrete Logarithm, Chair: Bart Preneel

Factorization of a 512-bit RSA Modulus, *Stefania Cavallar* (CWI, The Netherlands), Bruce Dodson (Lehigh University, USA), Arjen K. Lenstra (Citibank, USA), Walter Lioen (CWI, The Netherlands), Peter L. Montgomery (Microsoft Research, USA and CWI, The Netherlands), Brian Murphy (The Australian National University, Australia), Herman te Riele (CWI, The Netherlands), Karen Aardal (Utrecht University, The Netherlands), Jeff Gilchrist (Entrust Technologies Ltd., Canada), Gérard Guillerm (École Polytechnique, France), Paul Leyland (Microsoft Research Ltd., UK), Joël Marchand (École Polytechnique/CNRS, France), François Morain (École Polytechnique, France), Alec Muffett (Sun Microsystems, UK), Chris and Craig Putnam (USA), Paul Zimmermann (Inria Lorraine and Loria, France)

The authors factored the RSA challenge number RSA-512 with the general number field sieve (NFS). The algorithm has four steps: polynomial selection, sieving, linear algebra, and square root extraction. For N known to be composite, two irreducible polynomials with a common root mod N are needed. f_1 (of degree 5 in this case) should have many roots modulo small primes as well as being as small as possible. f_2 is simply $x - m$. The idea in choosing f_1 is to keep the higher-order coefficients small while manipulating the lower-order ones to maximize the number of roots mod small primes. They spent one month with 300 workstations to find a polynomial with yield 13.5 times better than the average of such skewed polynomials. The sieving step took four months and produced 130.8 million relations, i.e., (a, b) pairs such that both $f_1(a/b)b^5$ and $f_2(a/b)b$ are smooth over their respective factor bases. Post processing was used to remove duplicate, singleton, and erroneous relations and then to merge equations in when a prime (or prime ideal) occurred eight or fewer times. The resulting system had about 6.7 million equations with average column weight of 62. A modified block Lanczos process was run on a Cray using 2G bytes of RAM to find several dependencies in 225 hours, and then a square root in the splitting field of f_1 over $\mathbf{Q}$ was computed with Montgomery's algorithm.

An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves, *Pierrick Gaudry* (École Polytechnique, France)

This is an algorithm for computing discrete logarithms on the Jacobians of hyperelliptic curves, which were proposed for cryptographic use by Koblitz (*J. Crypt.*, 1989). For small genus, the parallel Pollard-ρ method is the best-known algorithm, but for larger genus, this work showed that there exists a subexponential algorithm. Genus 1 is an elliptic curve. For higher genus, the curve itself is not a group, but on its Jacobian, which is represented by a set of pairs of polynomial divisors, a group can be defined. Cantor's algorithm allows the group law to be computed quickly. The Hasse-Weil bound is an estimator for the group size, but computing the exact group size is generally difficult. As with

elliptic curves, the Frey-Rück algorithm can be used in the supersingular case to compute discrete logarithms. For the general case, they applied the Haffner-McCurley algorithm. For large genus, the complexity is $O(q^2 + qg!)$, where q is the field size. The algorithm works by defining prime divisors and using smoothness over a factor base. As in the Pollard-ρ method, a pseudo-random walk is generated, but here the *smooth* points are retained, until enough are found to compute dependencies over the factor base. The $g!$ term comes from the smoothness probability. The cross-over with the Pollard-ρ algorithm (which is $O(q^{g/2})$)is about $g = 4$. He noted that automorphisms on curves can be used to build faster crypto systems but also help the attacker. Applications to Weil descent may allow better attacks on certain elliptic curve systems (see Galbraith, Hess, and Smart, 1999).

Analysis and Optimization of the TWINKLE Factoring Device, *Arjen K. Lenstra* (Citibank, USA), Adi Shamir (The Weizmann Institute, Israel)

Many factoring algorithms (in particular, the quadratic sieve [QS] and NFS) use sieving followed by a matrix step. This talk was about the sieving step. The NFS uses line sieving and lattice sieving. Both types require post-processing and lattice sieving also requires significant pre-processing. TWINKLE does not help with pre-processing, post-processing, or re-sieving. It works by reversing time and space for sieving and inspecting all primes simultaneously. It uses a 15 cm x 25 cm GaAs wafer with 10,000 LEDs for optical output. After the initial design was described, many doubts about its feasibility were expressed. Also, many non-optical solutions were proposed. But analog adders are too slow due to the high capacitance of wires, digital adders with binary numbers represented by trees need more area and power than LEDs, and systolic arrays have the same problems. So these alternative designs have been rejected, but several improvements have been made. Slowing the device down reduces the power requirement, and ripple counters also help. An optical feedback path now handles reports to solve the re-sieving problem. The original wafer had 10^5 cells, which, for QS, becomes insufficient above 384 bits. But for QS on 384-bit composites, using 11 PCs, using TWINKLE results in a speed-up factor of 65 over the QS without TWINKLE. For 512 bits, a single TWINKLE device simply does not help. However, with 50 wafers, it would succeed in two years. For the NFS, substantially more cells are needed. TWINKLE is extremely efficient for line sieving. Running 10 devices at 1 GHz, 512-bit factoring would take 30 weeks with five supporting PCs for an improvement ratio of seven. For lattice sieving, the idea is to change the contents of the A and B registers between intervals. The improvement ratio is only 2.3, but the design may actually be practical. Another design with 5000 TWINKLEs and 80,000 PCs can sieve a 768-bit number in half a year, but then there is the matrix step. The 80,000 PCs could handle the matrix in three months if "properly networked."

Session 2: Cryptanalysis I: Digital Signatures, Chair: Hans Dobbertin

Noisy Polynomial Interpolation and Noisy Chinese Remaindering, *Daniel Bleichenbacher* (Bell Laboratories, USA), Phong Q. Nguyen (École Normale Supérieure, France)

At STOC'99, Naor and Pinkas introduced a two-party protocol called secret polynomial evaluation. It is useful for two-party RSA key generation and multi-party list intersection. There are also applications to password authentication schemes (see Monrose, CCS'99). Noisy polynomial interpolation (NPI) involves determining P given sets of points on lines, some of which are on the polynomial. The companion problem is reconstruction of P when the possible points are not on lines. It turns out that the first problem appears to be easier than the second. Guruswami and Sudan (FOCS'98) gave an error-correcting algorithm for both problems. In this work, they described a meet in the middle construction and showed how lattice basis reduction can help. They gave a reduction from NPI to the shortest vector problem in a lattice and verified their results experimentally. Most Chinese Remaindering problems can be converted into noisy polynomial problems.

A Chosen Message Attack on the ISO/IEC 9796-1, Signature Scheme, *François Grieu* (Innovatron, France)

ISO/IEC 9796-1 is based on RSA. It was designed in 1989 and 1990 and approved in 1990. The idea is not to use a hash function, since the hash function may be a weakness. Redundancy is necessary for any such scheme. The first approach was duplication and padding, but RSA is multiplicative, so this does not work well, and it is also weak against small public exponents. Therefore, the actual method expanded each byte with a local injection. The new attack presented here selects a small pair of integers (a, b) and looks for message pairs with ratio a/b. If two such pairs A/B and C/D are found, then $AD = BC$. Then the multiplicative property of RSA can be used to forge the signature of one message from the signatures of the other three. We can choose $a < b$ and $\gcd(a, b) = 1$. Then A and B are found by computing one 16-bit multi-precision segment at a time. The search then amounts to a graph traversal problem. For a 256-bit modulus, we can choose $(a, b) = (11, 19)$. If the signer controls the message space or a hash function is used, the attack may not be practical, but in any event, the standard is likely to be removed.

Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1, *Marc Girault,* Jean-François Misarsky (France Télécom - CNET, France)

ISO/IEC 9796-1 as described above is a digital signature scheme with message recovery standardized in 1991. It was assumed sound until an attack on a slight variation and then a full attack on the actual system appeared in 1999 (see Coron, Naccache, and Stern [Crypto′99] and Coppersmith, Halevi, and Jutla [*IEEE P1363a* contribution]). Together with these attacks, five potential countermeasures were proposed, but this paper showed that none of these countermeasures is sound either. The first countermeasure can be defeated in most cases with LLL lattice basis reduction. The second and third can now also be attacked with Grieu's method (Eurocrypt′2000, above), and the fourth actually destroys message recovery as well as allowing selective forgery. Naccache also found two new forgeries against the fifth proposal. The second of these is uses new and interesting number theoretic constructions based on sums of two squares.

Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme, *Jean-Sébastien Coron* (École Normale Supérieure, France), David Naccache (Gemplus Card International, France)

This scheme has a proof of security based on a division-intractability assumption on the hash function and the strong RSA conjecture. An assumption like division intractability is weaker than using the random oracle (RO) model. This paper, however, proposed an attack subexponential in the length k of the hash function. The GHR system uses an RSA modulus, but the message appears in the exponent. Finding a division intractable hash function requires searching for a prime exponent, which can take a substantial amount of time, so it was suggested that SHA-1, for example, be used instead. Therefore, they examined the difficulty of finding division collisions on well-known hash functions. It was known that this could be done with $2^{k/8}$ messages, but they actually improved on this. Lenstra's elliptic curve method was used to try to factor values of the hash function and find ones that are smooth. For k = 256, the complexity is 2^{47}, for k =512, 2^{62}, for k = 1024, 2^{86}. To compute the probability that a division collision exists in a set of hash values, they made a heuristic assumption. For a 512-bit hash, $2^{40.5}$ values give a 1% probability. A hash function that only produces prime digests is safe from these attacks.

Session 3: Invited Talk, Chair: Kaisa Nyberg

Mobile telephony has a long history of fraud and eavesdropping. Second generation systems like GSM used cryptography, but the press and scientific community have not accepted these methods. Today, high confidence, third generation systems are being developed in Japan. The speaker is Chair of the 3GPP SA3 Security Committee.

On the Security of 3GPP Networks, *Mike Walker* (Vodafone, UK)

3GPP is Third Generation Partnership Project for CDMA radio systems. Most of the work is being done in this group and ETSI. The security principles were to build on GSM (to enhance interoperability), to correct the problems with GSM, real and perceived, and finally to add new security features as needed. The requirements are authentication, confidentiality on the air link, removable SIMs, operation without user assistance, and minimal trust in the serving network.

GSM only provides access security and does not protect signalling in the fixed network or prevent active attacks (impersonation of a network element [NE]), lawful interception was an afterthought, and a channel can be hijacked. Trust in the terminal identity was misplaced, the system could not be upgraded, and users were given insufficient feedback about security. The crypto algorithms were never trusted. (In 1987, open crypto processes would have been totally infeasible.) Keys were too short; A5/1 needs to be replaced, but algorithm replacement is hard; COMP-128 was an ill-advised choice. User traffic and signalling are in the clear on microwave links. Keys are transferred in the clear between networks. The biggest threat however, is the deployment of rogue base stations. These allow the identity of mobile-originated calls to be intercepted, and cloning follows. The 3GPP will solve these problems.

They have designed a 3-layer architecture. Authentication is now two way and establishes cipher and an integrity keys. Key freshness and an authenticated management protocol are provided. The protocol uses challenge and response and also produces an anonymity key. All keys are 128 bits, and MACs are 64 bits (except for signalling messages). Air interface encryption applies to all user traffic and signalling. A stream cipher called Kasumi is the default, but null encryption and other algorithms can be used. The ciphering is at a low layer and applies also to the microwave link. The integrity mechanism is similar in scope and strength, but integrity is mandatory. However, signalling MACs are only 32 bits long. The mobile initiates algorithm negotiation. Re-authentication is performed when entering a new network or when new keying material is needed.

Security between NEs consists of manual key establishment followed by automatic session key generation and distribution. Security for signalling is in general controversial. Exportability is an issue, but today full-strength algorithms are in vogue. The default crypto and MAC algorithm, Kasumi, is a derivative of MISTY. The design has undergone extensive external evaluation by multiple teams, but only for one month. The algorithms will likely be published on the 3GPP and ETSI Web sites in June 2000 (after their next meeting).

Session 4: Private Information Retrieval, Chair: Christian Cachin

Single Database Private Information Retrieval Implies Oblivious Transfer, Giovanni Di Crescenzo (Telcordia Technologies Inc., USA), Tal Malkin (AT&T Labs Research, work done at Massachusetts Institute of Technology, USA), *Rafail Ostrovsky* (Telcordia Technologies Inc., USA)

In many applications, it is important to hide *which* items are being retrieved from a database (DB). Private information retrieval (PIR) is clearly possible if one downloads the whole database, but the goal is an efficient solution. One was demonstrated in 1995 if the database is replicated into two copies that cannot communicate, and it was shown that an information theoretic solution is impossible without replication. But Kushilevitz and Ostrovsky (FOCS′97) demonstrated a single DB solution based on a cryptographic assumption. Cachin, Micali, and Stadler (Eurocrypt′99) improved this solution later.

Oblivious transfer (OT) comes in many equivalent formulations. One-out-of-two OT works as follows: the first party has two bits; the second party gets one of the bits and no knowledge of the other. The first party gets no information about which bit is received. OT can be the basis for any secure two-party protocol. It is not likely that OT can be based on a one-way function (OWF). One-out-of-n OT is another equivalent formulation, but it is not PIR, because with PIR the user may learn about other bits in the DB, whereas in OT, the user must learn nothing about other bits. They showed that any non-trivial PIR implies OT.

Most likely, PIR cannot be based on any OWF. Also, "secure PIR," i.e., efficient PIR whereby the user does not get more than requested, is a consequence of PIR, given an added security term in the computational complexity. As a primitive, PIR is as important as OT, it is the first communication complexity complete problem, and it implies secure code evaluation.

One-Way Trapdoor Permutations are Sufficient for Non-Trivial Single-Server Private Information Retrieval, Eyal Kushilevitz (IBM T.J. Watson Research Center, USA), *Rafail Ostrovsky* (Telcordia Technologies Inc., USA)

PIR is difficult to implement, even saving only one bit. Kushilevitz and Ostrovsky's (FOCS′97) single DB PIR solution was $O(n^{\epsilon})$ and was based on the quadratic residuosity assumption. Cachin, Micali, and Stadler's (Eurocrypt′99) was $O(\text{polylog}(n))$. These were based on number theoretic or algebraic assumptions. It is known that one-way permutations are unlikely to imply PIR, and the goal is to find the weakest assumptions. This work shows that trap-door one way permutations imply PIR.

In the construction, the user always gets the bit she wants, communications must be less than the size of the DB, and if the DB can predict the bit the user wants, then the trapdoor permutation can be inverted. The construction for a *fixed* database uses hard-core bits and universal one-way hashing from n bits to $n - 1$ bits. This is a multi-round protocol. Ignoring the communications from the user to the DB and ignoring a malicious DB, partition the DB into two blocks and use universal hashing. Then amortize this approach to smaller blocks. The assumption about the fixed DB can be lifted by using interactive hashing.

Single DB PIR is a natural and useful primitive. It trades communications complexity for privacy. This paper showed non-trivial PIR based on general assumptions, but the complexity is not as good as using specific assumptions. The questions are open whether the number of rounds and communication complexity can be reduced.

Session 5: Key Management Protocols, Chair: Paul van Oorschot

Authenticated Key Exchange Secure Against Dictionary Attacks, Mihir Bellare (University of California at San Diego, USA), David Pointcheval (École Normale Supérieure, France), *Phillip Rogaway* (University of California at Davis, USA)

A and *B* want to establish a secure session key (SK) in the presence of an active adversary. The trust models vary: *A* and *B* may have a shared long term key; *B* may have a one-way function of *A*'s key; *A* and *B* may share keys with a third party (Needham-Schroeder). Interleaving attacks must not be damaging, loss of a SK should cause minimal

damage, and loss of a long-term key should not reveal old SKs. Also, dictionary attacks should be unlikely to succeed even against poorly chosen users' secrets, which is a relatively newer requirement. Bellovin and Merritt published EKE in 1992, whereby the components of a Diffie-Hellman (DH) exchange are encrypted with a user's secret. Several other protocols followed.

This work provided new definitions and an analysis of EKE2 (CCS′93). The definitions are prescriptive rather than being given in terms of a simulator. The ideas of freshness and forward secrecy are built in. Finally, the adversary's goal is defined in terms of a test scenario. The query types are Send, Reveal, Corrupt, Execute, Test, and Oracle, and precise semantics are given for each in pseudo-code. The last two are intrinsic to the security definition. A distinction is made between accepting and terminating, and the security definition is given in terms of the probability that an adversary succeeds. The theorem on the security of EKE2, which bounds the success probability of the adversary, uses the Diffie-Hellman assumption and presumes that the relatively smaller number of user's secrets can be sampled efficiently. The proof turns out to be surprisingly hard.

Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman, Victor Boyko (Massachusetts Institute of Technology, USA), *Philip MacKenzie* (Bell Laboratories, USA), Sarvar Patel (Bell Laboratories, Lucent Technologies, USA)

The setting is as above. The parties have a short, shared secret password p subject to dictionary attack, and the network is untrusted. The users want to agree on a fresh and longer session key. Simple challenge and response is subject to a dictionary attack. The client does not have a public key to verify a signature as with SSH or SSL. Intuitively, a solution can be constructed by running DH and hashing the password together with the shared DH secret, but this is vulnerable to active attacks. So they proposed entangling the password in the DH exponent. Many such protocols have been proposed, e.g., EKE and SPEKE, but these have often been broken, and many constructions, like g^{x+p}, do not work. Their construction is simply to multiply the DH value by the hash of the password concatenated with some other values. Unlike the paper above, they proved security in the simulation model using random oracles. The capabilities of the adversary were modeled in an ideal world. Then they used the simulator to reduce security in the real world to security in the ideal world. They also gave a two-round protocol for implicit authentication. Finally, they showed an example for UNIX-like password verifiers using self-certifying ElGamal encryption.

Fair Encryption of RSA Keys, *Guillaume Poupard,* Jacques Stern (École Normale Supérieure, France)

The aim is to ensure that people use encryption fairly, that is, that anybody can verify the correctness of an encryption. The common example is encryption of a secret key that is related to a known public key. All of these problems have theoretical, general zero knowledge (ZK), solutions, which, for the most part, are totally impractical. This work treats only practical solutions. It uses RSA digital signatures, and ZK schemes (Fiat-Shamir, Schnorr). Generally, proofs are easier for systems based on discrete logarithms, whereas factoring-based systems are simpler and more efficient. The problem is similar to bounded range commitment, which uses the strong RSA assumption, but they wished to avoid that approach. Using the ideas of Young and Yung, (Eurocrypt′98), which provided escrow at the time of certification, and Boudot (Eurocrypt′2000), they gave a solution for all kinds of public key (PK) systems: RSA, Rabin, and ElGamal. Their proof tools were Paillier's cryptosystem (Eurocrypt′99), Schnorr's scheme (1989), and Diophantine commitment (Eurocrypt′91) and (Eurocrypt′98).

Session 6: Threshold Cryptography and Digital Signatures, Chair: Torben Pedersen

Computing Inverses over a Shared Secret Modulus, *Dario Catalano* (Universitá di Catania, Italy), Rosario Gennaro (IBM T. J. Watson Research Center, USA), Shai Halevi (IBM T. J. Watson Research Center, USA)

Given an integer f shared among m players, and an integer e with $\gcd(f, e) = 1$, how can the players compute a shared value $e^{-1} \bmod N$? This has applications for distributed RSA key generation and threshold versions of new signature schemes including GHR signatures. Boneh and Franklin (Crypto′97) and Frankel, McKenzie, and Yung (STOC′98) solved the problem. This work improves the inversion part of the solution for shared RSA keys, but this step is simpler than the generation of the primes. They used a single iteration of the Ben-Or, Goldwasser, and Wigderson (BGW) protocol and efficient t-out-of-n secret sharing. The solution starts with a known upper bound N and each player holding a multiple of f of size about N^2. Then each player does a broadcast followed by a computation. The full protocol uses Shamir's secret sharing. Only two rounds are needed, and the protocol is information theoretically secure, but a malicious player can still defeat it. Therefore, error correction is needed. Pedersen's VSS did not provide

tools to check the size of the secret. The two modifications needed were to use a larger field (still based on the discrete log [DL] problem) and a group of unknown order (with the strong RSA assumption).

Practical Threshold Signatures, *Victor Shoup* (IBM Zürich Research Laboratory, Switzerland)

The motivation was to design a Trusted Third Party (TTP) service with optimistic fair exchange. (The TTP is only brought in for dispute resolution.) An asynchronous Byzantine agreement protocol was needed, and this was a missing piece. The DL schemes seem to require synchronization. The RSA systems can be asynchronous but do not have non-interactivity, provable security, and small share size. The central problem in prior work seemed to be interpolation over $\mathbf{Z}_{f(N)}$, where of course, $f(N)$ is unknown, but this is avoided here, as long as one works with Sophie-Germain primes and large enough prime e. The dealer uses polynomial secret sharing over the quadratic residues in $\mathbf{Z}_{N^*}$. The model includes a trusted dealer and a number of servers, from which certain subsets can generate signatures. This scheme, for RSA, is unforgeable and robust (assuming RSA is hard in the RO model), is completely non-interactive, and has small shares O(log(N)). For t corrupted parties and k the number of signers needed, $k \leq t + 1$ for non-forgeability.

Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures, Stanislaw Jarecki, *Anna Lysyanskaya* (Massachusetts Institute of Technology, USA)

A single trusted server may be hard to find, but most servers may be honest, so the goal is to implement cryptography with n servers, of which any t can be corrupted. The idea is to develop practical protocols with the strongest known security (adaptive adversary) for threshold cryptography.

The setting is partial synchrony, point to point links, and broadcast. The definition of security is that the view of the adversary can be simulated. Adversaries can be active and adaptive. Servers have concurrency and are either erasure free or erasure enabled. (In practice, erasures are hard to implement.) With erasure, they gave a tool for turning a statically secure threshold cryptosystem into an adaptively secure one while preserving concurrency. Without erasure, they adapted the result of Canetti, Gennaro, Jarecki, Krawczyk, and Rabin (Crypto′99) to the erasure-free model. The proof techniques use "committed ZK." That is, the prover convinces the verifier that *something* is true, then the prover reveals what was proved later. This is built from trapdoor commitment, e.g., Pedersen commitment. The second building block is an honest verifier ZK proof of knowledge. The prover has the statement, a witness, and randomness. The verifier just has randomness. The protocol has three rounds and uses erasure in an essential way. The security proof shows how to simulate an adversary.

Confirmer Signature Schemes Secure against Adaptive Adversaries, *Jan Camenisch* (IBM Zürich Research Laboratory, Switzerland), Markus Michels (Entrust Technologies, Switzerland)

Signature schemes consist of generation, signing, and verification algorithms. Universal verifiability may be too strong for some applications, so Chaum and van Antwerpen introduced undeniable signatures (Crypto′89), whereby the signer has to be involved in the verification. This raises new problems, because the signer may be unavailable. Therefore, the idea was generalized to confirmer signatures, for which the designated confirmer must not be able to forge signatures. The signer may also specify some policy to the confirmer, and the confirmer may have the ability to convert undeniable signatures to ordinary signatures. This work addressed a signature transformation attack in previous schemes, constructed a new model, and demonstrated a general and practical scheme. The security requirements are correctness, security for the signer, security for the confirmer, and non-transferability of confirmation. To avoid an adaptive attack, the new model includes, in addition to the confirm and disavow protocols, also selective convertibility. The properties needed are separability of the key generation algorithms and perfect conversion. Their scheme satisfying these properties can be built from any ordinary signature scheme secure against adaptive chosen ciphertext attack.

Session 7: Public-Key Encryption, Chair: David Pointcheval

Public-Key Encryption in a Multi-User Setting: Security Proofs and Improvements, Mihir Bellare (University of California at San Diego, USA), *Alexandra Boldyreva* (University of California at San Diego, USA), Silvio Micali (Massachusetts Institute of Technology, USA)

In the simple one-user PK setting, there is a single public key and the ciphertext has no meaning to the adversary. Proofs of security come in different settings: the adversary may have chosen plaintext or chosen ciphertext, and the model may be semantic security or indistinguishability. Attacks like Haståd's on RSA only work in a multi-user setting: encrypting the same message under different public keys. Thus one-user security may not imply multi-user

security. But basic RSA is not even secure in the single user setting. Is RSA + OAEP secure? The idea is to develop systems and security proofs against any attack.

They defined a model in which single user security implies multi-user security via a general reduction for both chosen plaintext and chosen ciphertext attacks. In the indistinguishability model, the advantage of the P-time-bounded adversary to distinguish which of two messages corresponds to a ciphertext must be small. In the multi-user setting, we want the advantage of the adversary to be small, even after having seen the encryptions of related messages under other public keys. For the proof, a hybrid argument is used, because standard simulation did not work. In practice, it may be important that the security bound in a multi-user setting is a multiple of the security in the single user setting, but the bound in this scheme is tight. They also developed improvements for two systems based on the DDH problem: ElGamal and Cramer-Shoup. These improved reductions used existing single-user proofs and the random self-reducibility of the DDH problem.

Using Hash Functions as a Hedge against Chosen Ciphertext Attack, *Victor Shoup* (IBM Zürich Research Laboratory, Switzerland)

Chosen ciphertext security is also called IND-CCA2 or non-malleability. This appears to be a strong and correct definition, because it captures the notion of partial information, which is often of practical importance. The first truly practical scheme is due to Bellare and Rogaway (CCS'93 for the RO model and Crypto'94 for RSA with OAEP). At Eurocrypt'98, Shoup and Gennaro used CDH and DDH in RO model. Cramer and Shoup (Crypto'98) used DDH without the RO model, and Fujisake and Okamoto used CDH (Crypto'99). This new result builds on Cramer and Shoup's. It is DDH-secure without the RO model and CDH-secure with the RO model, and it does pay an undue price in efficiency. This "second line of defense" is the hedge in the title.

In a key encapsulation scheme, the plaintext is a random-looking string generated by the PK encryption process, which is how PK encryption is usually used. K is the random looking string and y is its encryption, so e.g., for RSA + RO model, $K = \mathrm{H}(r)$, $y = r^e \bmod N$. They constructed a secure PK encryption scheme from a key encapsulation scheme by using K as input to a pseudo-random generator. To make an ElGamal-like system chosen ciphertext secure in the RO model, the adversary must make explicit queries, so the simulator sees these, which help it respond to decryption queries. For RSA it is easy to recognize solutions, so it is correspondingly easy to build the simulator correctly. The problem for ElGamal is that it is hard to recognize CDH solutions: this is the DDH problem, so that is why the key encapsulation step helps the proof go through by using the random self-reducibility property of DDH.

Session 8: Quantum Cryptography, Chair: Dan Boneh

Security Aspects of Practical Quantum Cryptography Gilles Brassard (Université de Montréal, Canada), Norbert Lütkenhaus (Helsinki Institute of Physics, Finland), *Tal Mor* (University of California at Los Angeles, CA, USA and College of Judea and Samaria, Israel), Barry C. Sanders (Macquarie University, Australia)

Quantum information processing can efficiently factor integers, solve discrete logs, and destroy most of the PK systems we have, but it also allows quantum key distribution. The basic protocol is due to Bennett and Brasard. Quantum bits have superposition but do not allow redundancy. We can use either of two conjugate bases to measure a qubit, but not both. This is equivalent to the "no cloning" principle, which is why quantum key distribution is secure. The quantum exchange must be followed by error correction and privacy amplification. An adversary that reads and resends causes a 25% error rate, which can be detected. A more general attack is for the adversary to store qubits and read them later. Most of the research today examines more realistic scenarios. The source is imperfect, or the channel and detector are lossy. First, there is the multi-photon effect, which involves superposition. The eavesdropper can peel away one photon from a clump without introducing any noise and wait until its basis is revealed later. The second effect is photons lost during transmission. If the probability of sending two photons is higher than the probability of no loss, the eavesdropper can get the key. An eavesdropper can also control "dark counts," i.e., detections of photons that were not actually sent. This effect was also included in their analysis. In conclusion, about 100 Km is a practical limit, and existing experiments are often actually insecure, given the effects described here. One tool that provides some advantage is parametric down conversion.

Perfectly Concealing Quantum Bit Commitment from Any One-Way Permutation, Paul Dumais (Université de Montréal, Canada), Dominic Mayers (NEC Research Institute, Princeton, USA), *Louis Salvail* (BRICS, Aarhus University, Denmark)

Mayers (*Phys. Rev. Letters*, 1997) proved that quantum bit commitment is impossible, so the idea in this work is to base unconditionally concealing bit commitment in the quantum model on weak computational assumptions. Naor, Ostrovsky, Venkatesan, and Yung (*J. Crypt.*, 1998) did this with interactive hashing, but their approach did not work against a quantum adversary (because there is no quantum "rewinding"). So the question remained as to what the advantages of quantum schemes are and how they compare with their classical counterparts. This new scheme is based on any family of quantum one-way permutations; it is unconditionally concealing and computationally binding. Unlike the classical schemes, it is non-interactive and has computational complexity O(n) qubits, where n is a security parameter. The main open problem is to find candidates for such families of quantum one-way permutations. Another question is how to handle noise on the quantum channel.

Rump Session, Chair: Kevin McCurley

- Efficient Protocols from Homomorphic Threshold Cryptography, Ivan Damgård

  Paillier's cryptosystem is semantically secure, homomorphic, and has a large message space, so it can be used as a tool to build secret sharing, ZK, and, almost immediately, a voting system. Also, he presented a multiparty computation scheme for secure function computation by using a homomorphic threshold cryptosystem instead of VSS. It has linear communications complexity in the number of players and is secure in the RO model.

- Elliptic Curve Systems Too Risky? Or TRoublesome? Arjen K. Lenstra

  This new PK system works in the trace subgroup of size p^2 of $\mathbf{GF}_{p^6}$. The parameters are similar to Schnorr's signature scheme, and the system is easy to set up. Therefore, the system has many of the advantages of elliptic curves.

- The Schoof-Elkies-Atkin Algorithm in Characteristic 2—The previous World Record, Frederick Vercauteren

  Their implementation counts points on curves over $\mathbf{GF}_{2^{161}}$ in about 10 seconds. In 1999, they counted the points on a curve over $\mathbf{GF}_{2^{1999}}$ in 65 days, which was then a world record.

- A New Record in Point Counting on Elliptic Curves, Pierrick Gaudry

  They used Satoh's algorithm and computed the number of points on a curve over $\mathbf{GF}_{2^{3001}}$ in 54 hours, which was far faster than previous approaches.

- A New Tool for Non-Intrusive Analysis of Smart Cards Based on Electro-Magnetic Emissions. The SEMA and DEMA Methods, Jean-Jacques Quisquater

  This attack is orthogonal to and complementary with the various power analysis attacks. They used a small antenna in the vicinity and read DES keys in a manner similar to Kocher's results.

- On the Soundness of Girault's Scheme, Fabrice Boudot

  Soundness can be defined against a weak attacker who cannot choose the public key, and Poupard and Stern proved security in this model (Eurocrypt'98). If the attacker can choose the public key, the soundness proof from Crypto'97 is wrong, because knowing the DL of $-y$ is not equivalent to knowing the DL of y for odd exponent.

- The NESSIE Call for Cryptographic Algorithms, Eli Biham

  This is a three-year project starting in 2000 with participants from eight countries. They are looking for many kinds of primitives including block and stream ciphers, but also other symmetric and asymmetric mechanisms. The criteria are security, market requirements, performance, and flexibility. September 29, 2000 is the submission deadline. See www.cryptonessie.org.

- FPGA Implementation of Modular Exponentiation Using Montgomery Method, Elena Trichina

  They used a Xilinx XC6000 FPGA with 64 x 64 cells. After optimizing the design, they got 800K bits/sec throughput for a 512 bit modulus.

- One Round Secure Computation and Secure Autonomous Mobile Agents, Christian Cachin, Jan Camenisch, Joe Kilian, Joy Müller

  They got the first results for two-party, two-flow, secure function evaluation in the cases in which there is no restriction on the function and either only Alice is bounded or both parties are bounded. The application is to provide protection against malicious hosts. The paper will be presented at ICALP'00.

- Braid Group Cryptosystem, the Arithmetic Key Agreement Protocol, Jim Hughes

The Arithmetica Key Agreement Protocol is based on Artin's braid group. Twists are always with left or right neighbors and can be positive or negative. Multiplication is concatenation. The word and conjugacy problems have been studied for a long time, and the conjugacy problem is reputed to be hard. Birman, Ko, and Lee recently solved the word problem with a canonical form construction (*Math. Res. Letters*, 1999). The cryptosystem uses public generators, secret words, and sets of conjugates of the generators (i.e., a change of basis). Both parties compute the same commutator. This system is extremely fast, but more work on security and encoding is needed.

- Update on UMAC Fast Message Authentication, Phil Rogaway

  UMAC based on universal hashing is much faster than HMAC or CBC MAC. It has provable security and flexible parameters, public-domain code is available, and it is patent free. There is an Internet Draft. With 64-bit MACs and 2^{-60} security, they got performance measurements between one and two cycles per byte on a Pentium. See http://www.cs.ucdavis.edu/~rogaway/umac/.

- Small, Generic, Hard-Core Subsets for the Discrete Logarithm: Short, Secret DL Keys, Claus P. Schnorr

  For a group of prime order q, he showed that the complexity of the DL on subsets of size $q^{1/2}$ is generically as hard as on the whole group. Therefore, half-size seeds can be used to generate keys.

- A Popular Protocol Whose Security Decreases as Key Size Increases, David Naccache

  PKCS#1 version 1.5 uses a pad string of non-zero bytes. The format is flag (byte with value 02), pad, zero byte, and session key. Assume that the 40 least significant bits of the key are zero. Multiply by $(1 - 1/2^{40})^e \bmod N$ and use this message as a probe. This multiplication preserves the flag byte 02 and can be used as a test for the correct format. The chance of success corresponds to the title.

- Necessary and Sufficient Assumptions for Non-Interactive Zero Knowledge Proofs of Knowledge for all *NP* Relations, Giovanni Di Crescenzo

  Characterizing NIZK is a foundational problem in cryptography. Proofs of knowledge are different from proofs of membership. NIZK is similar to NP, except that there is a shared random string. He used extractable commitment strings to get equivalent conditions for the existence of NIZK proofs of knowledge for all of *NP*. His second result presented new constructions of concurrent zero knowledge without complexity assumptions.

- A Proven Source Tracing Algorithm for the Optimal KD Traitor Tracing Scheme, Kaoru Kurosawa, Mixke Burmester, Yvo Desmedt

  Each user has a personal encryption key. If some of these are used to create a pirate key, the pirate key should reveal at least one of the traitors. They constructed a scheme that meets the proven bound on coalition resistance, so their system is optimal. They also gave the corresponding tracing algorithm with a proof that it works.

- Efficient Algorithms for Differential Probability of Addition Modulo 2^n and Related Problems, Helger Lipmaa

  Because addition mod 2^n is an important operation, this may be a design consideration for cryptosystems. They showed a new and efficient algorithm for this problem, which also lets one find, for example, minimal and maximal differentials. Some differentials are impossible.

Session 9: Multi-Party Computation and Information Theory, Chair: Moti Yung

General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme, *Ronald Cramer* (BRICS, Aarhus University, Denmark (work done while at ETH Zürich, Switzerland)), Ivan Damgård (BRICS, Aarhus University, Denmark), Ueli Maurer (ETH Zürich, Switzerland)

Secret sharing assumes that the dealer is honest, so verifiable secret sharing (VSS) was invented to handle an adversary that may corrupt the dealer. Multi-party computation (MPC) emulates a trusted center to perform secure function evaluation. This work investigated the relationship between secret sharing and MPC in the information theoretic security model. The main result is as follows: If M is a linear secret sharing scheme over a finite field (each share is a linear combination of secrets plus the dealer's randomness) with admissible sets G, then there exist efficient VSS and MPC protocols secure against a malicious adversary not in G. A paper by Cramer, Damgård, and Dziembowski (STOC′00) shows that the structure is essential for this result. To prove the result, it is not sufficient to plug Shamir's secret sharing into the Ben-Or, Goldwasser, and Wigderson protocols. They showed an example of MPC of multiplication. In the active adversary case, they used a homomorphic commitment scheme. Corresponding results exist in the broadcast and cryptographic models.

Minimal-Latency Secure Function Evaluation, *Donald Beaver* (CertCo, USA)

The idea is to have Alice's program execute on Bob's data without Bob's learning the algorithm (in an information theoretic sense) or Alice's learning Bob's data. They reduced interaction and latency to a one-round solution for multi-party function evaluation in *NLOGSPACE*. With a trapdoor one-way permutation, encrypted circuit solutions work, but that does not get information theoretic security. The tools included homomorphic VSS, pyramids (inattentive computing), 3×3 matrix products for NC^1, $N \times N$ matrix products for *NLOGSPACE*, secret quadratic forms, and secret group inverse. The one new tool is called inverse-free reduction.

Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free, Ueli Maurer, *Stefan Wolf* (ETH Zürich, Switzerland)

Shannon showed that information theoretic secrecy implies the entropy of the key must be as large as the entropy of the message. But this is pessimistic, because it assumes that Eve has perfect access to the ciphertext. Wyner considered the Wire Tap Channel, in which Eve receives a noisy version of the message. Maurer generalized this model to an interactive communications (*IEEE Trans. IT*, 1993), from which the secret key rate of the channel can be derived. This definition is weak because it does not bound the total information obtained by the adversary. The main result is that the strong definition, whereby this bound e does not depend on the key length N, can be satisfied whenever the weak one can by running the weak protocol and using privacy amplification with extractors.

Session 10: Cryptanalysis II: Public-Key Encryption, Chair: Jean-Jacques Quisquater

New Attacks on PKCS#1 v1.5 Encryption, Jean-Sébastien Coron (École Normale Supérieure and Gemplus Card International, France), Marc Joy (Gemplus Card International, France), *David Naccache* (Gemplus Card International, France), Pascal Paillier (Gemplus Card International, France)

Two new attacks on PKCS#1 v1.5 were described. Unlike Bleichenbacher's attack, these only require chosen *plaintext*. The first applies only to small e and plaintexts ending in many zeros. It works by examining a function D of two encryptions of the same message (with different padding). If the message ends in enough zeros, D may be less than N, a relationship between the two messages can be computed based on factoring D, and Coppersmith's small e attack can be applied. Some technical difficulties like obtaining enough values of D to expect that one can be factored were explained as well. They implemented the attack and applied it with $e = 3$ for RSA-309 (1024 bits). The second attack applies to any e, and it is the first attack on RSA of this sort. It applies only to short messages. Boneh originally pointed it out as an attack on ElGamal.

One of the highlights of the conference took place when the photographer entered the hall, and the speaker responded in rapid sequence with necktie, comb, hair spray, and overhead display of a proof that $NP = P$, which he later admitted only held for the case $N = 1$.

A NICE Cryptanalysis, *Éliane Jaulmes,* Antoine Joux (SCSSI, France)

Chosen ciphertext attacks were presented against NICE and HJPT (which is analogous to ElGamal), two PK systems based on arithmetic in the maximal order (which is a $\mathbf{Z}$ module) of an imaginary quadratic fields with discriminant $\equiv 1 \bmod 4$. (The class group determines an equivalence relation between ideals, and one reduced ideal per equivalence class is used.) NICE works by embedding the message in an ideal. The private computations take place in the class group of the maximal order D_1, and the public computations take place in the class group of the order of discriminant D_q. There is a mapping between the two that is bijective for elements of sufficiently small norm. This bound on the norm is what enables the attack. By encrypting an element of norm just above this bound and obtaining the decryption, a relationship is obtained. It was shown that two ciphertexts are sufficient to recover the key by factoring a 256-bit number. This attack takes only a few minutes on a PC. By adding redundancy to the message (e.g., with a construction like OAEP), the attack is avoided (because one cannot obtain legal chosen ciphertexts).

Efficient Algorithms for Solving Over-Defined Systems of Multivariate Polynomial Equations, *Nicolas Courtois* (Toulon University, France), Alexander Klimov (Moscow State University, Russia), Jacques Patarin (Bull CP8, France), Adi Shamir (The Weizmann Institute of Science, Israel)

HFE (Eurocrypt'96) is a PK system based on multivariate polynomials. Let m be the number of equations and n be the number of variables. They got a subexponential algorithm for the case $m = n + e$. The multivariate polynomial systems used in cryptography are quadratic. The classical algorithms using Gröbner bases (Buchberger, 1965) are impractical for $n > 15$. Shamir and Kipnis attempted to break HFE with re-linearization (Crypto'99). This, however, increases the size of the system. Therefore, the authors of this work introduced a new process called XL. It did not work for $n = m$, but did for $m = n + 1$, $m = n + 2$, etc. Also, the case $m = e\,n^2$ has polynomial time solutions. An extension FXL guesses some of the variables and becomes faster than exhaustive search for large n ($n > 100$).

Cryptanalysis of Patarin's 2-Round Public Key System with S Boxes (2R), *Eli Biham* (Technion - Israel Institute of Technology, Israel)

Patarin proposed several PK systems, one of which is built from the product of two rounds of secret S-boxes sandwiched between three layers of linear transformations. The S-boxes are quadratic Boolean functions. The public key is an equivalent circuit. His attack has complexity about $2^{n/2}$ where n is the block size. It is "black box ," i.e., it does not care about the algebraic structure. The S-boxes and linear transformations are not bijective, and the attack looks for collisions: pairs of plaintexts that have the same ciphertext. The collisions reveal information about the linear transformations. Then one can compute how many S-boxes were "active" (i.e., had different inputs) for a collision. By collecting the collisions with exactly one active S-box for each S-box in turn, a basis for each S-box can be found, and the system unravels. For a block size of 64 bits, the complexity is about 2^{30}; for 128, it is 2^{60}.

Session 11: Invited Talk, Chair: Whitfield Diffie

Colossus and the German Lorenz Cipher, *A. E. Sale* (Bletchley Park Trust)

In cryptology, one has to consider theory, practice, and culture. The speaker, Tony Sale, is responsible for the restoration and museum at Bletchley Park including Colossus, arguably the first digital computer.

There are only four existing German Lorenz machines today. When the people at Bletchley Park first saw the rotor machine, they had been breaking the cipher for two and one half years. It used a 5-bit Baudot code and is a stream cipher based on a pseudo random sequence. The first twelve letters of the message explained the setting of the rotors. On August 30, 1941, a message was sent twice, once in a slightly shortened form. This yielded 4000 characters of keystream, from which certain patterns with a period of 41 were found, and eventually the machine was completely reverse engineered. Each message was encrypted with a different starting position, so it still took days to find the settings needed to crack a message. The process of doing high-speed comparisons of the statistics of the tapes needed to be automated. A major breakthrough was the idea that the physical tape could be simulated in vacuum tube circuits. It took from March to December 1943 to build the machine. The tapes were punched from pen recordings of the intercepts. The clock speed of the major cycle was 5000 Hz, which corresponded to the tape speed. The machine output the statistics from each run. It worked the first time and allowed the Allies to know the position of 58 out of 60 German divisions just before D-Day. After D-Day, 10 more machines were built, and in total 41 million characters of intercepts were decrypted. (The Luftwaffe used the Siemens Geheimschreiber, which was cryptographically stronger, because the tracks on the tapes were inter-related.) He rebuilt the machine from photos, drawings, and fragments, down to the circuit boards on the racks. The reconstruction started in 1994, and they got the replica working in 1996. The Duke of Kent switched it on, with the original designer, Tommy Flowers present in a wheelchair.

Session 12: Zero Knowledge, Chair: Ronald Cramer

Efficient Concurrent Zero-Knowledge in the Auxiliary String Model, *Ivan Damgård* (BRICS, Aarhus University, Denmark)

A prover may be communicating with several verifiers at once, so the question arises whether the verifiers can obtain any additional information, for example, if they cooperate. We know how to do standard ZK proofs and arguments in a constant number of rounds, but this is not so for concurrent ZK. It is not sufficient for the individual proofs to be ZK, because the simulator can be forced to rewind an exponential amount. However, assuming some additional constraints or pre-processing, the rewinding problem can be overcome. This work takes another approach: assume there is a uniform and random string available to all parties as in NIZK. If a PK system is available, the public key of a third party (e.g., the CA) can be used to construct the pseudo random string and with it a three-move concurrent ZK argument or ZK proof of knowledge. The pre-processing result of Dwork and Sahai (Crypto'98) can be based on any one-way function. The crucial technique used here was trapdoor commitments.

In the auxiliary string model, a verifier may be able to send a transcript to a third party and convince the third party that the verifier actually talked to the prover (if the third party trusts the CA). By modifying the scheme and using the verifier's key, this problem can be avoided.

Efficient Proofs that a Committed Number Lies in an Interval, *Fabrice Boudot* (France Télécom - CNET, France)

A commitment scheme has the properties that the committer, Alice, cannot change the value committed, and the second party Bob gets no information about the value before it is revealed. In this case, Alice wants to prove to Bob that x belongs to an interval $[a, b]$. There are applications to gradual release of secrets, e-cash, group signatures, proofs of primality, and so forth. This paper improved on existing results. Belonging to an interval is equivalent to two instances of proving that a committed number is positive. The first construction uses proofs of knowledge of a committed number, proofs of additional properties, and Lagrange's four square theorem. The second uses the fact that every positive integer K can be written as the sum of a square and a number less than $2K^{1/2}$. However, this result is not sharp: K can be written as $(t/2^{131})^2 + (u/2^{262})$ where t is an integer and $0 \le u \le 2^{142}$.

Session 13: Symmetric Cryptography, Chair: Mitsuru Matsui

A Composition Theorem for Universal One-Way Hash Functions, *Victor Shoup* (IBM Zürich Research Laboratory, Switzerland)

Universal hash functions (Carter and Wegman), universal one-way hash functions (Naor and Yung, STOC'89), and collision resistant hash functions (Damgård, Crypto'89) are keyed families of hash function that can be characterized by the time at which an adversary trying to find a collision gets the key. Universal one-way hash functions are not subject to birthday attacks or known cryptanalytic methods and also satisfy Simon's separation result (Eurocrypt'98). They are sufficient for many applications, such as signatures. Thea starting point toward practical constructions is to use building blocks like SHA-1, the Merkle-Damgård composition theorem, and a key that is XORed with the input block at each step. Bellare and Rogaway noted that this does not work for universal one-way hash functions unless one also masks the compression chain value at every step. But the goal is to keep the key short, not proportional to the message length. By using a tree structure, Naor and Yung kept the key size logarithmic in the input size. Bellare and Rogaway, in 1997, improved on this. This paper presented a simpler and more efficient construction. The new scheme is a modification of Bellare and Rogaway's original XOR chain with the masks, but the masks are recycled in a data dependent way.

Exposure Resilient Functions and All-or-Nothing Transforms, Ran Canetti (IBM T. J. Watson Research Center, USA), *Yevgeniy Dodis* (Massachusetts Institute of Technology, USA), Shai Halevi (IBM T. J. Watson Research Center, USA), Eyal Kushilevitz (IBM T. J. Watson Research Center, USA), Amit Sahai (Massachusetts Institute of Technology, USA)

One of the fundamental assumptions of cryptography is that secret keys can be protected. Techniques like tamper resistance, secret sharing, and forward secrecy have been proposed. The question of partial exposure of a key has not been discussed. However, all or nothing transforms (AONTs) have the property that part of the output reveals nothing about the input. So an AONT of the key can be stored instead of the key itself, which avoids damage from partial leakage. Previous constructions of AONTs were weak or heuristic, until Boyko gave definitions and a proof of security for an AONT in the RO model. This work defined three models: perfect (unbounded adversary, no error), statistical (unbounded adversary, negligible error), and computational (bounded adversary, negligible error) and gave efficient, nearly optimal constructions in all three models. The main building block is exposure-resilient functions, whereby the output looks random, even if almost all of the input bits are revealed. Randomness extractors are used in the statistical case.

The Sum of PRPs is a Secure PRF, *Stefan Lucks* (Universität Mannheim, Germany)

For n bit to n bit functions or permutations, the test for pseudorandomness is for an adversary to distinguish outputs of the function from truly random strings. We may bound the number of queries and running time. In practice, one often uses a PRP as a PRF, particularly if the number of queries is less than the birthday bound. But for blocksize 2^{64}, today's disk sizes exceed this bound. Bellare, Krovetz, and Rogaway (Eurocrypt'98), Hall, Wagner, Kelsey, and Schneier (Crypto'98), and Bellare and Impagliazzo (1999) gave previous constructions. This paper gives two new constructions secure beyond the birthday bound based on sums and XORs of PRPs. The key step is maintaining fairness as values of the function are extracted by marking certain pairs as bad.

IACR Business Meeting

The IACR was founded in 1983, has about 1000 members, sponsors three conferences a year, has a journal published by Springer, runs a pre-print server (http://eprint.iacr.org), and issues an electronic newsletter. The University of California (iacrmem@iacr.org) handles membership services. Upcoming conferences are:

- Crypto 2000, August 20–24, Santa Barbara
- Asiacrypt 2000, December 3–7, Kyoto (papers due May 25)
- Eurocrypt 2001, May 6–11 Innsbruck (papers due November 6)
- Crypto 2001, August 19–23, Santa Barbara
- Asiacrypt 2001, December 9–13, Gold Coast

The next newsletter deadline is May 30, 2000. Previous issues can be read at http://www.iacr.org/newsletter/. Additional information can be found on the main site, http://www.iacr.org/.

Session 14: Boolean Functions and Hardware, Chair: Thomas Johansson

Construction of Nonlinear Boolean Functions with Important Cryptographic Properties, *Palash Sarkar,* Subhamoy Maitra (Indian Statistical Institute, India)

Boolean functions are used in many cryptographic settings. Two questions are what properties are desirable and how to construct functions with these properties. For example, for a stream cipher of fixed size n, one wants balanced functions of high degree. Properties include balancedness, algebraic degree (as a multivariate polynomial), non-linearity (distance from affine), correlation immunity, and m-resiliency. These properties are interrelated and cannot all be optimized simultaneously. Bent functions have high non-linearity, but for odd numbers of variables Patterson and Weidemann (PW) showed how to get even higher non-linearity. In this work, they modified these PW functions to get balanced functions and measured the impact on the non-linearity for functions of 15 variables. (For even n they used other techniques.) They used several composition rules to derive general methods of construction and presented examples.

Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions, Anne Canteaut (INRIA, France), *Claude Carlet* (Université de Caen, France), Pascale Charpin (INRIA, France), Caroline Fontaine (Université des Sciences et Technologie de Lille, France)

Shannon's confusion corresponds to non-linearity and diffusion corresponds to the propagation characteristics of the derivatives. Meier and Staffelbach identified functions with maximal non-linearity and perfect propagation called bent. But bent functions are not balanced. Cryptographic functions must be balanced, have high degree, and have high non-linearity. They showed how to use the Walsh spectrum to get bounds on non-linearity. An additional property is correlation immunity, which is related to t-resilience.

Their first result, which is a generalization of Meier and Staffelbach's result, was on the relationship between the sum of squares indicator and the Walsh spectrum. They gave examples of "almost optimal" functions on several variables. Their second result was on the relationship of the propagation criterion to high non-linearity. Next, they weakened the Meier and Staffelbach hypothesis and obtained several equivalent characterizations of almost optimal functions, first for odd n and then for even n. Finally, they showed that any Boolean function with n odd and at most seven unbalanced derivatives is almost optimal and its Walsh spectrum has two magnitudes.

Cox-Rower Architecture for Fast Parallel Montgomery Multiplication, *Shinichi Kawamura,* Masanobu Koike, Fumihiko Sano, Atsushi Shimbo (Toshiba Corporation, Japan)

Montgomery's multiplication mod N works by transforming numbers modulo a power of 2, R, where $R > N$. A Residue Number System (RNS) uses a pairwise co-prime basis to represent a number modulo all of the basis elements. Posch and Posch (*IEEE Trans. Para. Dist. Sys.*, 1995) showed how to use a RNS together with Montgomery multiplication. This lends itself naturally to parallelism, but it is difficult to perform division and comparison in a RNS. However, if the Montgomery constant R is chosen as a power of 2, as it is for the non-RNS case, divisions are just shifts.

Their main result is a base extension representation, so that intermediate products still have a unique representation and do not have to be reduced. The remaining issue is how to construct this base extension efficiently. The straightforward method is to use the CRT twice: to reconstruct x in the original basis and then represent x in the extended basis. The main trick is to pick the original basis elements close to a power of two. This avoids a costly division step in the direct

computation of the values in the extended base. For a 1024-bit modulus, they used 33 basis elements that fit in 32-bit words. With 100MHz hardware, they got about 1 Mbps throughput.

Session 15: Voting Schemes Chair: Markus Jakobsson

Efficient Receipt-Free Voting Based on Homomorphic Encryption, Martin Hirt (ETH Zürich, Switzerland), *Kazue Sako* (NEC Corporation, Japan)

Early electronic voting systems allowed voters to verify that their vote was tallied correctly. However, receipts for voting open the scheme to coercion and vote selling. In paper-based voting, the system is not verifiable, and these issues do not arise. An optimal system would be both verifiable and receipt free. Several protocols have solved this problem by separating the coercer and voter. Benaloh and Tuinstra ([BT94], STOC′94) used a "voting booth." Sako and Kilian ([SK95], Eurocrypt′95) used untappable messages. Deniable encryption (Canetti, Dwork, Naor, and Ostrovsky, Crypto′97) and non-coercible encryption (Canetti and Gennaro, FOCS′96) are also relevant. Mix-nets are less efficient than homomorphic encryption. This work showed that [BT94] is actually not receipt free, and then constructed a faster scheme (t times faster than [SK95], where t is a security parameter) that works with any homomorphic encryption scheme. They showed a scheme for universally verifiable voting, but the encrypted votes are actually receipts. To make it receipt free, authorities control the randomness and generate encryptions for all possible votes. The encrypted votes are shuffled repeatedly by several parties, each of whom tells the voter how the shuffling worked. The next step is to have the authorities prove the shuffling was honest in a way that the voter can verify the proof but cannot transfer the proof. This step used designated verifier proofs (Jakobsson, Sako, and Impagliazzo, Eurocrypt′96). The scheme is correct, receipt-free, private, and verifiable. A couple of issues are still open: the coercer can force the voter to vote randomly, and there is no security against collusion between authorities and coercers.

How to Break a Practical MIX and Design a New One, *Yvo Desmedt* (Florida State University, USA and Royal Holloway, UK), Kaoru Kurosawa (Tokyo Institute of Technology, Japan)

This paper has two parts. First, they showed that the MIX system by Jakobsson ([J98], Eurocrypt′98) is not robust, even though it was proven secure. Chaum introduced MIX nets in 1981. In 1989, Pfitzmann and Pfitzmann broke the RSA-based MIX net. Then Park, Itoh, and Kurosawa (Eurocrypt′93) constructed an efficient scheme based on ElGamal. Sako and Kilian's (Eurocrypt′95) is verifiable but not robust. Ogata, Kurosawa, Sako, and Takatani (ICICS′97) added robustness. Then, efficiency for robust schemes followed. [J98] has four stages: two rounds of permutation and superencryption, and then the corresponding unblinding steps, concluding with verification based on a product, which is where the problem is. It is the MIXEXP (MIX exponentiation) that is not robust. So one dishonest party can affect the whole result.

The new scheme uses two new tools: existential honesty and t-open verification. In each block, there is a dedicated mixer. The other t parties in the block verify and detect. If exactly one party complains, the block is ignored. There always exists a block of $t + 1$ honest parties. The second property allows the MIX secrets to be revealed only within a block. The protocol uses non-malleable ElGamal encryption. The designated parties in the blocks perform permutations and superencryption and privately send the results to the other blocks. Parameters were given for how to construct the blocks. The cost per MIX server is $O(N)$, but more of them are needed, so the total cost is still $O(t^2N)$. The scheme has verifiability, robustness, and privacy.

Session 16: Cryptanalysis III: Stream Ciphers and Block Ciphers, Chair: Lars Knudsen

Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5, *Anne Canteaut* (INRIA, France), Michaël Trabbia (École Polytechnique, France)

Siegenthaler attacked combination generators by getting a correlation between the output and one of the input LFSRs. But this does not work if the combiner is correlation immune. Then, more than one LFSR must be considered simultaneously. The number depends on the order t of the correlation immunity. So t +1 registers together with addition must be examined. To do this, the fast correlation attack of Meier and Staffelbach (*J. Crypt*., 1989) is needed. Using this requires solving a decoding problem, and the method they used was Gallager's iterative algorithm (*IRE Trans. IT*, 1962). This attack was compared with one based on convolutional codes (Johansson and Jönsson, Crypto′99). Gallager's has advantages for equations of weight four and five over all previous attacks. They added a pre-processing step, and they showed that the attack no longer depends on the weight of the feedback polynomial, but

the disadvantage is the time complexity of the preprocessing. However, this step only needs to be performed once per system.

Advanced Slide Attacks, Alex Biryukov (Technion - Israel Institute of Technology, Israel), *David Wagner* (University of California at Berkeley, USA)

The authors introduced slide attacks on Feistel ciphers with weak key schedules, regardless of the number of rounds, at FSE'99. Two plaintexts are encrypted with the same key. If the same key is used at each round, and the second plaintext is the output of round one from the first encryption, then most of the processing is the same in both cases. Such pairs can be found with a birthday attack. In general, the key schedule may repeat with some period p. If $p = 2$, after a one-round slide the exclusive or of the subkeys will always be the same D. Feistel ciphers have a complementation property, so we can pick pairs of texts so that the left side of the first differs from the right side of the second by D. Then, by sliding an encryption against a decryption, the round keys again match up. If the subkey period is greater than 2, say $p = 4$, then a "twist and slide" leaves the subkeys in every other round the same and with constant difference D in the others. They got attacks on Brown-Seberry-DES, DESX ($2^{32.5}$ *known* texts and $2^{87.5}$ operations), and 20-round GOST. The open question is applying this for other values of p.

The preparation of this report was partially supported by the Advanced Telecommunication/Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0002. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes not-withstanding any copyright notation thereon. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.