MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht 28a/1991

E.I.S.S.-Workshop
Public-Key Cryptography: State of the Art and Future Direction

3.7. bis 6.7.1991

In view of the recent developments on the scientific, technological and political side about the use of public-key systems as a future primitive for secure data-processing around the world the *European Institute for System Security (E.I.S.S.)* has convened a workshop to assess the *State of the Art and Future Directions of Public-Key Cryptography* within its mission that it has been given by the state government of Baden-Württemberg to provide *know-how* and technology transfer at top scientific level to authorities and industrial concerns in Germany, Europe and the high-tech community worldwide.

The recent announcement of the NIST (National Institute of Standards and Technology) through its Deputy Director Raymond G. Kammer at the House of Representatives of the United States of America on June 27, 1991 — less than one week before the beginning of the meeting — provided even more evidence to the fact that a survey assessment of todays present state of the art carried out by independent body of research and technology representatives would be welcomed by the high-tech community around the world.

The task to give a fair assessment of the present state of public-key technology was only to be managed by a serious planning and a thoroughly composed list of invitees each of whom could contribute to at least two special topics of public-key cryptography at frontline research and technological level. In order to document the scientific importance and independence of the workshop it was a happy circumstance that this meeting could take place at the *Mathematisches Forschungsinstitut Oberwolfach*.

Its relaxed and positive atmosphere and the beautyful surrounding landscape — as well as the well-known hospitality of all staff — combined to achieve a very close working relationship among the participants, in spite of the hot July weather, which indeed enforced several evening sessions! It was especially noted that without the special support and the dedication of the director of the institute, Professor Barner, this meeting which has been arranged in addition to already tight schedule could not have taken place.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

The Role of Public-Key Cryptography

During the fifteen year period since its invention the concept of public-key cryptography has completely changed the field of security.

Secrecy, the classical feature, has not remained the essential topic of secure systems in the open high-tech-community. It is rather the problem of authentication, identification and integrity verification, that has made clear that the central topic is rather the notion of **trust**, its generation, transport, preservation and management in complex systems. Owing to modern mathematical research, the invention of one-way-functions has provided an algorithmic tool to develop mechanisms for these primitives of trust handling.

The only known public-key algorithms are based on algebraic data structures which are closely related to the areas of Algebra and Computational Number Theory. Results from these areas formed an essential part of the workshop, showing that the essential directions for the future development of what is still called "Public-Key **Cryptography**" is is rather that of preserving trust than that of preserving secrecy.

List of Topics choosen through Self-Assessment

Following the long-standing tradition at the *Mathematisches Forschungsinstitut Oberwolfach* a detailed selection of topics to be covered had not been imposed on or issued to the participants before the meeting.

As a better alternative, a list of the most interesting and important topics has been worked out in a mutual discussion by the participants as the first task of the workshop. As the meeting developed more emphasis was placed on certain topics requiring more in depth consideration according to following short self assessment reviews after each session. The topics initially defined are given in the following list.

- State of the Art in Factoring
- Factoring, Primality Tests and other Applications using Elliptic Curves
- Relations between Computing the Discrete Logarithm and Factoring
- (Fast) Generation of Primes (with certain Properties)
- Comparison of the RSA-Scheme and PKC's based on the Discrete Logarithm

Gefördert durch DFG Deutsche Forschungsgemeinschaft

- Fast Computation for Public-Key Cryptosystems
- Other known Public-Key Cryptosystems
- Embedding of Public-Key Cryptosystems in Protocols
- Hash Functions and their Interface to Public-Key Cryptosystems
- Specific Hash Functions
- Lifetime and Use of Systems

The form of topics which crystallized through several self-assessment reviews which took place after each session, is represented by the following abstracts.

Thomas Beth, E.I.S.S., Universität Karlsruhe

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Abstracts

Factoring

The security of many cryptosystems relies on the assumption that factoring large integers is a computationally infeasible problem. In this talk I have discussed various factoring algorithms from a practical point of view. Among these the most important, and most practical algorithms are: the elliptic curve method, the double large prime variation of the multiple polynomial quadratic sieve (ppmpqs), and the number field sieve (nfs).

Despite an enormous computational effort during the last 6 years, nobody has ever found a factor of more than 38 digits using the elliptic curve method (ecm). Future better implementations (FFT in the second stage, MASPAR) might be able to find factors of up to 40 digits, but it is considered unlikely, that ecm will ever be able to find factors of 50 or more digits.

The largest number ever factored with ppmpqs, a general purpose factoring algorithm, currently has 116 decimal digits. This computation took 400 MIP years and was distributed over a worldwide network of workstations, communicating via electronic mail. Using the run time estimates for ppmpqs, one finds that factoring 512 bit numbers (currently a popular choice in cryptosystems) is 1300 times more difficult than factoring 116 digits. Factoring a 512 bit number would thus require about 500.000 MIP years, which makes it an exceedingly hard, but not necessarily impossible computation for the first stage. The second stage would require approximately 300 Gbyte of storage, and 7 months on a 16K MASPAR. No practical experience has been obtained yet with the general number field sieve. In a later lecture Robert Silverman presented his data that are relevant for the nfs. This made us believe that the number field sieve is not unlikely to be better than ppmpqs for numbers in the 512 bit range.

Arjen K. Lenstra, Morristown, NJ

The number field sieve

The number field sieve is an algorithm for factoring positive integers n.

It is conjectured to run in time $L_n[\frac{1}{3}, O(1)]$, where $L_n[r,c] = \exp(c \cdot (\log n)^r \cdot (\log\log n)^{1-r})$. The initial idea of the number field sieve is due to John Pollard (1988), who proposed it for the factorization of a very special class of numbers. The modifications necessary to make it applicable to general n are due to Joe Buhler, Carl Pomerance, myself, and Len Adleman. As many other factoring algorithms, the number field sieve attempts to factor n by solving the congruence $x^2 \equiv y^2 \bmod n$, subject to $x \not\equiv y \bmod n$; namely, then $\gcd(x \pm y, n)$ is for each choice of the sign a non-trivial divisor of n. Instead of searching for "square ≡ square" mod$n$, one looks for solutions of "square ≡ smooth" mod$n$, where "smooth" means "built up from small prime divisors"; namely, using linear algebra over $\mathbf{F}_2$, one can multiply many solutions of "square ≡ smooth" into one solution of "square ≡ square". Also a solution of "smooth ≡ smooth" can be used, since if x, y are smooth with $x \equiv y \bmod n$, then $x^2 \equiv xy \bmod n$ and xy is smooth as well. The way in which factoring algorithms often generate smooth numbers is that they generate small numbers and exploit the fact that small numbers are more likely to be smooth than large ones. However, in any congruence $x \equiv y \bmod n$ with $x \not\equiv y$ at least one of x, y is at least $\frac{1}{2}n$ in absolute value, so that x, y cannot be very small; but this obstruction can be gotten around by exploiting algebraic number fields. In the lecture it was explained how this works, and how the problems caused by the presence of units and the lack of unique factorization can be resolved by means of quadratic characters.

Hendrik W. Lenstra, Jr., University of California, Berkeley

Computational Experience with the General Number Field Sieve

The Number Field Sieve (NFS) is a new algorithm for factoring very large integers of special form. It is remarkably fast. A theoretical generalization is known, but no one knew whether it was practical.

Based on analysis of norms that arise in the computation, one can show that the crossover point (for general integers) with the Quadratic Sieve is somewhere between 140 and 150 digits.

I ran the algorithm on a variety of numbers between 30 and 90 digits. Extrapolation of this data confirms the theoretical crossover estimate.

It can also be shown that there exist large sets of integers for which NFS is substantially faster than QS. However, these sets are only a small fraction of the entire set of integers. The relevant criterion is whether the number to be factored can be written as a low degree polynomial with small coefficients. Unfortunately, there does not seem to be any good methods for determining when this is possible.

Robert D. Silverman, Bedford, MA

Quadratic Sieve (QS) Improvements

Multiple polynomials

Instead of $F(x) = \left(x + \lfloor\sqrt{N}\rfloor\right)^2 - N$ when factoring N, try $f(x) = ax^2 + bx + c = \frac{1}{4a}[(2ax+b)^2 - (b^2 - 4ac)]$. When sieving over $-M \le x \le M$, then choosing $q \approx \frac{\sqrt{N/2}}{M}, b \approx 0, b^2 - 4ac = N$ gives $f(M) \approx f(-M) \approx -f(0)$. The largest $f(x)$ is $M\sqrt{N/8}$ rather than $2M\sqrt{N}$. Multiple values of a may be used to reduce the size of M when collecting relations.

Large and Two Large Prime Variations

Originally QS required $f(x)$ be B-smooth, where B is the factor base bound. An early modification (also used in CFRAC) allowed one large prime to divide $f(x)$. If $f(x_1) = s_1 R$ and $f(x_2) = s_2 R$ where s_1, s_2 are B-smooth, then $\frac{f(x_1)f(x_2)}{R^2} = s_1 s_2$ is B-smooth. With only slightly more effort R can have two prime factors below B, with several partial relations multiplied together to get a full relation. However this increases disk space and the matrix is more dense.

Peter L. Montgomery, University of California, L.A.

FFT extension to ECM

When attempting to factor an integer N, the Elliptic Curve Method (ECM) selects an elliptic curve E mod N and a starting point P on E. Step 1 computes $Q = M \cdot P$ using the group law, where M is divisible by all small primes. If step 1 fails to locate a zero divisor (and hence a factor) of N, step 2 assumes that $s \cdot Q = O$ (identity element) mod$p$ for some $p|N$ and prime s. The FFT extension will allow $s \approx 10^{10}$ compared to $s \approx 10^7$ for conventional implementations. Using convolution algorithms mod$N$ (see "An FFT extension to the $p-1$ factoring algorithm" by myself

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

and Silverman in Math. Comp. April, 1990), we let:

$$f(X) = \prod_i (X - x(m_i Q))$$

and test

$$\gcd(f(X), f'(X) \prod_j (X - x(n_j Q))) \bmod N$$

for certain chosen sequences $[m_i]$ and $[n_j]$, succeeding if $s|m_i \neq n_j$ with $i \neq j$ or $s|m_i \pm n_j$. Here $x(n \cdot Q)$ denotes the x-coordinate of $m \cdot Q$.

Peter L. Montgomery, University of California, L.A.

FFT-Arithmetics in algebraic extension fields

A short account of recent improvements on the speed of very long integer arithmetics was given. The methods developed are special versions of the so-called ADFT-Transform using normal bases in algebraic extension fields. The application of these tools is to provide a speed-up mechanism in the recursive algorithm design at the crucial point when breaking from the Schönhage-Strassen-Fermat-Transform to more conventional arithmetics. The importance of this method for sieve generation can be seen from the related talks by Silverman & Montgomery.

Thomas Beth, University of Karlsruhe

Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation

Let N be an integer with at least two distinct prime factors. We reduce the problem of factoring N to the task of finding $t+2$ integer solutions $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ of the inequalities

$$\left| \sum_{i=1}^{t} e_i \log p_i - \log N \right| \leq N^{-c} p_t^{1-\delta} \quad \text{and}$$

$$\sum_{i=1}^{t} |e_i \log p_i| \leq (2c-1) \log N + 2\delta \log p_t,$$

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

where $c > 1$ and $0 < \delta < 1$ are fixed and $p_1, \ldots, p_t$ are the first t primes. We show, under the assumption that the smooth integers distribute uniformly”, that there are $N^{\epsilon + o(1)}$ many solutions $(e_1, \ldots, e_t)$ if $c > 1$ and if $\epsilon := c - 1 - (2c - 1)\log\log N / \log p_t > 0$. We associate with the primes $p_1, \ldots, p_t$ a lattice $L \subset \mathbf{R}^{t+1}$ of dimension t and we associate with N a point $\mathrm{N} \in \mathbf{R}^{t+1}$. We reduce the problem of factoring N to the task of finding lattice vectors z that are sufficiently close to N in the 1-norm. The dimension t of the lattice L is polynomial in $\log N$. For $N \approx 2^{512}$ it is about 6300. We also reduce the problem of computing, for a prime N, discrete logarithms of the units in $\mathbf{Z}_{/N\mathbf{Z}}$ to a similar diophantine approximation problem.

Claus P. Schnorr, Universität Frankfurt

Some Reflections on Cryptography

1. While not dissenting from anything Andy Odlyzko said, there are a couple of additional points that should be noted about discrete logarithms. Like factoring, solving discrete logarithms is based on sieving followed by linear equation solving

   (a) The sieveing requires almost no memory, and with care can fit into machine registers, so is purely CPU bound, where as factoring sieving tends to be memory bandwidth bound.

   (b) The linear equations are to be solved over a large finite field (or a direct sum of fields), rather that over $GF(2)$. This tends to make the equation solving even more of a bottleneck that it is for factoring.

2. The amount of work going into sieving is enough to try all 32-bit seeds for typical random-number generators. Hence a source of many random bits is required. We have empirical evidence that carefully bulling bits off an Ethernet will provide a source of bits secure against anyone who wasn’t observing the actual traffic being used as a source of randomness. One open question is: what constitutes a ”good” prime for RSA, and/or for Diffie Hellman?

James Davenport, University of Bath, G.B.

Discrete Logarithms

The only discrete logarithm algorithms that work in all groups G run in time on the order of $\sqrt{|G|}$. Elliptic curve cryptosystems appear to be quite secure at the moment, as the recent work of Menezes, Okamoto and Vanstone applies only to a small and well understood class of curves. On the other hand, Coppersmith's algorithm in fields $GF(2^n)$ is very effective, and could be used to compute discrete logs for n up to perhaps 600. For fields $GF(p)$, discrete logarithm algorithms are only a little less efficient than algorithms for factoring integers of the same size.

Andrew Odlyzko, Murray Hill, NJ

An Efficient Cryptographic Hash Function

We propose an efficient algorithm that hashes messages of arbitrary bit length into an 128 bit hash value. The algorithm is designed to make the production of a pair of colliding messages computationally infeasible. The algorithm has interesting provable properties. Each hash value in $\{0,1\}^{128}$ occurs with frequency at most 2^{-120}.

Claus P. Schnorr, Universität Frankfurt

Planning Requirements for Cryptographic Systems

Workshop objective:
Advice to security system designer in the 1990's.

Problems

	Tactical	Strategic
Authentication	bounded	boundable
Secrecy	bounded	unboundable, esp. for storage systems

Lifetimes of Cryptosystems

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Cipher	From	To
Enigma (many versions)	1920's	≥ 1940's
M-209	1930's	≥ today
KL-7	≈1950	≈1980
KW-7	≈1960	≈1990
DES	1975	≥1993

Storage security systems may be in use much longer.

Traffic Lifetimes

Product announcements	days or
mergers, interest rates	weeks
Trade Secrets (Coca Cola)	decades
H-bomb Secret	> 40 years
Diplomatic Embarrassments	
Fate of Sidney Riley	> 65 years
Identities of Spies	> 50 years
(5th man Venoha)	
Personal Affairs	> 50 years
US. Census Data	100 years
(individual)	

Prediction Difficulties

	Hardware	Software
Expected	faster speeds bigger memories	e.g. better memory management
Not Expected	massively distributed	Coppersmith on logs in $GF(2^n)$ and Quadratic Sieve

Design Problem:

- A system fielded in 1995 may still be in use in 2025 and encrypt something that must be secret until 2075.
- What will we be able to factor in 2075?
- Will someone do an 80 year precomputation for logarithms?

Design Approach:

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

- Determine the longest modulus for fields size that can be accommodated in each application.
- Provide for upgrade paths in design.

Whitfield Diffie, Mountain View, CA

A users view of public-key cryptography

We first noted that ”The future for public-key cryptography is at least as much a function of *what needs to be done* as it is of *what can be done*”.Needs were examined from two points of view: a variety of information integrity protocols were analyzed from the standpoint of trust, and a long list of needed information integrity functions was presented, each item of which is the intended function for some prototcol.

While it is undoubted an oversimplification, a useful way of viewing information integrity protocols is that they are primarily devices for transferring trust from where it exists to where it is needed in order for a protocol function to the trustworthy. As a simple example; the key distribution protocol of ANSI X9.17 is a mechanism for transferring unconditional trust (by the subscribers) in the integrity of a key distribution center (KDC) into a trusted secure communication channel between a pair of the subscribers (the transmitter and receiver) — who must in turn unconditionally trust each other since they have interchangeble capabilities as a consequence of the key distribution: the transmitter can disavow messages that he did sent and the receivers can fraudulently attribute messages to the transmitter which the transmitter did not send. The consequence of the unconditional trust is that no such dispute can be logically arbitrated. A sequence of progressively more complex protocols were analyzed from the standpoint of identifying where trust existed initially, how, to where and when it was transferred — and what the nature of the trust was that finally existed as a result of the protocol being exercized.

The object of an information integrity protocol is to achieve some combination of functions in the presence of distrust and deceit; secrecy, authentication, concurrence, identification, certification, verification, etc. A list of some two dozen of the more important functions was presented and discussed — in part from the standpoint of identifying information integrity primitives. Associated which each function are protocols for its realization.

Gefördert durch
Deutsche
Forschungsgemeinschaft

The protocol must be designed to accommodate the trust relations existing between the participant prior to its execution and to realize the necessary relations thereafter.

The purpose of this talk was to provide an insight into likely future applications for public-key cryptography as a means to achieving information integrity protocols and functions.

Gustavus J. Simmons, Albuquerque, NM

Alternative approach to cryptanalysis

The new wave to design cryptographic schemes and protocols is to use the concept of proven secure cryptosystems. The traditional method of cryptanalysis is to attack the unproven assumption used to design the system. Other new approaches are emerging. To prove that a scheme fulfils a need, a formal model of the need is necessary. When this model is too weak, or is the wrong one, or even when there is no model, problems could occur and the resulting scheme could be insecure. Examples are given in detail. A different problem is that the mathematical proof could be wrong which could imply that the resulting scheme is insecure. Finally a proven secure scheme could be used for an application not covered by the model or the theorem. These problems imply that a cryptanalyst could use other methods to break real world cryptosystems based on proven secure schemes.

Yvo Desmedt, University of Wisconsin, MW

Editor: Markus Frisch, Karlsruhe

Participants

Thomas Beth
European Institute for System Security
Universität Karlsruhe
Am Fasanengarten 5
D-7500 Karlsruhe 1, West Germany
Tel.: ++49-721-608 4205
Fax: ++49-721-696893

Albrecht Beutelspacher
Universität Gießen
Mathematisches Institut
D-6300 Gießen, West Germany
Fax: ++49-641-7022099

James H. Davenport
School of Mathematical Sciences
University of Bath
Claverton Down
Bath, Avon, England BA2 7AY
Fax: ++44-225-826492

Yvo Desmedt
University of Wisconsin — Milwaukee
Department of Electrical Engineering
and Computer Science
P.O. Box 784
Milwaukee, Wisconsin 53201, USA
Tel.: ++1-414-229-4677
Fax: ++1-414-229-6958

Whitfield Diffie
Bell Northern Research
685A East Middlefield Road
P.O. Box 7277
Mountain View, CA 94039-7277, USA
E-Mail: diffie@bnr.ca

Markus Frisch
European Institute for System Security
Universität Karlsruhe
Am Fasanengarten 5
D-7500 Karlsruhe 1, West Germany
Tel.: ++49-721-608 4255
Fax: ++49-721-696893
E-Mail: frisch@ira.uka.de

Willi Geiselmann
Institut für Algorithmen und Kognitive
Systeme
Universität Karlsruhe
Am Fasanengarten 5
D-7500 Karlsruhe 1, West Germany
Tel.: ++49-721-608 4256
Fax: ++49-721-696893
E-Mail: geiselma@ira.uka.de

Hans-Joachim Knobloch
European Institute for System Security
Universität Karlsruhe
Am Fasanengarten 5
D-7500 Karlsruhe 1, West Germany
Tel.: ++49-721-608 4025
Fax: ++49-721-696893
E-Mail: knobloch@ira.uka.de

Arjen K. Lenstra
Bellcore
445 South Street
Morristown, NJ 07960, USA
Fax: ++1-201-829-4878
Tel.: ++1-201-538-9093
E-Mail: lenstra@flash.bellcore.com

Hendrik W. Lenstra, Jr.
Institute for Advanced Study
Olden Lane
Princeton, NJ 08540, USA
Tel.: ++1-609-734-8105
Fax: ++1-609-924-8399
E-Mail: lenstra@guinness.ias.edu

Peter L. Montgomery
University of California — Los Angeles
Departement of Mathematics
Los Angeles, CA 90024, USA
Tel.: ++1-213-826-9498
Fax: ++1-213-206-6673
E-Mail: pmontgom@imath.ucla.edu

Andrew M. Odlyzko
AT&T Bell Labs.
600 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636, USA
Fax: ++1-201-582-2379

Frank Schaefer
Institut für Algorithmen und Kognitive
Systeme
Universität Karlsruhe
Am Fasanengarten 5
D-7500 Karlsruhe 1, West Germany
Tel.: ++49-721-608 4260
Fax: ++49-721-696893
E-Mail: schaefer@ira.uka.de

Claus P. Schnorr
Universität Frankfurt
Fachbereich Mathematik
Robert-Mayer-Straße 6–10
Postfach 11 19 32
D-6000 Frankfurt am Main 11
West Germany
Tel.: ++49-69-798-2526
Fax: ++49-69-798-8383

Robert D. Silverman
The MITRE Corporation
Burlington Road
Bedford, MA 01730, USA
Tel.: ++1-617-271-2743
Fax: ++1-617-271-8752

Gustavus J. Simmons
Sandia National Laboratories
P.O. Box 5800, Org. 200
Albuquerque, NM 87185, USA
Tel.: ++1-505-844-1349
Fax: ++1-505-846-9493

Gefördert durch
DFG Deutsche
Forschungsgemeinschaft