IACR

NEWSLETTER

A Publication of the International Association
for Cryptologic Research

Volume 8 Number 2 June 1991

CONTENTS

IACR Contact List

IACR Business Office
P.O. Box 303
Palo Alto, CA 94302-0303
USA

Officers . . .

President
Thomas A. Berson
Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94301
USA
+1 415 324 0100, berson@sri.com

Vice President
Ingemar Ingemarsson
Linkoping University
Dept. of Electrical Engineering
S-581 83 Linkoping
Sweden
+46 13 281 300, I2@isy.liu.se

Secretary
Rainer A. Rueppel
R^3 Security Engineering
Bahnhofstrasse 242
8623 Wetzikon
Switzerland
+41 1 930 5358

Treasurer
Kevin S. McCurley
Sandia National Labs Div 1423
Albuquerque, NM 87185
USA
+1 505 844 2453, mccurley@sandia.gov

Eurocrypt 91 Chair
Andrew J. Clark
P.O. Box 1156
Brighton, E. Sussex BN1 5GT
United Kingdom
+44 273 566115 (voice/fax)

Crypto 91 Chair
Burton Kaliski, Jr.
RSA Data Security Inc.
10 Twin Dolphin Drive
Redwood City, CA 94065
USA
+1 415 595 8782
+1 415 595 1873 (fax)
burt@rsa.com

Newsletter Editor
Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
+1 519 885 1211 x3041
gbagnew@ccng.waterloo.edu

***Journal of Cryptology* Editor-in-Chief**
Gilles Brassard
Dept. IRO, Univ. de Montreal
C.P. 6128, Succ "A"
Montreal, Quebec H3C 3J7
Canada
+1 514 343 6807,
brassard@iro.umontreal.ca

Directors . . .

Thomas Beth
Institut fur Informatik
Universitaet Karlsruhe
Postfache 6380
D-7500 Karlsruhe 1
Fed Rep Germany
+49 721 608 4205
beth@ira.uka.de

Ernest Brickel
Sandia National Labs Div 1423
Albuquerque, NM 87185
USA
+1 505 846 7564, efbrick@sandia.gov

David Chaum
C.W.I.
Box 4079
1009 AB Amsterdam
The Netherlands
+31 20 529 4167
chaum@mcvax.cwi.nl

Norbert Cot
E.H.E. Informatique
45 rue des Saints-Peres
F-75 006 Paris
France
+33 1 47 03 31 27

Whitfield Diffie
Bell Northern Research
685A E. Middlefield Rd.
Mountain View, CA 94039-7277
USA
+1 415 940 2513, diffie@bnr.ca.us

John Gordon
Lynfield House
Datchworth Green, Herts. 8G3 6TL
United Kingdom
+44 438 811015

Ronald Rivest
MIT Lab for Computer Science
545 Technology Square
Cambridge, MA 02139
USA
+1 617 253 5880
rivest@theory.lcs.mit.edu

Jennifer Seberry
Dept. Comp. Sci., UNSW, AFDA
Canberra, ACT 2600
Australia
+61 62 688182
jennie@csadfa.cs.adfa.oz.au

Scott Vanstone
Dept CO, University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
+1 519 884 8110 x24
svanstone@watmath.waterloo.ca

Editor's Corner

As June has once again come (and gone), I find that, as usual, the newsletter is late for publication. Unfortunately, this time it's more late than usual!

In this issue, Andy Clark gives a report on EUROCRYPT'91 - a conference that almost didn't occur due to the conflict in the middle east. In his comments, he gives thanks to all the members of his team and the program committee who helped make the conference the success that it was. He does omit though, to give thanks to the person who probably did the most - himself. The job of organizing an international conference is a difficult enough task under normal circumstances. In the face of such turmoil and uncertainty, it was a heroic effort. I know from talking to Andy the sleepless nights he put in to ensure that the conference went off without a hitch. I think everyone who attended will join with me in extending our thanks to Andy for a job well done! (P.S., thanks for the EUROCRYPT'91 ale.)

Several items of news which may affect the cryptographic community have come to my attention over the past few weeks. In the United States, a bill (#266) has been introduced which outlines how manufacturers of cryptographic equipment and systems will cooperate with law enforcement agencies. This bill if passed, would seem to indicate that all systems would have a trap door that could be accessed by authorized agencies. I'm sure that we will hear much more about this in the near future.

Also in the US, the National Institute of Standards and Technology (formerly National Bureau of Standards), has announced it will endorse a variant of the ElGamal signature scheme as a standard for digital signatures. This will have significant impact in the North American community and again, I'm sure we'll hear more about this.

On a sadder note, hard economic times have led to the closing of the Philips Research Laboratory in Belgium. The members of this group have made substantial contributions to the science of cryptology over the years. I'm sure the membership of the IACR will join with me in expressing our regrets at this turn of events. One of the group members familiar to all of us, Jean-Jacques Quisquater, is requesting reprints of papers on cryptography in an effort to recreate their library. If you would like to help, these can be sent to:

Jean-Jacques Quisquater
Avenue des Canards, 3
B-1640 Rhode-Saint-Genese
Belgium

GBA.

From the President ...

Dear Members,

Cryptology is on the boil. There are 600 of us; we are in the middle of a heavy conference schedule; five issues of the *Journal of Cryptology* are about to hit our desks.

Eurocrypt '91. Andy Clark, General Chair, and Donald Davies, Program Chair, are to be congratulated for their production of Eurocrypt '91 at the University of Sussex. It was the first IACR sponsored conference with a sound track. Many of the delegates requested information on the music. The conference opened with: Elgar; Variations on an Original Theme, OP.36 'ENIGMA' Introduction and Allegro for String Orchestra, played by the London Philharmonic Orchestra, conducted by Sir Adrian Boult. EMI Ref: TC-CFP-40022. And then, for something different, we heard: Sousa; The Liberty Bell (Monty Python Theme) played by The Band of The Welsh Guards. Private recording provided by the British Broadcasting Corporation. The Engineerium Reception music included: Handel; Water Music, Music for the Royal Fireworks, and Sinfonia from "Messiah". Deutsche Grammophon Ref: 413-148-4 and Beethoven; Symphonies 1&6, played by the London Classical Players, conducted by Roger Norrington and sponsored by LOGICA. EMI Ref: EL-7-49746-4. Other excerpts were from Symphonies 4,5 and 7 in the same series; EMI Ref: EL-7-49656-4 and EL-7-49816-4. I also recall hearing the Pomp and Circumstance march. A few copies of the Eurocrypt '91 Pre-Proceedings are still available at UK£30, postage paid. Contact Andy Clark for details.

Upcoming Conferences. Preparations are being completed for **Crypto '91** by Burt Kaliski, General Chair and Joan Feigenbaum, Program Chair. A preliminary program is in this *Newsletter*. I am looking forward to hearing the papers behind the titles. **Asiacrypt '91** will be our third conference this year. Ninety-seven papers were submitted and are being evaluated by the program committee. There are more details in this *Newsletter*. Looking ahead, please remember that **Eurocrypt '92** will be held 24-28 May at Balatonfured, Hungary.

***Journal of Cryptology*.** We are finally in for a banquet of issues. Volume 3, numbers 2 and 3, and Volume 4, numbers 1, 2, and 3, are all at the publisher and will be mailed before the end of 1991 to those members who hold subscriptions to the various volumes. Many thanks to Ernie Brickell, who served as the Editor-in-Chief for these issues, to members of his editorial board, to the referees, and of course to the authors for their fine work in breaking our *Journal* logjam.

Election Coming – Nominations Sought. Our 1991 election, which will be conducted by a postal ballot mailed to members in early November, will be the largest election IACR has yet held. Seven posts will be contested: President, Vice-President, Secretary, Treasurer, and three Directors. Any member may nominate any member (including him- or herself) for any of these posts. The nominated member must give their consent to the nomination. Send your nominations to me to arrive not later than 1 October 1991.

I hope to see you all in Santa Barbara, and then again in Fujiyoshida,

Tom Berson

We are proud to announce that the Proceedings of Eurocrypt '89 have (finally) appeared in December 1990 in the Springer Lecture Notes in Computer Science (ISBN 3-540-53433-4).

What we are less proud of is that two introductory pages disappeared between the Editors (us) and the final version. These pages precisely thank the sponsors and a number of people that greatly contributed to the financial, organizational and scientific success of the conference. We are happy that these pages can be reprinted in this IACR newsletter.

J.J. Quisquater and J. Vandewalle

EUROCRYPT '89

A workshop on the theory and application of cryptographic techniques

Sponsored by the

International Association for Cryptologic Research (IACR)

Organizing Committee

Joos Vandewalle *(General Chairman)*
Tri An Banh *(ULg, Liège)*
Marijke De Soete *(RUG, Gent)*
Jean Doyen *(ULB, Bruxelles)*
Jean-Marie Goethals *(UCL, Louvain-la-Neuve)*
René Govaerts *(KUL, Leuven)*
Emile Peeters *(CEC, Brussels)*
Jean Ramaekers *(FUN, Namur)*
Bart Preneel *(Local Arrangement)*

Program Committee

Jean-Jacques Quisquater *(Program Chairman)*
Paul Camion *(INRIA, Rocquencourt)*
Yvo Desmedt *(UW, Milwaukee)*
Louis Guillou *(CCETT, Rennes)*
Johan Håstad *(RIT, Stockholm)*
Llorenç Huguet *(UAB, Barcelona)*
Wyn Price *(NPL, Teddington)*
Rainer Rueppel *(Crypto AG, Steinhausen)*
Johan van Tilburg *(PTT-DNL, Leidschendam)*

The conference was generously supported by

Cable Print, Erpe-Mere, Belgium
CRYPTECH, Brussels, Belgium
Digital Equipment Corporation, Brussels, Belgium
Generale Bank of Belgium
Philips Crypto B.V., Eindhoven, The Netherlands
Philips-MBLE, Information Security, Belgium
S.W.I.F.T., La Hulpe, Belgium

List of Previous Conferences Proceedings

1. Advances in Cryptology: A Report on CRYPTO '81, A. Gersho, Ed., UCSB ECE Report no. 82-04, Department of Electrical and Computer Engineering, Santa Barbara CA 93106.
2. Advances in Cryptology: Proceedings of CRYPTO '82, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., Plenum NY, 1983.
3. Advances in Cryptology: Proceedings of CRYPTO '83, D. Chaum, Ed., Plenum NY, 1984.
4. Advances in Cryptology: Proceedings of CRYPTO '84 (Lecture Notes in Computer Science; 196), G.R. Blakley and D. Chaum, Eds., Springer-Verlag, 1985.
5. Advances in Cryptology: Proceedings of CRYPTO '85 (Lecture Notes in Computer Science; 218), H. C. Williams, Ed., Springer-Verlag, 1986.
6. Advances in Cryptology: Proceedings of CRYPTO '86 (Lecture Notes in Computer Science; 263), A.M. Odlyzko, Ed., Springer-Verlag, 1987.
7. Advances in Cryptology: Proceedings of CRYPTO '87 (Lecture Notes in Computer Science; 293), C. Pomerance, Ed., Springer-Verlag, 1988.
8. Advances in Cryptology: Proceedings of CRYPTO '88 (Lecture Notes in Computer Science; 403), S. Goldwasser, Ed., Springer-Verlag, 1990.
9. Advances in Cryptology: Proceedings of CRYPTO '89 (Lecture Notes in Computer Science; 435), G. Brassard, Ed., Springer-Verlag, 1990.
10. Cryptography: Proceedings, Burg Feuerstein 1982 (Lecture Notes in Computer Science; 149), T. Beth, Ed., Springer-Verlag, 1983.
11. No Proceedings were published for EUROCRYPT '83, which was held in Udine, Italy.
12. Advances in Cryptology: Proceedings of EUROCRYPT '84 (Lecture Notes in Computer Science; 209), T. Beth; N. Cot, and I. Ingemarsson, Eds., Springer-Verlag, 1985.
13. Advances in Cryptology: Proceedings of EUROCRYPT '85 (Lecture Notes in Computer Science; 219), F. Pichler, Ed., Springer-Verlag, 1986.
14. No proceedings were published for EUROCRYPT '86, which was held in Linköping, Sweden.
15. Advances in Cryptology: Proceedings of EUROCRYPT '87 (Lecture Notes in Computer Science; 304), D. Chaum, W. Price, Eds., Springer-Verlag, 1988.
16. Advances in Cryptology: Proceedings of EUROCRYPT '88 (Lecture Notes in Computer Science; 330), Ch. Günther, Ed., Springer-Verlag, 1988.

Eurocrypt '91 Conference Report

Eurocrypt '91 was held between 8th and 11th April 1991 at the University of Sussex in Brighton, U.K.. The conference was sponsored by I.A.C.R. and held in association with Logica Aerospace and Defence Limited, ABN Bank, Coopers and Lybrand Deloitte and Northern Telecom.

Although 284 delegates from 27 countries registered an intent to attend, only 275 actually made it through the door. This represented a small increase over the previous year (272 at Aarhus). While this might appear a rather 'average' performance, you may recall that events in the Gulf in late 1990, early 1991 had a major impact on people's travel plans! As a result, a large number of potential delegates had to decline to register. Without the shadow of these unfortunate events, Eurocrypt '91 may have been a world beater.

The geographical representation was as follows:

Australia	6	Republic of China	2
Austria	4	Romania	2
Belgium	12	Singapore	2
Canada	3	South Africa	3
Denmark	9	South Korea	3
Finland	2	Spain	5
France	26	Sweden	13
Germany	37	Switzerland	8
Hungary	5	The Netherlands	23
Israel	4	United Kingdom	55
Italy	10	USA	21
Japan	7	USSR	2
Norway	7	Yugoslavia	1
People's Rep of China	3		

This year saw the first ever papers being presented by authors from the USSR - two delegates attended. The Organising Committee was also pleased to welcome two delegates from Romania who also attended for the first time.

43 formal papers were presented over the four day period, these were selected from 97 papers submitted. A most stimulating Rump Session under the chairmanship of 'Gentleman' John Gordon provided an excellent opportunity to savour even more complex papers, each delivered in under 7.5 minutes.

Through the generosity of the supporting associates, the Organising Committee was able to organise two social events. The first, a trip to the British Engineerium, was held on the Monday evening and gave all the delegates who attended an early opportunity to get to know each other in a most stimulating environment. The second, held on the Tuesday evening, was a private guided tour of the Royal Pavilion. Our guide, Anne Kenney, helped develop a unique opportunity for the delegates to inspect this remarkable building and its contents at close quarters.

The highlight of the conference of course was the material presented, and congratulations must go to the Programme Committee who made such an excellent selection:

Donald Davies	(Programme Chair, RHBNC)
Thomas Beth	(Univ. Of Karlsruhe)
Colin Boyd	(Univ. Of Manchester)
Norbert Cot	(EHEI Universit, Paris)
Viveke Fåk	(Linkping University)
John Gordon	(Cybermation Limited)
Siegfried Herda	(GMD, Germany)
Arjen Lenstra	(Bellcore, NJ)
Tsutomu Matsumoto	(Yokohama National Univ.)
Fred Piper	(RHBNC)
Claus Schnorr	(Universität Frankfurt)

As well as those whose submissions made it possible.

I would like to record my personal thanks to a remarkable team who made the job of General Chair a comfortable one to occupy - the other members of the Organising Committee:

Keith Martin	(RHBNC)
Martin Meikle-Small	(Aspen Consultants)
Ben Meisner	(RHBNC)
Kathleen Quinn	(RHBNC)
Matthew Robshaw	(RHBNC)

And a special mention for Mick Tucker who, despite the collapse of his employer's company, still managed to arrange all of the travel for the four days and negotiate special discounts!

We were all happy with the outcome of the conference and hope that you all were too. Eurocrypt is a unique opportunity to make friends with kindred spirits from many other countries and backgrounds - to my successor at Eurocrypt '92 (Tibor Nemetz) I wish you and your team every success - hang in there, it feels great when it's all over!

Andrew J Clark, General Chair
June 1991

Preliminary Schedule for CRYPTO'91

Sunday, August 11, 1991

========================

4:00 - 8:00 p.m. Registration
5:30 - 6:30 p.m. Dinner
7:00 - 10:00 p.m. Cocktail Party

========================

Monday, August 12, 1991

========================

Session 1: Protocol Design and Analysis
Chair: Michael Merritt (AT&T Bell Laboratories, USA)

8:30 - 9:15 a.m.
Invited Lecture: Martin Abadi (DEC Systems Research Center, USA)
A Calculus for Access Control in Distributed Systems
(with M. Burrows (DEC-SRC, USA), B. Lampson (DEC-CRL, USA), and
G. Plotkin (University of Edinburgh, Scotland))

9:30 - 9:50 a.m.
Deriving the Complete Knowledge of Participants in
Cryptographic Protocols
M. Toussaint (University of Liege, Belgium)

9:55-10:15 a.m.
Systematic Design of Efficient Provably Secure Two-Way
Authentication Protocols
R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten,
R. Molva, and M. Yung (IBM)

10:20 - 10:40 a.m. Break

Session 2: Combinatorics and Authentication
Chair: Ueli Maurer (Princeton University, USA)

10:40 - 11:00 a.m.
Combinatorial Characterizations of Authentication Codes
D. Stinson (University of Nebraska, USA)

11:05 - 11:25 a.m.
Universal Hashing and Authentication Codes
D. Stinson (University of Nebraska, USA)

11:30 - 11:50 a.m.
On Correlation-Immune Functions
P. Camion, C. Carlet, P. Charpin and N. Sendrier (INRIA, France)

12 noon - 1 p.m. Lunch

Session 3: Secret Sharing and Information Theory
Chair: Ingemar Ingemarson (University of Linkoping, Sweden)

1:30 - 1:50 p.m.
On The Size of Shares for Secret Sharing Schemes
R. Capocelli (University of Rome, Italy), A. DeSantis,
L. Gargano, and U. Vaccaro (University of Salerno, Italy)

1:55 - 2:rk (IBM Almaden, USA)

2:20 - 2:40 p.m.
Non-Interactive and Information-Theoretic Secure Verifiable
Secret Sharing
T. Pedersen (Aarhus University, Denmark)

2:45 - 3:05 p.m.
Secret Key Exchange Using a Random Deal of Cards
M. Fischer and R. Wright (Yale University, USA)

3:05 - 3:25 p.m. Break

Session 4: Cryptanalysis
Chair: Tom Berson (Anagram Laboratories, USA)

3:25 - 3:45 p.m.
Differential Cryptanalysis of Snefru, Khafre, REDOC-II,
LOKI, and Lucifer
E. Biham and A. Shamir (Weizmann Institute, Israel)

3:50 - 4:10 p.m.
A Known Plaintext Attack on FEAL-4 and FEAL-6
A. Tardy-Corfdir and H. Gilbert (CNET, France)

4:15 - 4:35 p.m.
A Switching Closure Test to Analyze Cryptosystems
H. Morita, K. Ohta, and S. Miyaguchi (NTT, Japan)

4:40 - 5:00 p.m.
An Attack on the Last Two Rounds of MD4
B. Den Boer (Philips Crypto BV, The Netherlands) and
A. Bosselaers (Katholieke Universiteit Leuven, Belgium)

5:05 - 5:25 p.m.
The Cryptanalysis of a New Public-Key Cryptosystem based on Modular Knapsacks
Y. M. Chee (NCS, Singapore)

5:30 - 6:30 p.m. Dinner
7:00 - 10:00 p.m. Cocktail Party

========================

Tuesday, August 13, 1991

========================

Session 5: Complexity Theory
Chair: Joan Feigenbaum (AT&T Bell Laboratories, USA)

8:30 - 8:50 a.m.
A One-Round, Two-Prover, Zero-Knowledge Protocol for NP
D. Lapidot and A. Shamir (Weizmann Institute, Israel)

8:55 - 9:15 a.m.
Interactive Proofs With Space-Bounded Provers
R. Rubinfeld (DIMACS-Princeton, USA)

9:20 - 9:40 a.m.
Functional Inversion and Communication Complexity
S.-H. Teng (Carnegie Mellon University, USA)

9:45 - 10:05 a.m.
The Use of Interaction in Public Cryptosystems
S. Rudich (Carnegie Mellon University, USA)
10:10 - 10:30 a.m. Break
Session 6: Cryptographic Schemes based on Number Theory
Chair: Kevin McCurley (Sandia National Laboratories, USA)
10:30 - 10:55 a.m.
New Public-key Cryptosystems Based on Elliptic Curves over the Ring Z_m
K. Koyama (NTT, Japan), U. Maurer (Princeton University, USA),
T. Okamoto (NTT, Japan), and S. A. Vanstone (University of
Waterloo, Canada)
11:00 - 11:20 a.m.
Efficient Algorithms for the Construction of Hyperelliptic
Cryptosystems
T. Okamoto (NTT, Japan) and K. Sakurai (Mitsubishi, Japan)
11:25 - 11:45 a.m.
CM-Curves with Good Cryptographic Properties
N. Koblitz (University of Washington, USA)
11:50 a.m. - 12:10 p.m.
A New ID-Based Key Sharing System
S. Tsujii and J. Chao (Tokyo Institute of Technology, Japan)
12:15 p.m. - 1:00 p.m. Lunch
Free Afternoon
5:30 p.m. - 6:30 p.m. Dinner
7:00 p.m. - ??? Rump Session

======================

Wednesday, August 14, 1991

======================

Session 7: Pseudorandomness
Chair: Josef Pieprzyk (University of New South Wales, Australia)
8:30 - 9:15 a.m.
Invited Lecture: Michael Luby (ICSI, USA)
Construction of Pseudorandom Generators from Any One-Wan Diego, USA), and L. Levin (Boston University, USA))
9:30 - 9:50 a.m.
New results on Pseudorandom Permutation Generators Based
on the DES Scheme
J. Patarin (INRIA, France)
9:55 - 10:15 a.m. Break
Session 8: Applications and Implementations
Chair: Tony Rosati (Newbridge Microsystems)
10:15 - 10:35 a.m.
Faster Modular Multiplication by Operand Scaling
C. D. Walter (UMIST, England)
10:40 - 11:00 a.m.
Universal Electronic Cash
T. Okamoto and K. Ohta (NTT, Japan)
11:05 - 11:25 a.m.
How to Break and Repair a "Provably Secure" Untraceable Payment System
B. Pfitzmann and M. Waidner (University of Karlsruhe, Germany)
11:30 - 11:55 a.m.
Practical Quantum Oblivious Transfer and Bit Commitment
C. Bennett (IBM Yorktown, USA), G. Brassard (University of
Montreal, Canada), and C. Crepeau (University of Paris-Sud, France)
12:00 - 1:00 p.m. Lunch
1:30 - 1:50 p.m.
Exploiting Parallelism in Hardware Implementation of the DES
A. Broscius M Yorktown, USA)
2:15 - 2:45 p.m.
Foundations of Secure Interactive Computing
D. Beaver (AT&T Bell Laboratories, USA)
2:55 - 3:25 p.m.
Secure Computation
S. Micali and P. Rogaway (MIT, USA)
3:35 - 3:55 p.m.
A Cryptographic Scheme for Computerized General Elections
K. Iversen (Norwegian Institute of Technology, Norway)
4:00 - 4:20 p.m.
Efficient Multiparty Protocols Using Circuit Randomization
D. Beaver (AT&T Bell Laboratories, USA)
4:30 - 6:00 p.m. IACR Business Meeting
6:00 - Dusk Beach Barbecue

======================

Thursday, August 15, 1991

======================

Session 10: Viruses
Chair: Joan Feigenbaum (AT&T Bell Laboratories, USA)
8:30 - 9:15 a.m.
Invited Lecture: Jeff Kephart (IBM Yorktown, USA)
Epidemiological Models of Computer Viruses
(with S. White (IBM Yorktown, USA))
9:30 - 9:50 a.m. Break
Session 11: Public-Key Cryptosystems and Signatures
Chair: Eiji Okamoto (NEC, Japan)
9:50 - 10:20 a.m.
Non-Interactive Zero-Knowledge Proof of Knowledge and
Chosen-Ciphertext Attack
C. Rackoff and D. Simon (University of Toronto, Canada)
10:25 - 10:55 a.m.
Towards Practical Public Key Systems Secure Against
Chosen-Ciphertext Attacks
I. Damgaard (Aarhus University, Denmark)
11:00 - 11:20 a.m.
Shared Generation of Authenticators and Signatures
Y. Desmedt and Y. Frankel (University of Wisconsin, USA)
11:25 - 11:45 a.m.
Cryptographically Strong Undeniable Signatures, Unconditionally
Secure For The Signer
D. Chaum (CWI, The Netherlands), E. van Heijst (CWI, The
Netherlands), and B. Pfitzmann (University of Karlsruhe, Germany)
11:50 a.m. - 1:00 p.m. Lunch

CONFERENCE INFORMATION
ASIACRYPT'91

November 11-14, 1991

Cosponsored by
the International Association for Cryptologic Research
and
the Institute of Electronics, Information and Communication Engineers

ASIACRYPT'91 is the first international symposium on cryptology held in Asia. The conference deals with all aspects of the theory and applications of cryptography. It is planned to start **in the morning of Monday 11th November** and end **in the noon of Thursday 14th November**. Advance check-in on the Sunday with overnight accommodation will be available.

The meeting will take place at the **Hotel Highland Resort** (Phone: +81-555-22-1000, FAX: +81-555-22-3115) which is located at the foot of Mt. Fuji in a natural setting. Autumn is the best season in Japan, fresh air, beautifully colored leaves, ... You can enjoy a great view of Mt.Fuji every day at the meeting place. The hotel is first class western style (Single;¥14,000 / Twin;¥10,000). Chuo Kosoku (Highway) bus service is available from Shinjuku Station to this hotel every 30 minutes. It takes approximately 100 minutes.

Planned social activities include a reception, a rump session and banquet for the evening. An optional tour has been arranged on Tuesday afternoon to visit a Japanese shrine, a historical museum in this area and lake Yamanaka, including a Japanese barbecue lunch "*Robatayaki (炉端焼き)* ".

Registration form for the conference is enclosed here in. Please enclose your payment (conference fee plus optional tour if desired) with your registration form. Hotel and transport charges must be paid separately by each person. Reservations for both can be made through ASIACRYPT'91. The deadline for registration is **30th September 1991** .

If your friends or colleagues are interested in this conference, please pass this information along.

I am looking forward to seeing you in Fujiyoshida this November!

Kenji Koyama, ASIACRYPT'91
NTT Basic Research Lab.
3-9-11 Midoricho, Musashino-shi, Tokyo 180, Japan
Facsimile: +81-422-59-3240, Telephone: +81-422-59-2189
E-mail: koyama%ntt-20.ntt.jp@relay.cs.net

ASIACRYPT'91 REGISTRATION FORM

The deadline for registration is 30th September 1991

Last Name: ____________________ First Name: ____________________

Affiliation: ____

Address: ____________________ Title: □Mr. □Ms. □Dr. □Prof.

____________________ Phone: ____________________

____________________ Fax: ____________________

ZIP Code: ______Country: __________ Email: ____________________

I will attend **ASIACRYPT'91** and wish to register for the conference and following facilities:

Conference Fee: regular ¥50,000 (¥55,000 after Sept. 1st) ¥ ____________

attended EUROCRYPT'91 or CRYPTO'91 ¥45,000 (¥50,000 after Sept. 1st)
full-time students (proof required) ¥30,000 (¥33,000 after Sept. 1st)
(Remark: Payment of the conference fee entitles you to become a member of the IACR through December 1992 at no extra charge. Members joining the IACR at ASIACRYPT'91 will receive volume 5 of the *Journal of Cryptology*, published by Springer-Verlag, at no extra charge.) Do you wish to be an **IACR member?** □Yes □No.

Accompany person meal ticket: ¥10,000 (including three lunches and a banquet)
(Remark: Conference Fee includes one person meal ticket.) ¥ ____________

Optional tour ¥2,000 per person
number of persons: ______. ¥ ____________

TOTAL FEE ENCLOSED (This fee is NOT Returnable) ¥____________

PAYMENT FROM ABROAD MUST BE IN JAPANESE YEN DRAWN ON A JAPANESE BANK OR INTERNATIONAL MONEY ORDER PAYABLE IN JAPANESE YEN PAYABLE TO ASIACRYPT'91. JAPANESE DELEGATES MUST PAY BY POSTAL DRAFT (郵便小為替) PAYABLE TO ASIACRYPT'91.

Send it to: Kenji Koyama, ASIACRYPT'91
NTT Basic Research Lab.
3-9-11 Midoricho, Musashino-shi, Tokyo, 180, Japan

---

*Hotel and transport charges must be paid separately by each person. Reservations for both can be made through **ASIACRYPT'91.***

HOTEL RESERVATION (the Hotel Highland Resort):

Number of accompanying persons: ___. Reservation: □ single or □ twin room(s)

If you select twin room(s), preferred roommate: ____________________.

Check In Date: November ______ Check Out Date: November ______

Price per person and per day, single (¥14,000) / twin (¥10,000)

TRANSPORTATION (Bus Service from/to Shinjuku in Tokyo):

Fee of ¥1,520 paid to driver.
I would like use the highway bus service.
□ no
□ yes and I expect to leave Shinjuku in Tokyo at __________ AM/PM on ____ November.
and to leave the Hotel Highland Resort at __________ AM/PM on ____ November.

1992 Membership Application (Memberships Expire 12/92)

International Association for Cryptologic Research

Membership is open to all persons supporting the purpose of IACR, which is to further research in cryptology and related fields. Membership benefits include subscriptions to the *Journal of Cryptology* and to the *IACR Newsletter* and voting privileges.

Membership is for a calendar year. Persons who attend Eurocrypt 91, Crypto 91, or Asiacrypt 91 are already enrolled for the calendar year 1992. Payment on this form will bring Volume 5 of the *Journal of Cryptology*, whenever it is published.

Full-time students may become members at reduced fees provided they obtain a signature certifying their status from a faculty member at their institution.

Please type or print clearly!

First Name ________________ Last Name ___________________________

Affiliation/Institution____

Address ____

____

____

Telephone ____

Network Address____

Type of membership desired (check one)
__ Regular member (Dues: $40)
__ Full-time Student member (Dues: $20)

Faculty name ____________________________________

Faculty signature ______________________________

New Member? ___. Renewing Member? ___.

Amount enclosed (**<u>US$ on a US bank</u>** payable to IACR) $________

Return this form to:

IACR
P.O. Box 303
Palo Alto, CA 94302-0303
USA

IACR
PO Box 303
Palo Alto CA 94302-0303
USA