Andrew M. Odlyzko, Claus P. Schnorr,
Adi Shamir (editors):

Cryptography

Dagstuhl-Seminar-Report; 74
27.09.-01.10.93 (9339)

ISSN 0940-1121

Tel.: +49-6871 - 2458
Fax: +49-6871 - 5942

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Bezugsadresse: Geschäftsstelle Schloss Dagstuhl
Universität des Saarlandes
Postfach 15 11 50
D-66041 Saarbrücken, Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

Report

on the First Dagstuhl Seminar on

Cryptography

September 27 – October 1, 1993

The First Dagstuhl Seminar on Cryptography was organized by Andrew M. Odlyzko (Murray Hill), Claus P. Schnorr (Frankfurt) and Adi Shamir (Tel Aviv). The 38 participants came from 12 countries. Unfortunately Andrew Odlyzko fell ill shortly before the meeting and could not attend.

The 31 lectures covered a broad range of actual research in cryptography dealing with new cryptographic systems and their cryptanalysis. New schemes have been presented for public key signatures, key distribution, key sharing, authentication and cryptographic hashing. Some talks were given about various aspects of number theory like lattice reduction and factorization. Other talks studied cryptographic problems in the framework of coding and information theory. Adi Shamir proposed in an off–schedule discussion an encryption scheme for pictures. It later on has been visualized on some nice slides by Antoine Joux.

Reporter: Carsten Rőssner

Schedule

Monday, 27.09.1993

Morning session. Chair: Jacques Stern

9.15 – 9.30	CLAUS P. SCHNORR	Opening
9.30 – 9.55	MICHAEL BURMESTER:	A Practical and Efficient Conference Key Distribution System as Secure as Diffie Hellmann 6
10.00 – 10.50	HARALD NIEDERREITER:	Factorization Algorithms for Polynomials over Finite Fields, A Progress Report 6
11.20 – 11.50	LEONID BASSALYGO:	A Lower Bound of Probability of Substitution for Authentication Codes without Secrecy 6

Afternoon session. Chair: Arjen K. Lenstra

15.30 – 16.20	FRANÇOIS MORAIN:	Computing the Number of Points on an Elliptic Curve *mod p* : Practical Considerations 7
16.30 – 17.15	ANTOINE JOUX:	Parallel Lattice Reduction (LLL): How to derive a Reduction Algorithm, Uniting the Speed–up of Schnorr and the Parallelisation of Villard..... 7
17.25 – 17.55	CARSTEN RŐSSNER:	A Stable Algorithm for Integer Relations..... 7

Tuesday, 28.09.1993

Morning session. Chair: Kevin McCurley

9.00 – 9.45	CLAUS P. SCHNORR:	Parallel FFT–Hashing 8
9.50 – 10.20	MONI NAOR:	Broadcast Encryption..... 8
10.50 – 11.20	JOAN DAEMEN:	A New Approach towards Block Cipher Design . 8
11.25 – 11.45	MICHAEL PORTZ:	Interconnection Networks in Cryptography 9

Afternoon session. Chair: Moti Yung

14.30 – 15.15	GILLES BRASSARD:	Privacy Amplification..... 9
15.20 – 16.05	UELI M. MAURER:	The Right Definition of Secret Key Rate 10
16.30 – 17.00	ODED GOLDREICH:	Using Error–correcting Codes to Enhance the Security of Signature Schemes..... 10
17.05 – 17.25	VALERI I. KORJIK:	The Influence of Real Random Sequence Generator on the Capacity of the Wire–Tap Channel 11
17.30 – 18.00	NIELS FERGUSON:	Designated Confirmer Signatures..... 11

Wednesday, 29.09.1993

Morning session. Chair: Ueli M. Maurer

Thursday, 30.09.1993

Morning session. Chair: Michael Burmester

Afternoon session. Chair: Gilles Brassard

Friday, 01.10.1993

Morning session. Chair: Claude Crépeau

Abstracts

MICHAEL BURMESTER

An Efficient and Secure Conference Key Distribution System

Joint work with YVO DESMEDT (UNIVERSITY OF WISCONSIN, MILWAUKEE)

Key management is one of the main problems in cryptography and has attracted a lot of attention. Research has focused on secure key distribution and many practical schemes have been proposed. A conference key distribution system is a key distribution system in which more than two users compute a common key. Designing such systems can be particularly challenging because of the complexity of the interactions between the users. Many conference key distribution systems have been presented recently. These however are either impractical (the unconditionally secure ones), or only heuristic arguments were used to address their authenticity and/or security against a wiretapper.

A new conference key distribution system was presented for which the common key is a cyclic function and for which authenticity is achieved by using a separate public key (interactive) authentication scheme. The combined system is secure against *any* type of attack (including those by active adversaries), provided the Diffie Hellman problem is hard.

HARALD NIEDEREITER

Factorization Algorithms for Polynomials over Finite Fields, A Progress Report

New deterministic algortihms for factoring polynomials over finite fields were designed by the speaker in 1992, and these methods have become a subject of intensive study since then. The algorithms are based on the same central idea of using differential equations in the rational function field over the given finite field to linearize the factorization problem. The resulting factorization algorithms have several advantages over the classical Berlekamp algorithm, and they are particularly efficient for finite fields of small characteristic. The talk presents the current state of knowledge about these algorithms and covers the work of von zur Gathen, Göttfert, Lee and Vanstone, and the speaker.

LEONID BASSALYGO

A Lower Bound of Probability of Substitution for Authentication Codes without Secrecy

It is proved that the probability of successful substitution of a message for any authentication code without secrecy and the optimal strategy of the opponent is equal or greater than $K^{-1/2}$, where K is the number of keys, provided the probability of any message does not exceed $1/2$.

FRANÇOIS MORAIN

Computing the Number of Points on an Elliptic Curve *mod p* : Practical Considerations

When implementing cryptosystems based on elliptic curves over finite fields, the first step is usually to compute the number of points on an elliptic curve. This problem was solved in a theoretical way by Schoof, who gave a polynomial time deterministic algorithm for achieving this task. However, the algorithm as such is very inefficient.
Atkin and Elkies have devised practical improvements to this algorithm, when one is dealing with elliptic curves over fields of large characteristic. The aim of this talk is to present these improvements and give some details on the implementation. In particular, we explain how to build modular equations for small primes. Data for fields of characteristic p with up to 225 decimal digits are given.

ANTOINE JOUX

A fast parallel lattice reduction algorithm

The famous L^3 algorithm by Lenstra, Lenstra and Lovász is a polynomial time lattice reduction algorithm. However, the original algorithm was quite slow. In order to improve it, C.P. Schnorr proved that it was possible to devise a similar algorithm with numerical stability properties. He thus created a much faster algorithm working on approximated representations of numbers, instead of the exact rational representation of L^3. G. Villard proved that it was possible to parallelize the L^3 algorithm, using the original rational numbers, thus yielding another improvement. We show here, that these two approaches are compatible, and we describe a parallel L^3 working on approximated numbers.

CARSTEN RŐSSNER

A Stable Algorithm for Integer Relations

Joint work with CLAUS P. SCHNORR

A non–zero vector $m \in \mathbb{Z}^n$ is called an integer relation for $x \in \mathbb{R}^n$ if $< x, m >= 0$, where $<,>$ denotes the Euclidean inner product. We let $\lambda(x)$ denote the length $\|m\| := < m, m >^{1/2}$ of the shortest integer relation m for x, $\lambda(x) = \infty$ if no relation exists. We present a polynomial time algorithm that given $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{N}$ proves a lower bound on $\lambda(x)$, that is reasonable close, and finds a short integer relation m for either x or a nearby point x' so that the length of m is bounded by a function $f(\alpha, n)$. It is important that the constructed x' is good in the sense that no short relation exists for any point $\bar{x}$ that is much closer to x.
Our algorithm uses at most $(n + \log \alpha)^{O(1)}$ many arithmetical operations on real numbers. If x is rational the algorithm operates on integers having at most $(n + \log \alpha + \log B)^{O(1)}$ many bits where B is the maximum of the denominators and numerators in x.
The problem to find in polynomial time integer relations for real numbers was first solved by the HJLS–algorithm of Hastad, Just, Lagarias, Schnorr (1989) which is a variation of the L^3–algorithm of Lenstra, Lenstra, Lovász (1982). The new algorithm is a stable variation of the HJLS–algorithm.

Claus P. Schnorr

Parallel FFT–Hashing

We propose a simple design and an algorithm for collision–resistant hashing of arbitrary messages into a 128 bit hash value. This improves and generalizes the algorithm FFT–Hash II presented at EUROCRYPT'91. We present a highly parallel hash algorithm that models the computation of the discrete Fourier transform. The algorithm operates on double bytes, i.e. bit strings of length 16. The compression function transforms the uniform distribution on input bit strings of length 256 into the uniform distribution of output bit strings of length 128. We introduce the notion of *multipermutations* that generalizes the boxes of the Fourier transform.

Moni Naor

Broadcast Encryption

Joint work with Amos Fiat

We deal with broadcast encryption. We consider a scenario where there is a center and a set of users. The center provides the users with prearranged keys when they join the system. At some point the center wishes to broadcast a message (e.g. a key to decipher a video clip) to a *dynamically* changing privileged subset of the users in such a way that non-members of the privileged class cannot learn the message. Naturally, the non-members are curious about the contents of the message that is being broadcast, and may try to learn it.

We present several schemes that allow a center to broadcast a secret to any subset of privileged users out of a universe of size n so that coalitions of k users not in the privileged set cannot learn the secret. The most interesting scheme requires every user to store $O(k \log k \log n)$ keys and the center to broadcast $O(k^2 \log^2 k \log n)$ messages regardless of the size of the privileged set. This scheme is resilient to *any* coalition of k users. We also present a scheme that is resilient with probability p against a random subset of k users. This scheme requires every user to store $O(\log k \log(1/p))$ keys and the center to broadcast $O(k \log^2 k \log(1/p))$ messages.

Joan Daemen

A New Approach towards Block Cipher Design

Joint work with René Govaerts and Joos Vandewalle

A hardware oriented design approach is applied to the design of symmetric key block ciphers. Key words in this approach are simplicity, uniformity, parallellism, distributed nonlinearity and high diffusion. Key components in the construction are a 3–bit nonlinear S–box and a linear mapping that can be described by modular polynomial multiplication in GF(2^{12}). The arrangement of the components facilitates software implementations. The proposed cipher structure is investigated with respect to both linear and differential cryptanalysis. In this context very powerful results were obtained.

MICHAEL PORTZ

How Interconnection Networks fit into certain Cryptographic Frameworks

As was shown in recent papers interconnection networks (INs) do have their applications in the field of cryptography, i.e., they can be used as design tool for permutation generators (PGs). A certain IN–topology due to Benes can be used to design pseudorandom permutation generators. In it is shown, how the classical DES–based PGs and the Benes–based PGs are related. Both can be shown to be special cases of the Clos–based PGs. In such a generator permutations are generated by evaluating the underlying Clos–networks switching elements by smaller permutation, e.g. one generates a DES–like permutation by evaluating them by permutations of the type $\pi(R) = R \oplus \mathrm{f}(L)$.
In the talk given the question was raised, whether replacing these undeniably simple permutations by permutations of a more complex type does improve the security of a thusly designed blockcipher. This question has no positive answer if one uses certain INs to evaluate the switching elements of a Clos–network with 2^{2n} inputs and one takes independent, uniformly distributed random bits to determine the switching elements setting. One needs $n \cdot 2^{n-1}$ bits for each switching element compared to n bits in the DES–based PG without gaining anything concerning the security of the resulting system. However, the assumption was made, that a kind of 'lower quality' random bits might be sufficient to achieve the same quality of the resulting PG.

GILLES BRASSARD

Generalized Privacy Amplification

Joint work with CHARLES H. BENNETT (IBM RESEARCH, YORKTOWN HEIGHTS), CLAUDE CRÉPEAU (ÉCOLE NORMALE SUPÉRIEURE, PARIS), UELI M. MAURER (ETH, ZÜRICH), JEAN–MARC ROBERT (UNIVERSITÉ DU QUÉBEC, CHICOUTIMI)
Assume Alice and Bob share an n–bit string x about which an eavesdropper Eve has incomplete information characterized by a probability distribution over the n–bit strings. For instance, Eve might have eavesdropped on some of the bits of x through a binary symmetric channel. Alice and Bob have some knowledge of this distribution, but they do not know exactly what is compromised about the secrecy of their string. Using a public channel, which is totally susceptible to eavesdropping but immune to tampering, they wish to agree on a function $g : \{0,1\}^n \to \{0,1\}^r$ such that Eve, despite her partial knowledge about x and complete knowledge of g, almost certainly knows nearly nothing about $g(x)$. This process transforms a partly secret n–bit string x into a highly secret but shorter r–bit string $g(x)$. We characterize how the size of the secret they can safely distill depends on the kind and amount of partial information Eve has on x. We also discuss applications to quantum cryptography.

Ueli M. Maurer

The Right Definition of Secret Key Rate

Three parties, Alice, Bob and Eve, know the sequences of random variables $X^N = [X_1, X_2, \ldots X_N]$, $Y^N = [Y_1, Y_2, \ldots Y^N]$ and $[Z^N = Z_1, Z_2, \ldots Z_N]$, respectively, where the triples $(X_i Y_i Z_i)$, for $1 \leq i \leq N$, are generated by a discrete memoryless source according to some probability distribution P_{XYZ}. Motivated by Wyner's and Csiszár and Körner's pioneering definition of, and work on, the secrecy capacity of a broadcast channel, the secret key rate of P_{XYZ} was defined by Maurer as the maximal rate M/N at which Alice and Bob can generate secret shared random key bits $S_1, \ldots, S_M$ by exchanging messages over an insecure public channel accessible to Eve, such that the rate at which Eve obtains information about the key is arbitrarily small, i.e., such that $\lim_{N\to\infty} I(S_1, \ldots, S_M; Z^N, C^t)/N = 0$, where C^t is the collection of messages exchanged between Alice and Bob over the public channel. However, this definition is not completely satisfactory because only the rate, but not the total amount of information about the key obtained by Eve is bounded. We introduce and investigate a stronger definition of secret key rate: it is required that the total amount of information about the key obtained by Eve be negligible, i.e. $\lim_{N\to\infty} I(S_1, \ldots, S_M; Z^N, C^t) = 0$, and that $[S_1, \ldots, S_M]$ be arbitrarily close to uniformly distributed, i.e. $\lim_{N\to\infty} M - H([S_1, \ldots, S_M]) = 0$. Using novel results on privacy amplification by Bennett, Brassard, Crépeau and Maurer we demonstrate that the known results for the secret key rate also hold for the stronger definition.

Oded Goldreich

Using Error–correcting Codes to Enhance the Security of Signature Schemes

The talk has consisted of two (very mildly related) parts. In the first part, I have advocated the formulation of theoretic results so that the transformation of security (specifically the running-time and success probability of adversary algorithms) is explicitly stated. Such a formulation enables to distinguish between results which have practical significance and results which pose a challenge for providing more efficient transformations. The two fundamental theorems demonstrating that one-way functions imply pseudorandom generators and secure signature schemes, respectively, both belong to the second category. (This part of the talk follows ideas first expressed by Leonid A. Levin.)

In the second part of the talk, I have presented an idea which can be used to enhance the security of signature schemes. The idea is to encode messages using a good error-correcting code and sign the resulting codewords instead of the original messages. The idea is shown to enhance security in the context of constructing one-time signature schemes out of any one-way function. (This part of the talk is based on recent work with Shimon Even and Silvio Micali.)

VALERI I. KORJIK

The Influence of Real Random Sequence Generator on the Capacity of the Wire–Tap Channel

Joint work with V. YAKOVLEV (ST. PETERSBURG, UNIVERSITY OF TELECOMMUNICATION)

The capacity of the code noising channel corresponding to Wyner's concept but for real random sequence generators is considered. We derive an explicit formula and different bounds of this capacity. These results allow us to set requirements to balance and correlation for the generators of random sequences to provide only slightly decreasing in information protection efficiency, in comparison with ideal random sequence generators.

NIELS FERGUSON, PRESENTING A WORK OF DAVID CHAUM (DIGICASH, AMSTERDAM)

Designated Confirmer Signatures

This paper introduces a new kind of signature authentication and gives a practical construction for it. In one extreme case, the new signatures approach the functionality of standard digital signatures; in another, they approach that of zero–knowledge proofs. And they have the undeniable signatures as a trivial case.

The new signatures solve the problem with undeniable signatures that no confirmation protocol can be performed if the signer is unavailable. The solution presented here in essence allows the signer to prove to the recipient of the signature that designated parties, presumably more sure to be available to the recipient than the signer, can confirm the signature without the signer. But the signer is still protected, since unless the designated parties confirm, the recipient of a signature remains unable to convincingly show the signature to anyone else.

ADI SHAMIR

Cryptographic Applications of Birational Mappings

A birational mapping is an invertible mapping from k–tuples to k–tuples such that both the forward mapping and the inverse mapping are expressible by rational functions (involving addition, subtraction, multiplications, divisions, but no radicals). In this talk we describe two new families of birational mappings, in which the inverse mapping cannot be easily deduced from (a truncated version of) the forward mapping. Such mappings could serve as the basis for efficient signature schemes, but the two particular constructions we are currently aware of can be broken by new algebraic techniques developed by Coppersmith, Stern and Vaudenay.

JACQUES STERN

Attacks on the Birational Permutation Signature Schemes

Joint work with DON COPPERSMITH (IBM RESEARCH, YORKTOWN HEIGHTS) AND SERGE VAUDENAY (ÉCOLE NORMALE SUPÉRIEURE, PARIS)

Shamir recently proposed a family of cryptographic signature schemes based on birational permutations of the integers modulo a large integer N of unknown factorization. These schemes are attractive because of the low computational requirements, both for signature generation and signature verification. However, the two schemes presented in Shamir's paper are weak. We show here how to break the first scheme, by first reducing it algebraically to the earlier Ong-Schnorr-Shamir signature scheme, and then applying the Pollard solution to that scheme. We then show some attacks on the second scheme. These attacks give ideas which can be applied to schemes in this general family: basically, we use the fact that the trapdoor reveals algebraic dependencies that do not hold for generic objects. When there is a lack of symmetry, these dependencies disclose pieces of information that are part of the original trapdoor. When full symmetry is present, we compute with symbolic objects, in a context very similar to Galois theory.

CLAUDE CRÉPEAU

Proving Security of Quantum Cryptographic Protocols

Joint work with GILLES BRASSARD (UNIVERSITÉ DE MONTRÉAL), RICHARD JOZSA (UNIVERSITÉ DE MONTRÉAL), DENIS LANGLOIS (UNIVERSITÉ PARIS–SUD)

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure $commit(x)$, to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure $unveil(x)$, the value of x and prove to *Bob* that the piece of evidence sent earlier really corresponded to that bit. Classical bit commitment schemes (by which *Alice*'s piece of evidence is classical information such as a bit string) cannot be secure against unlimited computing power and none have been proven secure against algorithmic sophistication. Previous quantum bit commitment schemes (by which *Alice*'s piece of evidence is quantum information such as a stream of polarized photons) were known to be invulnerable to unlimited computing power and algorithmic sophistication, but not to *arbitrary* measurements allowed by quantum physics: perhaps more sophisticated use of quantum physics could have defeated them.

We present a new quantum bit commitment scheme. The major contribution of this work is to provide the first *complete* proof that, according to the laws of quantum physics, neither participant in the protocol can cheat, except with arbitrarily small probability. In addition, the new protocol can be implemented with current technology.

ARJEN K. LENSTRA

QS versus NFS

The quadratic sieve factoring algorithm (QS) can be expected to factor a composite integer n in time $L(n) = \exp((1 + o(1))\sqrt{\log n \log\log n})$, for $n \to \infty$. This asymptotic runtime estimate can be used to derive a reasonably accurate estimate of the actual runtime to factor some number m using QS, if the runtime of some other number n close to m is known: if n took time $T(n)$, then m will probably take time $L(m)T(n)/L(n)$. Based on the actual runtimes of recent QS-factorizations of 116 and 120-digit numbers, one can estimate the time needed to factor the 129-digit RSA-challenge RSA129 (Scientific American 1977) as approximately 200 years on a DEC 5000 workstation; a less reliable estimate to factor 512-bit numbers could also be obtained in this way.

The number field sieve factoring algorithm (NFS) can be expected to factor a composite integer n in time $\exp((1.923 + o(1))(\log n)^{1/3}(\log\log n)^{2/3})$, for $n \to \infty$, which implies that NFS is asymptotically faster than QS. Actual runtime estimates for, for instance, the factorization of RSA129 using NFS can be obtained in two ways: either we implement NFS and see how fast it works on numbers of 120 or more digits. Or we could try to come up with a way to compare the practical performance of QS and NFS. Attempts in the latter direction have appeared at several places, but they give conflicting results, and they fail to take into account many important aspects of the two methods. Thus it seems that the only way to get a good impression of how NFS will work in practice is to actually implement and run it. It is too early to give precise figures, but estimates based on a very recent NFS implementation suggest that RSA129 could be factored by NFS in substantially less time than QS would take.

SCOTT A. VANSTONE

The Knapsack Problem in Cryptography

Joint work with MINGUA QU (University of Waterloo, Ontario)

The basic knapsack problem apllied to cryptography has had a somewhat brief but interesting and, one would say, not so illustrious history. The purpose of this lecture is to consider the failings of these early attempts and to describe a more general direction for future research.

The concept of group factorization in a finite group is fundamental to the discussion. Group factorization were defined in the early 1940's and have been studied by many people since that time. Magliveras applied these structures to cryptography in the 1970's and constructed private key schemes based on them. Various attempts to create public key systems have followed. Some of these will be described and a new scheme proposed.

KEVIN MCCURLEY

A Hacker's View of Cryptography

Computers serve several roles in cryptography, including cryptanalysis and the performance of cryptographic functions. In this talk we discuss two low-level views of the effectiveness of recent advances in computer architecture from a cryptographic viewpoint.

The two topics are the use of massively parallel computers for the computation of discrete logarithms and the use of common microprocessors for execution of the Secure Hash Algorithm (SHA). In both cases the algorithm that is used was tuned considerably to achieve high rates of performance. The common lesson from these two situations is that, in order to be successful, algorithms should be designed from the beginning to closely match the architecture of the machine that will execute them. Current and future trends in computer architecture will therefore continue to play an important role in the design of cryptographic algorithms.

TSUTOMU MATSUMOTO

A New Approach to Key Sharing

Joint work with HIDEKI IMAI (UNIVERSITY OF TOKYO)

This talk introduced a newly proposed class of cryptographic key sharing schemes [1], with each of which an entity (say i) in a very large network can locally compute a common key shared with another entity (say, j) by using

(1) i's secret algorithm selected by herself,

(2) j's identifier, and

(3) i's public algorithm generated by a protocol conducted by i and the managing center(s).

A highlight of the class is that a small amount of descriptive and executive complexity of the secret algorithm is sufficient to maintain any required security level if the complexity of the public algorithm can be reasonably increased. Thus very cheap powerless smart cards, storing and executing secret algorithms, can be used to build a highly practical and reliable key sharing system for any kind of networks. The class also attains the following interesting features: manageability of disenrolled entities; load sharing between a sender and a receiver; computational anonymity of senders, etc.

Reference: [1] T.Matsumoto, H.Imai, "An Approach to Key Sharing Problem — Preliminary Announcement ", (in Japanese) IEICE Technical Report, Information Security/Computation, July 12, 1993.

HANS–JOACHIM KNOBLOCH

Verifiable Secret Sharing for Monotone Access Structures

Joint work with THOMAS BETH AND MARCUS OTTEN (UNIVERSITÄT KARLSRUHE)

Several verifiable secret sharing schemes for threshold schemes based on poynomial interpolation have been published in the literature. Simmons and others have introduced secret sharing schemes based on finite geometries which allow to distribute a secret according to any monotone access structure.

We presented a verification method for a class of these geometry-based schemes which thus provides verifiable sharing of secrets according to general monotone access structures.

Our scheme relies on the homomorphic properties of the discrete exponentiation and therefore on the cryptographic security of the discrete logarithm. The version based on Simmons' scheme is non-interactive.

ELI BIHAM

On Matsui's Linear Cryptanalysis

In [1] Matsui introduced a new method of cryptanalysis, called *Linear Cryptanalysis*. This method was used to attack DES using 2^{47} known plaintexts. In this paper we formalize this method and show that although in the details level this method is quite different from differential cryptanalysis, in the structural level they are very similar. For example, characteristics can be defined in linear cryptanlysis, but the concatenation rule has several important differences from the concatenation rule of differential cryptanalysis.

Reference: [1] M.Matsui, "Linear Cryptanalysis Method for DES Cipher ", Abstracts of EUROCRYPT'93, pp. W112–W123, May 1993.

KAZUO OHTA

Differential Attack on Message Authentication Codes

Joint work with MITSURU MATSUI (MITSUBISHI ELECTRIC CORPORATION, KANAGAWA)

We discuss the security of Message Authentication Code (MAC) schemes from the viewpoint of differential attack, and propose an attack that is effective against DES–MAC and FEAL–MAC. The attack derives the secret authentication key in the chosen plaintext scenario. For example, DES(8–round)–MAC can be broken with 2^{22} pairs. The proposed attack is applicable to any MAC scheme, even if the 32–bits are randomly selected from among the 64–bits of ciphertext generated by a cryptosystem vulnerable to differential attack in the chosen plaintext scenario.

MOTI YUNG

Eavesdropping Games

Joint work with MATTHEW FRANKLIN (COLUMBIA UNIVERSITY), ZVI GALIL (COLUMBIA UNIVERSITY, TEL AVIV UNIVERSITY)

Security of computation has motivated a variety of basic issues in the last two decades. Here, we initiate a graph-theoretic approach to study the (information-theoretic) *maintenance of privacy* in distributed environments in the presence of a bounded number of *mobile* eavesdroppers ("bugs"). The system is modeled as a network of processors/switches in which the eavesdropping take place. The goals are to combinatorially characterize and compare privacy maintenance problems, to determine their possibility (under numerous bug models), to analyze their computational complexity, and when possible to suggest protocols.

For two fundamental privacy problems – *secure message transmission* and *distributed data base maintenance* – we assume an adversary is "playing eavesdropping games," coordinat-

ing the movement of the bugs among the sites to learn the current memory contents. We consider various *mobility settings* (adversaries), motivated by the capabilities (strength) of the bugging technologies (e. g. how fast can a bug be reassigned).
For secure message transmission, we show that privacy is achievable if and only if a certain *network connectivity condition* is met, *independent* of the mobility setting. Determining privacy is co-NP-complete in one variant, and in P-time for another (where the variant depends on the relation of the sender and receiver to the network).
For distributed database maintenance, we show a close connection to the problem of *graph searching* (cornering a fugitive by moving guards among the nodes of a graph). Determining privacy is, in the general case, PSPACE-complete. We also give natural mobility settings (i. e. simple constraints) for which determining privacy is NP-complete and co-NP-hard.
We further show that different mobility settings imply different privacy problems, by demonstrating sensitivity to various aspects of setting (e. g. parallel versus sequential bug movement, "edge-crawling" versus "node-hopping" bugs, infrequent versus frequent bug reassignment). To this end, we exhibit explicit families of graphs with large additive and multiplicative differences in number of bugs tolerated. We also show that the time required to compromise privacy can be exponential for bugs that can be reassigned at the network speed, while it is always polynomial for bugs that reassign sufficiently slowly.

ERNST M. GABIDULIN

How to avoid the Sidelnikov–Shestakov Attack against the Niederreiter System

Joint work with OLAF KJELSEN (ETH, ZŰRICH)

A simple criterion is given when the Sidelnikov–Shestakov attack is applicable against some Niederreiter PKC based on an MDS code. Two methods are proposed how to modify this PKC. The first one is hiding a Public–Key by means of adding to an old Public–Key parity check matrix some matrix of rank 1. The second one is using other than Generalized Reed–Solomon codes family of codes. Namely, codes correcting rank not Hamming errors seem to be as suitable for the Niederreiter PKC.

URIEL FEIGE

2–Prover 1–Round 0–Knowledge Proof Systems

Joint work with JOE KILIAN (NEC RESEARCH INSTITUTE, PRINCETON, NEW JERSEY)

We provide an error reduction technique for two-prover one-round zero-knowledge proof systems. Our technique is a modification of the algebraic error reduction technique of Lapidot-Shamir and Feige-Lovasz. Using this, we show that NEXPTIME has two-prover one-round perfect zero knowledge proof systems with exponentially small error, and that NP has such proof systems with polylogarithmic communication, and error smaller than the inverse of any polynomial. This solves an open question of Dwork, Feige, Kilian, Naor and Safra.
Our error reduction technique also has the desirable feature of transforming proof systems that are zero knowledge with respect to "super honest" verifiers (which we call *verifreiers*),

to proof systems that are zero knowledge with respect to any verifier, including cheating verifiers. This considerably simplifies the design of two-prover one-round zero-knowledge proof systems.

Birgit Pfitzmann

Defining Signature Schemes generally

Digital signature schemes are a fundamental tool for secure distributed systems. It is important to have a formal notion of what a secure digital signature scheme is, so that there is a clear interface between designers and users of such schemes. A definition that seemed final was given by Goldwasser, Micali and Rivest in 1988. Recently, however, several signature schemes with new security properties have been presented, which are not covered by the definition mentioned above. Hence their new properties cannot be defined as additions, but each new type of scheme needs a new definition from scratch, and many variants currently have no definition at all. This is unsatisfactory.
This talk presents (an overview of) a general definition of digital signature schemes that covers all known schemes, and hopefully all that might be invented in future. Additional properties of special types of schemes can then be defined in an orthogonal way, so that existing schemes can be classified systematically.
It turns out that signature schemes are best defined by a separartion of service, structure and degree of security, with a service specification in (temporal) logic. Several parts of such a definition can easily be reused for general definitions of other classes of cryptologic schemes. Some relations to definitions of secure multi-party function evaluation are discussed.

Yacov Yacobi

Minimal Asymmetric Authentication and Key Agreement Schemes

Joint work with M. J. Beller
We propose an asymmetric Authentication and Key Agreement scheme which is aimed at minimizing the on-line computation of one of the parties (e. g. a smart-card), and the communication complexity. The proposed protocol requires only ont to three (depending on situation) on-line multiplications for one of the sides. Evidence for its security is given.

René Peralta

Factoring with a Quadratic Residuosity Oracle

Given a composite number N and a secret factor P, assume that it is possible to efficiently decide whether or not a number x modulo N is a quadratic residue modulo P. Under this assumption we show a particularly efficient "large prime" variation of the elliptic curve method of obtaining P. We also show a (randomized) reduction to a combinatorial optimization problem which, although NP-Complete, might be efficiently solvable in the average.
Integers with secret factorization of the form PQ^2 have occasionally been proposed for

cryptographic use. For these integers, the above assumption holds since the Legendre symbol (x/P) is equal to the Jacobi symbol (x/N). Hence you are asking for trouble if you use integers of this type for cryptographic purposes.

Schedule of the Dagstuhl–Seminar "Cryptography" Monday, September 27, 1993

Time	Program
9.15 – 9.30	**Opening (C. P. Schnorr)**
Morning Session	**Chairman: J.Stern**
9.30 – 9.55	**M. Burmester:** A Practical and Efficient Conference Key Distribution System as Secure as Diffie Hellmann.
10.00 – 10.50	**H. Niederreiter:** Factorization Algorithms for Polynomials over Finite Fields, A Progress Report.
10.50 – 11.20	**Coffee**
11.20 – 11.50	**L. Bassalygo:** A Lower Bound of Probability of Substitution for Authentication Codes without Secrecy.
12.00 – 14.00	**Lunch**
15.00	**Coffee and Cakes**
Afternoon Session	**Chairman: A. K. Lenstra**
15.30 – 16.20	**F. Morain:** Computing the Number of Points on an Elliptic Curve *mod p* : Practical Considerations.
16.30 – 17.15	**A. Joux:** Parallel Lattice Reduction (LLL): How to derive a Reduction Algorithm, Uniting the Speed–up of Schnorr and the Parallelisation of Villard.
17.25 – 17.55	**C. Rössner:** A Stable Algorithm for Integer relations.
18.00	**Dinner**

Schedule of the Dagstuhl–Seminar "Cryptography" Tuesday, September 28, 1993

Time	Program
Morning Session	**Chairman: K. McCurley**
9.00 – 9.45	**C. P. Schnorr:** Parallel FFT–Hashing.
9.50 – 10.20	**M. Naor:** Broadcast Encryption.
10.20 – 10.50	**Coffee**
10.50 – 11.20	**J. Daemen:** A New Approach towards Block Cipher Design.
11.25 – 11.45	**M. Portz:** Interconnection Networks in Cryptography.
12.00 – 14.00	**Lunch**
Afternoon Session	**Chairman: M. Yung**
14.30 – 15.15	**G. Brassard:** Privacy Amplification.
15.20 – 16.05	**U. Maurer:** The Right Definition of Secret Key Rate.
16.05 – 16.30	**Coffee**
16.30 – 17.00	**O. Goldreich:** Using Error–correcting Codes to Enhance the Security of Signature Schemes.
17.05 – 17.25	**V. I. Korjik:** The Influence of Real Random Sequence Generator on the Capacity of the Wire–Tap Channel.
17.30 – 18.00	**N. Ferguson:** Designated Confirmer Signatures.
18.00	**Dinner**

Schedule of the Dagstuhl–Seminar "Cryptography" Wednesday, September 29, 1993

Time	Program
Morning Session	**Chairman: U. Maurer**
9.00 – 9.50	**A. Shamir:** Cryptographic Applications of Birational Mappings.
9.55 – 10.45	**J. Stern:** Attacks against Birational Signatures.
10.45 – 11.15	**Coffee**
11.15 – 12.05	**C. Crépeau:** Proving Security of Quantum Cryptographic Protocols.
12.05	**Lunch**
Afternoon	**Excursion**

Schedule of the Dagstuhl–Seminar "Cryptography" Thursday, September 30, 1993

Time	Program
Morning Session	**Chairman: M. Burmester**
9.00 – 9.30	**A. K. Lenstra:** QS ↔ NFS.
9.35 – 10.05	**S. A. Vanstone:** The Knapsack Problem in Cryptography.
10.10 – 10.40	**K. McCurley:** A Hacker's View of Cryptography.
10.40 – 11.10	**Coffee**
11.10 – 11.40	**T. Matsumoto:** A New Approach to Key Sharing.
11.45 – 12.05	**H.-J. Knobloch:** Verifiable Secret Sharing.
12.00 – 14.00	**Lunch**
Afternoon Session	**Chairman: G. Brassard**
15.00 – 15.40	**E. Biham:** On Matsui's Linear Cryptanalysis.
15.45 – 16.15	**K. Ohta:** Differential Attack on Message Authentication.
16.15 – 16.45	**Coffee**
16.45 – 17.15	**M. Yung:** Eavesdropping Games.
17.20 – 17.50	**E. M. Gabidulin:** How to avoid the Sidelnikov–Shestakov Attack against the Niederreiter System.
18.00	**Dinner**

Schedule of the Dagstuhl–Seminar "Cryptography" Friday, October 1, 1993

Time	Program
Morning Session	**Chairman: C. Crépeau**
9.00 – 9.30	**U. Feige:** 2–Prover 1–Round 0–Knowledge Proof Systems.
9.35 – 10.05	**B. Pfitzmann:** Defining Signature Schemes generally.
10.05 – 10.40	**Coffee**
10.40 – 11.10	**Y. Yacobi:** About current Cryptographic Work at Bellcore.
11.15 – 11.45	**R. Peralta:** Factoring with a quadratic Residuosity Oracle.
12.00	**End of Lectures & Lunch**

Dagstuhl-Seminar 9339:

Participants: **04.10.93**

Leonid **Bassalygo**
Moscow State University
Mechanical-Mathematical Dept.
Lenin Hill
117234 Moskau
GUS

Eli **Biham**
Computer Science Department
Technion
Haifa 32000
Israel
biham@cs.technion.ac.il
tel.: +972-4-2943-08

Gilles **Brassard**
Université de Montreal
Département IRO
C.P. 6128
Montreal Quebec H3C 3J7
Canada
brassard@iro.umontreal.ca
tel.: +1-514-343-6807

Michael **Burmester**
Royal Holloway
University of London
Department of Computer Science
Egham
Surrey
TW20 0EX
+44-784-44-30 84
tel.: Great Britain

Claude **Crépeau**
Ecole Normale Superieure
Dép. de Math. et Informatique
45 Rue d'Ulm
F-75230 Paris Cedex 05
France
crepeau@dmi.ens.fr
tel.: +33-1-44 32 20 61

Joan **Daemen**
ESAT Laboratories - Leuven
K.U.Leuven
K. Mercierlaan 94
B-3030 Leuven
Belgium
daemen@esat.kuleuven.ac.be
tel.: +32-16-22 09 31

Uriel **Feige**
Weizman Institute - Rehovot
Dept. of Applied Mathematics
P. O. Box 26
76100 Rehovot
Israel
feige@wisdom.weizmann.ac.il
tel.: +972-8-343364

Joan **Feigenbaum**
AT & T Bell Laboratories
Room 2C473
600 Mountain Avenue
Murray Hill N.J. 07974-0636
USA
jf@research.att.com
tel.: +1-908-582-69 10

Neils **Ferguson**
CWI - Amsterdam
Kruislaan 413
NL-1098 SJ Amsterdam
The Netherlands
tel.: +31-20-665-26 11

Ernst M. **Gabidulin**
Moscow Institute of
Physics & Technology
Institutskii pez 9
141700 Dolgoprundny
GUS
gab@re.mipt.su / gab@ippi.msk.su
tel.: +7-95-408-44 33

Oded **Goldreich**
Technion Haifa
Israel Institute of Technology
Computer Science Department
Technion City Haifa 32 000
Israel
oded@cs.technion.ac.il
tel.: +0972-4-294360

Erwin **Heß**
Siemens AG - Muenchen
ZFE ST SN 5
Zentralbereich Forsch. u. Technik
D-81730 München
tel.: +49-89-636-4140

Antoine **Joux**
Ecole Normale Superieure
Dép. de Math. et Informatique
45 Rue d'Ulm
F-75230 Paris Cedex 05
France
joux@dmi.ens.fr
tel.: +33-1-44-32-2061

Hans-Joachim **Knobloch**
Universität Karlsruhe
Inst. für Algorithmen und
Kognitive Systeme
Am Fasanengarten 5
D-76128 Karlsruhe
knobloch@ira.uka.de
tel.: +49-721-608-4260 /721-96400-14

Valeri I. **Korjik**
Leningrad Electroengineering
Institute of Communications
Dept. of Communication Theory
Mojka 61
191065 St. Petersburg
GUS
bymey@iec.spb.su
tel.: +7-812-315 8247 (office)
+7-812-550-18-80 (home)

Dror **Lapidot**
Applied Math. Department
Weizmann Institut of Science
Rehovot 76100
Israel
drorl@wisdom.weizmann.ac.il

Arjen K. **Lenstra**
Bellcore
Rm. 2Q-334
445 South St.
Morristown N.J. 07962-1910
USA
lenstra@bellcore.com
tel.: +1-201-829-48 78

Tsutomu **Matsumoto**
Yokohama National University
Div. of Elec. & Comp. Engr.
156 Tokiwadai Hodogaya
Yokohama 240
Japan
tsutomu@mlab.dnj.ynu.ac.jp
tel.: +81-45-335-1451

Ueli **Maurer**
Swiss Fed. Inst. Tech.
Inst. for Theoretical Computer Science
ETH Zentrum
CH-8092 Zürich
Switzerland
maurer@inf.ethz.ch
tel.: +41-1254-7420

Kevin **McCurley**
Sandia National Labs.
Div. 1423
P. O. Box 58 00
Albuquerque N.M. 87185
USA
mccurleyy@cs.sandia.gov
tel.: +1-505-845-7378

Francois **Morain**
Ecole Polytechnique
LIX
BP 105
F-91128 Palaiseau CEDEX
France
morain@poly.polytechnique.fr

Moni **Naor**
IBM Almaden Research Center
650 Harry Road
San Jose CA 95120
USA
naor@wisdom.weizmann.ac.il
tel.: +972-8-343-471

Harald **Niederreiter**
Österreichische Akademie der
Wissenschaften
Inst. f. Informationsverarbeitung
Sonnenfelsgasse 19
A-1010 Wien
Austria
nied@qiinfo.oeaw.ac.at
tel.: +43-1-5 15 81- 3 20

Kazuo **Ohta**
NTT Kanagawa
309A I-2356
Kanagawa 238-03 Yokosuka
Japan
ohta@sucaba.ntt.jp
tel.: +81-468 59 3383

René **Peralta**
Univ. Wisconsin-Milwaukee
Dept. EECS
P.O.Box 784
Milwaukee WI 53201
USA
peralta@cs.uwm.edu
tel.: +1-414-229-4677

Birgit **Pfitzmann**
Universität Hildesheim
Samelsonplatz 1
D-31141 Hildesheim
Germany
pfitzb@informatik.uni-hildesheim.de
tel.: +49-5121-883-7 39

John M. **Pollard**
Tidmarsh Cottage
Manor Farm Lane
Tidmarsh Reading RG8 8EX
Great Britain

Michael **Portz**
RWTH Aachen
Lehrstuhl f. Angewandte Mathematik
insbes. Informatik
Ahornstr. 55
D-52074 Aachen
Germany
michaelp@terpi.informatik.rwth-aachen.de
tel.: +49-0241-802-1062

Jean-Jacques **Quisquater**
University of Louvain
Dept. of Electrical Engineering
DICE
Place du Levant 3
B-1348 Louvain-la-Neuve
Belgium
quisquater@dice.uc.ac.be
tel.: +32-1047-8667

Carsten **Rössner**
Universität Frankfurt
Fachbereich Mathematik
Robert-Mayer-Str. 10
D-60054 Frankfurt
Germany
roessner@informatik.uni-frankfurt.de
tel.: +49-69-798-3581

Claus P. **Schnorr**
Universität Frankfurt
Mathematisches Institut
Robert-Mayer-Str. 6-10
D-60054 Frankfurt
Germany

Adi **Shamir**
The Weizman Institute of Sciences
Applied Mathematics Dept.
P.O.Box 26
Rehovot 76100
Israel

Jacques **Stern**
Ecole Normale Superieure
Dép. de Math. et Informatique
45 Rue d'Ulm
F-75230 Paris Cedex 05
France
stern@dmi.ens.fr
tel.: +33-1-44-322029

Brigitte **Vallée**
Université de Caen
Dép. de Mathématique et de Méc.
Esplanade de la Paix
F-14032 Caen
France
vallee@univ-caen.fr
tel.: +33-31-45-56-57 /27-02

Scott A. **Vanstone**
Univ. of Waterloo
Dep. of Combinatorics and
Optimization
Waterloo Ontario N2L 3G1
Canada
savanstone@math.waterloo.ca
tel.: +519-888-4063

Yacov **Yacobi**
Bellcore
Rm. 2A-217
445 South St.
Morristown NJ 07962
USA
yacov@bellcore.com
tel.: +1-201-829-46 68

Moti **Yung**
IBM T.J. Watson Research Center
P.O. Box 704
Yorktown Heights NY 10598
USA
moti@watson.ibm.com
tel.: +1-914-784-7196

Zuletzt erschienene und geplante Titel:

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)

J. Buchmann, H. Niederreiter, A.M. Odlyzko, H.G. Zimmer (editors):
Algorithms and Number Theory, Dagstuhl-Seminar-Report; 39; 22.06.-26.06.92 (9226)

E. Börger, Y. Gurevich, H. Kleine-Büning, M.M. Richter (editors):
Computer Science Logic, Dagstuhl-Seminar-Report; 40; 13.07.-17.07.92 (9229)

J. von zur Gathen, M. Karpinski, D. Kozen (editors):
Algebraic Complexity and Parallelism, Dagstuhl-Seminar-Report; 41; 20.07.-24.07.92 (9230)

F. Baader, J. Siekmann, W. Snyder (editors):
6th International Workshop on Unification, Dagstuhl-Seminar-Report; 42; 29.07.-31.07.92 (9231)

J.W. Davenport, F. Krückeberg, R.E. Moore, S. Rump (editors):
Symbolic, algebraic and validated numerical Computation, Dagstuhl-Seminar-Report; 43; 03.08.-07.08.92 (9232)

R. Cohen, R. Kass, C. Paris, W. Wahlster (editors):
Third International Workshop on User Modeling (UM'92), Dagstuhl-Seminar-Report; 44; 10.-13.8.92 (9233)

R. Reischuk, D. Uhlig (editors):
Complexity and Realization of Boolean Functions, Dagstuhl-Seminar-Report; 45; 24.08.-28.08.92 (9235)

Th. Lengauer, D. Schomburg, M.S. Waterman (editors):
Molecular Bioinformatics, Dagstuhl-Seminar-Report; 46; 07.09.-11.09.92 (9237)

V.R. Basili, H.D. Rombach, R.W. Selby (editors):
Experimental Software Engineering Issues, Dagstuhl-Seminar-Report; 47; 14.-18.09.92 (9238)

Y. Dittrich, H. Hastedt, P. Schefe (editors):
Computer Science and Philosophy, Dagstuhl-Seminar-Report; 48; 21.09.-25.09.92 (9239)

R.P. Daley, U. Furbach, K.P. Jantke (editors):
Analogical and Inductive Inference 1992 , Dagstuhl-Seminar-Report; 49; 05.10.-09.10.92 (9241)

E. Novak, St. Smale, J.F. Traub (editors):
Algorithms and Complexity for Continuous Problems, Dagstuhl-Seminar-Report; 50; 12.10.-16.10.92 (9242)

J. Encarnação, J. Foley (editors):
Multimedia - System Architectures and Applications, Dagstuhl-Seminar-Report; 51; 02.11.-06.11.92 (9245)

F.J. Rammig, J. Staunstrup, G. Zimmermann (editors):
Self-Timed Design, Dagstuhl-Seminar-Report; 52; 30.11.-04.12.92 (9249)

B. Courcelle, H. Ehrig, G. Rozenberg, H.J. Schneider (editors):
Graph-Transformations in Computer Science, Dagstuhl-Seminar-Report; 53; 04.01.-08.01.93 (9301)

A. Arnold, L. Priese, R. Vollmar (editors):
Automata Theory: Distributed Models, Dagstuhl-Seminar-Report; 54; 11.01.-15.01.93 (9302)

W. Cellary, K. Vidyasankar, G. Vossen (editors):
Versioning in Database Management Systems, Dagstuhl-Seminar-Report; 55; 01.02.-05.02.93 (9305)

B. Becker, R. Bryant, Ch. Meinel (editors):
Computer Aided Design and Test , Dagstuhl-Seminar-Report; 56; 15.02.-19.02.93 (9307)

M. Pinkal, R. Scha, L. Schubert (editors):
Semantic Formalisms in Natural Language Processing, Dagstuhl-Seminar-Report; 57; 23.02.-26.02.93 (9308)

W. Bibel, K. Furukawa, M. Stickel (editors):
Deduction , Dagstuhl-Seminar-Report; 58; 08.03.-12.03.93 (9310)

H. Alt, B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 59; 22.03.-26.03.93 (9312)

H. Kamp, J. Pustejovsky (editors):
Universals in the Lexicon: At the Intersection of Lexical Semantic Theories, Dagstuhl-Seminar-Report; 60; 29.03.-02.04.93 (9313)

W. Strasser, F. Wahl (editors):
Graphics & Robotics, Dagstuhl-Seminar-Report; 61; 19.04.-22.04.93 (9316)

C. Beeri, A. Heuer, G. Saake, S. Urban (editors):
Formal Aspects of Object Base Dynamics , Dagstuhl-Seminar-Report; 62; 26.04.-30.04.93 (9317)

R. V. Book, E. Pednault, D. Wotschke (editors):
Descriptional Complexity, Dagstuhl-Seminar-Report; 63; 03.05.-07.05.93 (9318)

H.-D. Ehrig, F. von Henke, J. Meseguer, M. Wirsing (editors):
Specification and Semantics, Dagstuhl-Seminar-Report; 64; 24.05.-28.05.93 (9321)

M. Droste, Y. Gurevich (editors):
Semantics of Programming Languages and Algebra, Dagstuhl-Seminar-Report; 65; 07.06.-11.06.93 (9323)

Ch. Lengauer, P. Quinton, Y. Robert, L. Thiele (editors):
Parallelization Techniques for Uniform Algorithms, Dagstuhl-Seminar-Report; 66; 21.06.-25.06.93 (9325)

G. Farin, H. Hagen, H. Noltemeier (editors):
Geometric Modelling, Dagstuhl-Seminar-Report; 67; 28.06.-02.07.93 (9326)

Ph. Flajolet, R. Kemp, H. Prodinger (editors):
"Average-Case"-Analysis of Algorithms, Dagstuhl-Seminar-Report; 68; 12.07.-16.07.93 (9328)

J.W. Gray, A.M. Pitts, K. Sieber (editors):
Interactions between Category Theory and Computer Science, Dagstuhl-Seminar-Report; 69; 19.07.-23.07.93 (9329)

D. Gabbay, H.-J. Ohlbach (editors):
Automated Practical Reasoning and Argumentation, Dagstuhl-Seminar-Report; 70; 23.08.-27.08.93 (9334)

A. Danthine , W. Effelsberg, O. Spaniol, (editors):
Architecture and Protocols for High-Speed Networks, Dagstuhl-Seminar-Report; 71; 30.08.-03.09.93 (9335)

R. Cole, E. W. Mayr, F. Meyer a.d.Heide (editors):
Parallel and Distributed Algorithms, Dagstuhl-Seminar-Report; 72; 13.09.-17.09.93 (9337)

V. Marek, A. Nerode, P.H. Schmitt (editors):
Non-Classical Logics in Computer Science, Dagstuhl-Seminar-Report; 73; 20.-24.09.93 (9338)

A. Odlyzko, C.P. Schnorr, A. Shamir (editors):
Cryptography, Dagstuhl-Seminar-Report; 74; 27.09.-01.10.93 (9339)

J. Angeles, G. Hommel, P. Kovács (editors):
Computational Kinematics, Dagstuhl-Seminar-Report; 75; 11.10.-15.10.93 (9341)

T. Lengauer, M. Sarrafzadeh, D. Wagner (editors):
Combinatorial Methods for Integrated Circuit Design, Dagstuhl-Seminar-Report; 76; 18.10.-22.10.93 (9342)