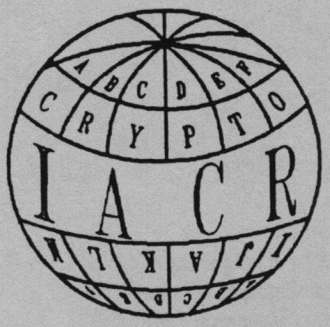

IACR

NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 7 Number 2 June 1990

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 90 Chair
Peter Landrock
Matematisk Institut
Aarhus Universitet
Ny Munkegade, Bygning 530
DK-8000 Aarhus C
Denmark
+45 6 127 188, landrock@daimi.dk

Crypto 90 Chair
Sherry McMahan
Cylink Corp.
110 So. Wolfe Road
Sunnyvale, CA 94086
USA
+1 408 735 5830

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

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
(see J. of Cryptology Editor)

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

Dorothy E. Denning
Digital Equipment Corp.
Systems Research Center
130 Lytton Ave.
Palo Alto, CA 94301
USA
+1 415 853 2252, denning@src.dec.com

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
Zergo Systems Ltd.
Communications House
Winchester Road
Basingstoke, Hants. RG22 4AA
United Kingdom
+44 256 818800

David Kahn
Cryptologia Magazine
120 Wolley's Lane
Great Neck, NY 11023
USA
+1 516 487 7181

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

Editor's Corner

It seems that every time I write this editorial, I must grope around to find newsworthy items. In this case though, some interesting events have occurred since the last newsletter. So, let's begin.

We have yet another cryptosystem designer challenging our collective abilities (see call for attack later in this issue). The REDOC system (coder spelt backwards) is up for attack and it carries a $25,000 US reward to the first person who can break one round of the system. For the record, this challenge is put to us by CRYPTECH Inc. of Jamestown, New York (this is in no way connected to CRYPTECH Systems Inc. of Canada, or CRYPTECH of Belgium) and $25,000 has been placed in an escrow account. We still have not heard any successful results for the FEAL challenge, so you now have two systems to try to break in your spare time.

The latest news from the factoring front is that Lenstra, et. Al have just completed the factorization of Fermat F9 ($2^{512}+1$)(see the predictions in the January newsletter).

2 ^ 512 + 1 =
1340780792994259709957402499820584612747936582059239337772356144372176401
30073546976801874298166903427690031858186486050853753882811946569946\
433649006084097 =
2424833
* 74556028256478842083373957362004549187833663426 57
* 74164006262753080152478714190193747405994078109751902390582131614441571
59504705008092818711693940737

We had an election ballot and bylaws ballot in the last issue. The results were (drumroll to be inserted here):

Thomas Berson is the President

Rainer Rueppel is the Secretary-Treasurer

The new bylaws were accepted as presented in the January newsletter

(P.S. a special thanks is extended to Wyn Price for organizing and conducting the election and ballot on the bylaws - Thanks Wyn.)

For those of you who attended EUROCRYPT, you'll join with me in thanking Peter Landrock (general Chair) and Ivan Damgård (program Chair) for an excellent conference. We were treated to the warm hospitality of Arhus and every detail of the conference ran smoothly - all in all, an excellent time. (P.S. Who would have guessed that so much musical talent lurks in the membership of the IACR?)

At the BoD's meeting at EUROCRYPT, the location of EUROCRYPT'92 was selected, the winner was.... Hungary, which seems quite appropriate in these days of detente.

There was only one sour note associated with EUROCRYPT'90, it appears that the Danish government refused to issue visas to two of our South Africa colleagues. While the workings of international politics are beyond our control, it is sad to think that our research should be hindered by such policies.

On the lighter side, I was pleased to note that Andy Clark, (general Chair for EUROCRYPT'91) has already finished arrangements for most of the social activities next year. It seems we will certainly be wined and dined in true British style.

From The President . . .

Dear IACR Members,

The last issue of this Newsletter contained a ballot. The election results are in. Rainer Rueppel and I would like to thank you for your confidence in reelecting us to the offices of Secretary-Treasurer and President. Even more gratifying was your approval of the proposed revision to the IACR Byelaws. The revision took effect on 15 March.

The newly revised byelaws establish two new officers. With the Board's approval, and with the appointees' gracious consent, I have asked Ingemar Ingemarsson to fill the vacant post of Vice President and Kevin McCurley to fill the vacant post of Treasurer. Both Ingemar and Kevin have already made significant contributions to IACR. I am looking forward to continuing to work with them.

There will be an election later this year for three directors to serve three-year terms on the IACR Board. Members interested in running should contact me not later than 1 October 1990.

You will have heard about the tragic and destructive fire in Santa Barbara, a city which has welcomed the cryptologic community during ten or so years of Crypto conferences. The news today says that the fire is under control, but not yet extinguished. So far as I can learn, our colleagues in Santa Barbara were not burned out, although the entire city is stunned by the sudden and brutal destruction. Also, it seems that the University has escaped damage, and that Crypto '90 can be held as planned.

I'm looking forward to seeing you there.

Tom Berson

Report on the Journal of Cryptology
prepared for Eurocrypt 90

The Journal of Cryptology is well on its way to getting back on publication schedule. Volume 2, Issue 1 is in press. The contents of it are:

- M. Abadi and J. Feigenbaum, **Secure circuit evaluation**
- K. Nishimura and M. Sibuya, **Probability to meet in the middle**
- D.R. Stinson, **The combinatorics of authentication and secrecy codes**
- Li Gong and D.J. Wheeler, **A matrix key-distribution scheme**

The following articles have been typeset:

- Harald Niedereiter, **A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences**, 8 pages.
- Gustavus J. Simmons, **A cartesian product construction for unconditionally secure authentication codes that permit arbitration**, 28 pages.

The following articles have been accepted and sent to the publisher for typesetting:

- Philippe Godlewski and Chris Mitchell, **Key-minimal cryptosystems for unconditional secrecy**, 54 pages.
- Michael Walker, **Information-theoretic bounds for authentication schemes**, 23 pages.
- Réjane Forré, **Methods and instruments for designing s-boxes**, 25 pages.
- Sean Murphy, **The cryptanalysis of FEAL-4 with twenty chosen plaintexts**, 12 pages.
- Chris Mitchell, **Enumerating boolean functions of cryptographic significance**, 34 pages.

This is enough material for another two issues. However, three of these papers are on authentication theory and I don't think it would be good to have more than one paper per issue on any such specific subject. In any case, there will be no problem in publishing three regular issues this year.

Of the regular submissions, I have the following statistics:

- 28 papers accepted
- 41 papers rejected
- 9 papers appear to have died from author apathy
- 7 papers are awaiting author revision
- 19 papers are awaiting review (referees are over deadline on 11 of these)

The special issues are also going well. Two articles have already been accepted by Joan Feigenbaum for the special issue on Crypto 89. They are:

- Ueli M. Maurer and James L. Massey, **Local randomness in pseudo-random sequences**
- Ernest F. Brickell and Danial M. Davenport, **On the classification of ideal secret sharing schemes**

In addition, one more paper is in close to final form and another is being revised by the author.

Tom Berson and Rainer Rueppel have received about 20 papers for possible inclusion in the special issue on applications. Depending on the quality of these submissions, this could overflow into more than 1 issue.

Springer has provided me with the following subscription information as of Dec. 31, 1989:

	1988	1989
North Am.	112	117
Outside North Am.	142	150
IACR	376	701

The Monte Verità Seminar

FUTURE DIRECTIONS IN CRYPTOGRAPHY *

In Spring 1989 a "Call for Applicants to Participate in the Monte Verità Seminar", October 15-21 in Switzerland was distributed by the organizers Prof. Dr. James L. Massey of the Swiss Federal Institute of Technology Zurich (Eidgenössische Technische Hochschule [ETH] Zurich) and Prof. Dr. Hansjürg Mey of the University of Bern.

The purpose of this seminar, to "provide a forum where fundamental questions concerning the future of cryptography can be discussed in an open and relaxed manner by both acknowledged experts and relative newcomers to cryptographic research", could be read in the invitation. A special aim was to consider fundamental questions and problems themselves and not to present solutions to problems as it is mostly done in technical meetings and conferences. To make the seminar most effective, it was located in a secluded place – the Centro Stefano Franscini at the Monte Verità near Ascona in Switzerland – and strictly limited to fifty participants. The format of the seminar was to be prepared talks followed by extended discussions. As will be seen later, spontaneous talks and sessions also arose.

Monte Verità is a hill 350 meters above sea level (or 150 meters above Ascona) on the beautiful lake, Lago Maggiore ("Greater lake"). Historically, it is a place where centuries ago the Romans enjoyed the beauty of this area, called Monte Monescio until about the end of the 19th century. Today Monte Verità is a secluded place and provides a relaxing environment. From 1900 to 1920 Monte Verità, "the Mountain of Truth" becomes famous as a center for a new way of life under the founders, the pianist and feminist leader, Ida Hofmann, Henry Oedenkoven, the son of an industrialist, and the brothers Karl and Arthur (Gusto) Gräser. The experiment ultimately failed and the founders of Monte Verità emigrated first to Spain and then Brazil. But the legend of this place and the near village attracted countless notables of literature, film, trade and industry to visit or settle around the Monte Verità and made Ascona to the famous tourist center that it is today. 1926 Monte Verità is acquired by Baron Eduard von der Heydt, banker of the former German Kaiser William II and one of the greatest collectors of contemporary, oriental and primitive art. 1927 the artists of the "Bauhaus" school (Albers, Bayer, Breuer, Gropius, Schawinsky and Schlemmer) discover Ascona as a holiday resort and a world apart from "Bauhaus"and the Monte Verità Hotel is built by Emil Fahrenkamp in "Bauhaus" style. This new trial also does not succeed and ends with a financial debacle. After the death of Baron Eduard von der Heydt, Monte Verità becomes 1964 the property of the Republic and Canton Ticino. According to his will, Monte Verità should become a site where cultural events of major importance take place. For a long period there were no "cultural events of major importance". Therefore, the government of the Republic and Canton Ticino began looking for a solution and solved the problem by first establishing the "Foundation Monte Verità" and shortly thereafter, in April 1989, by entering into an agreement with the ETH Zurich concerning the "Centro Stefano Franscini" at Monte Verità . This agreement proposed the utilization of that center's infrastructure by the ETH Zurich for five weeks in 1989 and for 15 to 20 weeks in 1990 to arrange seminars, workshops and similar events. As director of The Centro Stefano Franscini (and one of the major initiators for this solution), Professor K. Osterwalder from the ETH Zurich suggested the idea of promoting academic activities in the Italian-speaking part of Switzerland, where no university exists.

* Abridged version. Full version available from Newsletter Editor

The official inauguration of the Centro Stefano Franscini was held on the 2nd of October 1989. The impression is now that the five weeks of its activities in 1989 were a full success. The time-table and contents of those weeks were as follows:

September 25-29: Workshop on FIELD SCALE WATER AND SOLUTE FLUX IN SOIL. This workshop was intended to serve as a platform for an informal exchange of knowledge and ideas, as an occasion to define problem areas for future research in this field.

Oktober 2-7: Seminario IL COMMENTO AI TESTI. [Seminar on COMMENTS ON (literary) TEXTS. In a research report, attracting attention for a wide part of Italian philology, the following aspects will be treated:
1. Critical methods, theoretical and practical implications for the elaboration of comments to literary texts,
2. Historical development of text comments,
3. Reflections to existing comments and remarks on comments in preparation,
4. Plan for desirable comments.]

October 8-14: Symposium on BIOPHYSICAL AND MATHEMATICAL ANALYSIS OF NEURAL NETWORKS. In 1988, a special-interest group "Neuro-Informatik Zurich" was established jointly between the ETH and the University of Zurich with the aim to facilitate interdisciplinary studies, to provide an efficient sharing of knowledge and resources and to stimulate joint solutions to novel problems in the field of neuro-informatics.

October 15-21: Seminar on FUTURE DIRECTIONS IN CRYPTOGRAPHY. The meeting was intended to have an informal character, with few lectures but a great deal of time for discussions, informal seminars, and private work.

October 22-29: Workshop on GEOMETRIC QUANTUM FIELD THEORY. The meeting was intended to have an informal character, with few lectures but a great deal of time for discussions, informal seminars, and private work.

In each week there was one public session for the interested public, presented normally in Italian:

September 25: Four short talks concerning the workshop content (partly in German and English)

October 7: Prof. Dante Isella: ESPERIENZE DI COMMENTI (Experiences with Comments on Texts)

0ctober 13: Prof. Dr. Marco Annaratone: ELABORAZIONE DATI PARALLELA E RETI NEURALI: STATO ATTUALE E PROSPETTIVE FUTURE (Parallel Data Processing and Neural Networks: State of the Art and Future Developments)

October 17: Prof. Dr. Andrea Sgarro: CRITTOGRAFIA PER IL PROFANO (Cryptography for the Layman)

October 26: Prof. Dr. Gianni Jona-Lasinio: MATEMATICA E FISICA: FENOMENOLOGIA DI UN RAPPORTO (Mathematics and Physics: Phenomenology of a Relation)

As seen above, the fourth week of activity at the Centro Stefano Franscini was occupied by the seminar "Future Directions in Cryptography". The seminar location of Monte Verità, "the place where our minds can reach up to the heavens ...", "the mountain of truth ..." seems to have been chosen right. "What

better motto than this for our Monte Verità Seminar *Future Directions in Cryptography* ? We hope these six days will bring us all closer to the truth of our ancient art, but young science. We hope too a little of the spirit left behind by these utopians will make these days special ones in your life" claimed the organizers James L. Massey and Hansjürg Mey in their welcome. The question whether their hope has been fulfilled is to be answered with a clear YES ! First, one must thank the organizers for their excellent work. There was nothing that could be criticized , beginning with the seminar program and execution, the infrastructure and support, rooms and food and so on. The seminar was attended by 51 participants, including the organizers, from fifteen countries whereby 33 were speakers for 37 talks and eleven served as chairman for the fourteen Sessions with the following distribution (the first figure shows the number of participants, the second the number of talks, and third the number of chairmen):

Austria (6/5/1), Belgium (1/1/0), England (1/1/0), Federal Republic of Germany (4/2/0), Finland (1/0/0), France (3/2/0), German Democratic Republic (1/1/0), Italy (2/3/0), Japan (1/1/0), Netherlands (3/2/3), Saudi Arabia (1/0/0), Sweden (5/2/2), Switzerland (14/7/5), USA (6/9/3), Yugoslavia (2/1/0).

Summarizing it can be said: A very busy and active team! This becomes also obvious from the "Final Program" which was not final in the least. Jim Massey distributed later the "Program as Actually Presented" which is reproduced in the enclosed table 1. There were two changes from the "Final Program":

- Gus Simmons replaced with his talk on "Information integrity" in the Thursday morning session on "User Considerations" the talk on "Operational aspects of cryptographic systems" by Pierre Schmid who could not come, and
- Guy Chassé in the Friday morning session on "Public-Key Cryptography" with his talk "The discrete logarithm problem and algebraic curves" replaced the talk on "Complexity of public-key cryptography" by F. R. Cossec who also could not come.

Two additional talks were given:

- one on Friday morning by José Pastor-Franco on "The 'Smart Post' System" and
- one on Saturday morning by Erwin Leitner on "Computational security of secret-key cipher algorithms".

Initiated by Jim Massey and David Chaum respectively, two spontaneous activities took place namely

- an impromptu session on "The relation between the information-theoretic and complexity-theoretic approach to cryptography" on Monday evening and
- a second impromptu session on "The development of a European Encryption Standard" on Thursday evening, that was continued on Friday evening.

Both of these impromptu sessions attracted many interested participants and contained a lot of good ideas and points of discussion.

The aim of the organizers was especially to have as much discussion as possible. Therefore all speakers listed in table 1 were alloted twenty-five minutes of presentation time, except for a few long talks with 45 and some short talks with fifteen minutes. About the same amount of time was then available for discussion and – as reality showed – that was not too much. Taking a look at the program, it may at first seem conventional like that of other workshops or seminars on cryptography. In the fourteen sessions naturally conventional items e.g. Design of Secret-Key Ciphers I and II, Stream Ciphers I and II, Authentication I and II and Public-Key Cryptography were included, but the viewpoint was totally different. There was no attempt at solutions of problems, but some old unsolved problems were highlighted, some new problems were made evident in keeping with the seminar motto, "future directions in cryptography". A closer look at the talks shows this

immediately. On the other hand, some rather new items were discussed, for example, user needs in the session on "User Considerations". The same is true for "Protocol Considerations"as becomes clear from the subject of these talks.

Alternative Cryptographic Approaches I and II concerned matters never before pointed out in such clarity as at Monte Verità. Totally unusual for similar meetings was the publicly presented lecture on "Cryptography for the Layman". The topics of the two impromptu sessions also have not been discussed very often. Lastly, the view of Hansjürg Mey on future development of cryptography in the seminar closing and the retrospective by Jim Massey and him were rather surprising.

Naturally such intensive engagement by the participants requires also time for relaxing. This could be found to a certain degree during the daily buffet lunch at the hotel terrace in bright sunshine as well as during dinner in the evening. But – unavoidable for specialists – more often discussion continued instead of relaxing. Therefore an excursion was planned for Wednesday afternoon. Transported by bus the whole party changed from Lago Maggiore to Lago di Lugano (Lake Lugano) to view the famous private art collection at the Villa Favorita owned by Thyssen-Bornemisza in the small village, Castagniola, near Lugano. After that cultural event, the cryptographers' tourist party enjoyed a boat trip across Lake Lugano to the Grotto Theresa where rural food and wine could be tried, served on stone tables in the garden at the lakeside. Crossing the lake again to the famous promenade in Lugano, this very nice and interesting excursion ended with a bus trip back to Monte Verità. Last but not least worthy to note is Jim Massey's wife, Lis, who took care of the accompanying wives of some attendees and served as a guide for them.

Closing up this report it can be said that the experiment of doing a seminar on "Future Directions in Cryptography" at Monte Verità was a full success, quite opposite to the experiment that the founders of Monte Verità started nearly nine decades ago. It may be that the Spirit of Monte Verità has helped in this success and it is hoped that there will again be another Monte Verità Seminar on Cryptography before too long.

Otto J. Horak, Austria

Table 1: "Program as Actually Presented"

FUTURE DIRECTIONS IN CRYPTOGRAPHY

15-21 October 1989

Monday, 16 October

OPENING REMARKS AND ORIENTATION, Chairman: J.L. Massey

J.L. Massey and H. Mey: Opening remarks

J. Feigenbaum (45 min.): Report on recent DIMACS workshop on "Distributed Computing and Cryptography"

DESIGN OF SECRET-KEY CIPHERS I, Chairman: J.L. Massey

F. Pichler: VLSI testability versus crypto-security

J.D. Golić: On information-theoretic secrecy criteria for cipher systems

DESIGN OF SECRET-KEY CIPHERS II, Chairman: W. Diffie

S. Mund: Using pseudorandom generators in block ciphers

O. Staffelbach: Design criteria for cryptographic functions

I. Schaumüller: How new technology can influence cryptography

A.P. Borsalino: Statistical analysis of the avalanche effect in hash functions

IMPROMPTU SESSION, Chairman: J.L. Massey

Discussion: The relation between the information-theoretic and complexity-theoretic approaches to cryptography

Tuesday, 17 October

STREAM CIPHERS I, Chairman: O. Horak

R.A. Rueppel (45 min.): On the foundations of stream-cipher design

H. Niederreiter: Linear complexity profiles of random sequences

T. Schaub: The multi-window problem

STREAM CIPHERS II, Chairman: R. Rueppel

P. Nyffeler: Random and pseudorandom sequences

C.J.A. Jansen: New methods to generate keystream sequences

AUTHENTICATION I, Chairman: R. Rueppel

G.J. Simmons (45 min.): Status report on unconditionally secure authentication

SPECIAL LECTURE FOR THE PUBLIC IN CANTON TICINO, Chairman: K. Osterwalder

A. Sgarro: Crittografia per il profano

Wednesday, 18 October

AUTHENTICATION II, Chairman: G.J. Simmons

A. Sgarro: Lower bounds for authetication codes with and without splitting

R. Johanneson (15 min.): Can Simmons' lower bound on impersonation be strengthened?

G.J. Simmons and B. Smeets: How good is the lower bound on deception in multiple authentication?

Y. Desmedt: Subliminal-free authentication in an international environment

EXCURSION (Afternoon, optional) to view the famous art collection at the Villa Favorita near Lugano and take a boat trip from there across Lake Lugano to Grotto Theresa and from there to the Promenade in Lugano.

Thursday, 19 October

USER CONSIDERATIONS, Chairman: T. Berson

J. Vandewalle: Impact of VLSI and network security needs on cryptography

N. Thoery: Application aspects of public-key systems in public teleservices

G.J. Simmons: Information integrity

T. Matsumoto: Development of an IC card for the realization of key distribution

J. Pastor-Franco (15 min.): The 'Smart Post' system

PROTOCOL CONSIDERATIONS, Chairman: I. Ingermarsson

D. Chaum (45 min.): Random comments on results

T.A. Berson: Formal security analysis of cryptographic protocols

Y. Desmedt: Practical applications of zero-knowledge

IMPROMPTU SESSION, Chairman: D. Chaum

Discussion: The development of a "European Encryption Standard"

Friday, 20 October

PUBLIC-KEY CRYPTOGRAPHY, Chairman: D. Chaum

W. Diffie (45 min.): Future directions in cryptography

G. Chassé: The discrete logarithm problem and algebraic curves

D. Gollman: Implementing public-key algorithms

ALTERNATIVE CRYPTOGRAPHIC APPROACHES I, Chairman: R. Johannesson

T. Beth (45 min.): Cryptologic systems theory – a more feasible approach?

I. Ingemarsson (45 min.): Some connections between information theory and cryptology

IMPROMPTU SESSION (CONTINUATION), Chairman: D. Chaum

Discussion: The development of a "European Encryption Standard"

Saturday, 21 October

ALTERNATIVE CRYPTOGRAPHIC APPROACHES II, Chairman: H. Mey

W. Müller: On the possibilities and limits of the use of commutative polynomial functions in modern cryptography

G. Cohen and A. Lobstein: Links between coding theory and cryptography

U. Maurer: A provably-secure randomised cipher

E. Leitner (15 min.): Computational security of secret-key cipher algorithms

SEMINAR CLOSING AND RETROSPECTIVE

J.L. Massey and H. Mey

$25,000 (U.S.)
Call For Attack on REDOC II

###

Cryptech, Inc. will award the following:

* **$5,000** for the **best theoretical attack** performed on **one round** (the first of ten) of the REDOC II cryptosystem.

* **$20,000** to the **first attacker** to obtain at least 85 percent of the plaintext corresponding to a challenge set of ciphertext generated after **two rounds** (the first two of ten) of REDOC II encryption. (A large set of corresponding two round plaintext and ciphertext will also be provided.)

REDOC II

REDOC II is a high-speed Shannon confusion/diffusion/arithmetic/cryptosystem capable of enciphering 800 kilobits per second on a 20MHz clock. The current implementation involves a 10-round procedure performed on a 10-byte (80 bit) data block. A 140 bit key is also used.

GENERAL GUIDELINES

Below is a partial list of the guidelines concerning the call for attack. A complete list of rules, regulations, and guidelines will be provided with the participant packet.

TIME LIMIT: The call for attack will run from July 1, 1990 to January 1, 1992. On July 1, the participant packets will be mailed to all registrants. Registration forms will be accepted until March 1, 1991. All theoretical one round attacks and two round attacks must be received by Cryptech no later than January 1, 1992 to be eligible for the reward.

REGISTRATION: A $5 (U.S.) registration fee is required to become a valid, registered participant. The rewards will be given to registered participants only.

In order to register, participants should send the registration fee and a legible mailing address to:

NOTICE: IACR is not a sponsor of this contest and accepts no liability for the promised awards. This Call for Attack is published here simply as a service to IACR members.

Cryptech, Inc.
508 Lafayette Street
Jamestown, NY 14701
USA

PREFACE

This book is the proceedings of AUSCRYPT '90, the first conference sponsored by the International Association for Cryptological Research to be held in the southern hemisphere and the first outside the EUROCRYPT series held in European countries each northern spring and the CRYPTO series held in Santa Barbara, USA each August.

The proceedings from these earlier conferences have been published in the Springer-Verlag, Lecture Notes in Computer Science series, since 1986.

Papers in this volume are organized into eleven sections. The first ten sections comprise all of the papers on the regular program, including a few papers on the program which, unfortunately, were not presented at the meeting. The last section contains some of the papers presented at the "Rump Session" organized by Josef Pieprzyk.

AUSCRYPT '90 was attended by 95 people representing sixteen countries.

For the first time a skills workshop was held the day before the conference, with such eminent cryptographers as D. Gollmann (West Germany), I. Ingemarsson (Sweden), K. Ohta (Japan), R. Rueppel (Switzerland) and S. Vanstone (Canada) teaching in the area of their expertise. J. Seberry represented Australia at this event. Forty-one people attended the workshop.

It gives us great pleasure to express our thanks here to the members of the program committee: Dr R. Rueppel, Dr W.Price, and Dr I. Ingemarsson from Europe; Dr S. Vanstone, Dr R. Mullin, and Dr G. Agnew from North America; and Dr R. Safavi-Naini, and the other members of the Centre for Computer Security Research, for the rest of the world. They were all efficient, pleasant and wonderful co-workers.

Local organization was arranged by Ms C. Burke of the IPACE Institute, on the Sydney campus of The University of NSW. The conference dinner was held on a ferry on Sydney Harbour and was a spectacular success.

Many thanks to all the members of the Centre for Computer Security Research: Dr R. Safavi-Naini; Mr L. Brown; Ms L. Condie; Mr T. Hardjono; Mrs C. Newberry; Mr M. Newberry; Mr D. Rubie; Mrs E. Trott and Mrs E. Tait, all of whom readily worked at every task they were given to make the conference function smoothly and ensure its scientific success.

This conference was made possible by the support of the International Association for Cryptologic Research, The Centre for Computer Security Research, Prentice Hall Pty Ltd, and Telecom Australia.

Jennifer Seberry
Josef Pieprzyk

EUROCRYPT 90 - ABSTRACTS

May 21-24, 1990
Scanticon, Århus, Denmark.

Sponsored by The International Association for Cryptologic Research (IACR)
and
Cryptomathic AS, Dataco AS, Den Danske Bank AS, Jutland Telephone Company

General Chairman: Peter Landrock (Aarhus University)
Organizing Committee:
Jørgen Brandt (Aarhus University)
Palle Brandt Jensen (Jutland Telephone Company)
Torben Pedersen (Aarhus University)
Århus Congress Bureau

Program Chairman: Ivan Damgård (Aarhus University)
Program Comittee:
Ueli Maurer (ETH, Zürich)
Andrew J. Clark (Computer Security Ltd., Brighton)
Claude Crépeau (LRI, Paris)
Thomas Siegenthaler (AWK, Zürich)
Joan Boyar (Aarhus University)
Stig Frode Mjølsnes (ELAB, Trondheim)
Marc Girault (SEPT, Caen)
Walter Fumy (Siemens AG, Erlangen)
Othmar Staffelbach (Gretag, Regensdorf)

EuroCrypt 90 Program

MONDAY, May 21, 1990

10:00 Registration opens
13:00 - 14:00 Lunch
14:00 - 14:10 Welcome to EuroCrypt 90

Session 1: Protocols
Chair: David Chaum

14:10 - 14:40 *All Languages in NP have divertible zero-knowledge proofs and arguments under cryptographic assumptions*, M.V.D. Burmester (University of London) and Y. G. Desmedt (University of Wisconsin, Milwaukee).....1

14:40 - 15:00 *On the importance of memory resources in the security of key exchangeprotocols*, G. Davida, Y. Desmedt and R. Peralta (University of Wisconsin, Milwaukee).....11

15:00 - 15:20 *Provably secure key-updating schemes in identity-based systems*, S.Shinozaki, T.Itoh, A.Fujioka and S.Tsujii (Tokyo Institute of Technology).....19

15:20 - 15:40 *Oblivious transfer protecting secrecy*, Bert den Boer (Philips Crypto B.V.).....37

15:40 - 16:00 **Coffee Break**

16:00 - 16:30 *Public-randomness in public-key crypto-systems*, A. De Santis (IBM Yorktown) and G. Persiano (Harvard University).....45

16:30 - 17:00 *An interactive identification scheme based on discrete logarithms and factoring*, E.F. Brickell and K.S. McCurley (Sandia National Laboratories).....59

18:00 **Reception at City Hall, Århus.**

TUESDAY, May 22, 1990

Session 2: Number-Theoretic Algorithms
Chair: Kevin S. McCurley

9:00 - 9:30 *Factoring with two large primes*, A.K. Lenstra (Bell Com.Research) and M.S. Manasse (Dig. Equip. Corp.).....69

9:30 - 10:00 *Which RSA signatures can be computed from some given RSA signatures?*, J.H. Evertse (University of Leiden) and E. van Heyst (CWI, Amsterdam).....81

10:00 - 10:30 *Implementation of a key exchange protocol using real quadratic fields*, J.A. Buchman (Universität des Saarlandes), H.C. Williams and R. Scheidler (University of Manitoba).....101

10:30 - 11:00 **Coffee Break**

11:00 - 11:20 *Distributed primality proving and the primality of* $(2^{3539}+1)/3$, F. Morain (INRIA, Le Chesnay).....113

Session 3: Boolean Functions
Chair: Walter Fumy

11:20 - 11:40 *Properties of binary functions*, S. Lloyd (H.P. Laboratories, Bristol).....125

11:40 - 12:00 *How to construct pseudorandom permutations from single pseudorandom Functions*, J. Pieprzyk (Univ. of New South Wales).....137

12:00 - 12:30 *Construction of bent functions and difference sets*, K. Nyberg (Univ. of Helsinki).....147

12:30 - 14:00 **Lunch**

14:00 - 14:30 *Propagation characteristics of boolean functions*, B. Preneel, W. Van Leekwijk, L. Van Linden, R. Govaerts and J. Vandewalle (K.U. Leuven).....155

EuroCrypt 90 Program

WEDNESDAY, May 23, 1990

Session 4: Binary Sequences

Chair: James Massey

14:30 - 14:50 *The linear complexity profile and the jump complexity of keystream sequences*, H. Niederreiter (Austrian Academy of Sciences).....169

14:50 - 15:10 *Lower bounds for the linear complexity of sequences over residue rings*, Z. Dai (University of Linköping) and D. Gollmann (University of Karlsruhe).....175

15:10 - 15:30 *On the construction of run permuted sequences*, C.J.A. Jansen (Philips Crypto B.V.).....181

15:30 - 16:00 **Coffee Break**

16:00 - 16:30 *Correlation properties of combiners with memory in stream ciphers*, W. Meier (HTL Brugg-Windisch) and O. Staffelbach (Gretag).....189

16:30 - 17:00 *Correlation functions of geometric sequences*, A.H. Chan, M. Goresky and A. Klapper (Northeastern University).....197

18:00 - 20:00 **Reception at Jutland Telephone company.**

21:00 **Rump Session at Scanticon.**
Chair: John Gordon

8:45 - 9:00 **IACR Business Meeting**

Session 5: Implementations

Chair: Andy Clark

9:00 - 9:20 *Exponentiating faster with addition chains*, Y. Yacobi (Bellcore).....205

9:20 - 9:40 *A cryptographic library for the motorola DSP 56000*, S.R. Dusse and B.S. Kaliski Jr. (RSA Data Security Inc.).....213

9:40 - 10:00 *VICTOR - an efficient RSA hardware implementation*, H. Orup, E. Svendsen and E. Andreasen (Aarhus University).....219

10:00 - 10:30 *Experimental quantum cryptography*, C.H. Bennett (IBM T.J. Watson Research Center) F. Bessette, G. Brassard, L. Savail (Université de Montréal) and J. Smolin (UCLA).....229

10:30 - 11:00 **Coffee Break**

Session 6: Combinatorical Schemes

Chair: Ernest F. Brickell

11:00 - 11:30 *A protocol to set up shared secret schemes without the assistance of a mutually trusted party*, I. Ingemarsson (Linköping University) and G. Simmons (Sandia Nat. Labs.).....245

11.30 - 11:50 *Lower bounds for authentication codes with spliting*, A. Sgarro (Univ. di Udine).....255

11:50 - 12:10 *Essentially l-fold secure authetication systems*, A. Beutelspacher (Univ. Gießen) and U. Rosenbaum (Siemens A.G.).....261

12:10 - 12:30 *On the construction of authentication codes with secrecy and codes which stand spoofing attacks of order L≥2*, B. Smeets, P. Vanrose and Z. Wan (Univ. of Lund).....271

12:30 - 14:00 **Lunch**

EuroCrypt 90 Program

THURSDAY, May 24, 1990

Session 7: Cryptanalysis

Chair: Marc Girault

14:00 - 14:30 *Cryptanalysis of a public-key cryptosystem based on approximation by rational numbers*, J. Stern (Université Paris) and P. Toffin (Univ. de Caen).....277

14:30 - 14:50 *A known-plaintext attack on two-key triple encryption*, P.C. van Oorschot and M.J. Wiener (BNR, Ottawa).....285

14:50 - 15:10 *Confirmation that some hash functions are not collision free*, S. Miyaguchi, K. Ohta and M. Iwata (NTT Labs).....293

15:10 - 15:30 *Inverting the pseudo exponentiation*, F. Bauspieß, H.J. Knobloch and P. Wichmann (Universität Karlsruhe).....309

15:30 - 15:50 **Coffee Break**

Session 8: New Cryptosystems

Chair: Gilles Brassard

15:50 - 16:10 *Cryptosystem for group oriented cryptography*, T. Hwang (Nat. Cheng Kung Univ.).....317

16:10 - 16:40 *A provably-secure strongly-randomized cipher*, U. Maurer (Swiss Inst. of Tech.).....325

16:40 - 17:00 *A general method to construct public key residue cryptosystems and mental poker protocols*, K. Kurosawa, Y. Katayama, W.Ogata and S. Tsujii (Tokyo Inst. of Technology).....335

17:00- 17:20 *A proposal for a new block encryption standard*, X. Lai and J. Massey (Swiss Inst. of Technology).....361

17:20 - 17:40 *A new trapdoor in knapsacks*, V. Niemi (University of Turku).....367

19:00 **Conference Banquet.**

Session 9: Signatures and Authentication

Chair: Joan Boyar

9:00 - 9:30 *On the design of provably secure cryptographic hash functions*, A. De Santis and M. Yung (IBM Yorktown).....377

9:30 - 9:50 *Fast signature generation with the Fiat-Shamir scheme*, H. Ong (Deutsche Bank AG) and C.P. Schnorr (Universität Frankfurt).....399

9:50 - 10:05 *A remark on a signature scheme where forgery can be proved*, G. Bleumer, B. Pfitzmann and M. Waidner (Universität Karlsruhe).....403

10:05 - 10:30 *Membership authentication for hierarchical multigroups using the extended Fiat-Shamir scheme*, K. Ohta, T. Okamoto and K.Koyama (NTT Laboratories).....409

10:30 - 11:00 **Coffee Break**

11:00 - 11:30 *Zero-knowledge undeniable signatures*, D. Chaum (CWI, Amsterdam).....419

11:30 - 11:50 *Precautions taken against various potential attacks in ISO/IEC DIS 9796*, L. Guillou (CCETT) and J.J. Quisquater (Philips Research).....427

11:50 - 12:00 **Closing Remarks**

12:00 - 13:00 **Lunch**

Program for Crypto '90

August 12, Sunday

SESSION 1: CRYPTANALYSIS

Chair: S. Vanstone

[8:30 – 9:20 am] : *Differential Cryptanalysis of DES-like Cryptosystems (invited talk)* - E. Biham, A. Shamir (Weizmann).

[9:25 am – 9:45 am] : *A Statistical Attack of the Feal-8 Cryptosystem* - H. Gilbert, G. Chasse (CNET).

[9:50 am – 10:10 am] : *An Improved Linear Syndrome Algorithm in Cryptanalysis with Applications* - K. Zeng (USTC), C. Yang (S.W. Louisiana), T. Rao (S.W. Louisiana).

MORNING COFFEE BREAK

SESSION 2: PROTOCOLS

Chair: Y. Desmedt

[10:30 am – 10:50 am] : *Quantum Bit Commitment and Coin Tossing Protocols* - G. Brassard (Montréal), C. Crépeau (Paris).

[10:55 am – 11:15 am] : *Security with Low Communication Overhead* - D. Beaver (Harvard), J. Feigenbaum (AT&T), J. Kilian (MIT), P. Rogaway (MIT).

[11:20 am – 11:40 am] : *Fair Computation of General Functions in Presence of Immoral Majority* - S. Goldwasser (MIT), L. Levin (Boston).

[11:45 am – 12:05 pm] : *One-way Group Actions* - G. Brassard (Montréal), M. Yung (IBM).

LUNCH

SESSION 3: ALGEBRA AND NUMBER THEORY

Chair: H. Williams

[1:45 pm – 2:05 pm] : *Solving Large Sparse Linear Systems over Finite Fields* - B. LaMacchia (MIT), A. Odlyzko (AT&T).

[2:10 pm – 2:30 pm] : *On the Computation of Discrete Logarithms in Class Groups* - J. Buchmann, S. Dullmann (Saarlandes).

[2:35 pm – 2:55 pm] : *Matrix Extension of the RSA Algorithm* - C. Chuang, J. Dunham (SMU).

[3:00 pm – 3:20 pm] : *Constructing Elliptic Curve Cryptosystems in Characteristic 2* - N. Koblitz (Washington).

AFTERNOON COFFEE BREAK

SESSION 4: SIGNATURES AND AUTHENTICATION
Chair: D. Stinson

[3:45 pm – 4:05 pm] : *Identification Tokens - or: Solving the Chess Grandmaster Problem* - T. Beth (Karlsruhe), Y. Desmedt (Wisconsin).
[4:10 pm – 4:30 pm] : *Arbitrated Unconditionally Secure Authentication Can be Unconditionally Protected Against Arbiter's Attacks* - Y. Desmedt (Wisconsin), M. Yung (IBM).
[4:35 pm – 4:55 pm] : *Convertible Undeniable Signatures* - J. Boyar (Aarhus), D. Chaum (CWI), I. Damgard (Aarhus), T. Pedersen (Aarhus).
[5:00 pm – 5:20 pm] : *Unconditionally Secure Digital Signatures* - D. Chaum (CWI), S. Roijakkers (Eindhoven).

August 13, Monday

SESSION 5: SECRET SHARING
Chair: M. De Soete

[8:30 am – 9:20 am] : *An Introduction to Shared Secret and/or Shared Control Schemes and Their Application* - G. Simmons (Sandia).
[9:25 am – 9:45 am] : *Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes* - E. Brickell (Sandia), D. Stinson (Nebraska).
[9:50 am – 10:10 am] : *Collective Coin Tossing Without Assumptions Nor Broadcasting* - S. Micali, T. Rabin (MIT).

MORNING COFFEE BREAK

SESSION 6: KEY DISTRIBUTION
Chair: T. Berson

[10:30 am – 10:50 am] : *A Key Distribution "Paradox"* - Y. Yacobi (Bellcore).
[10:55 am – 11:15 pm] : *A Modular Approach to Key Distribution* - W. Fumy, M. Munzert (Siemens).

SESSION 7: HASH FUNCTIONS
Chair: R. Rueppel

[11:20 am – 11:40 am] : *Structural Properties of One-way Hash Functions* - Y. Zheng, T. Matsumoto, H. Imai (Yokohama).
[11:45 am – 12:00 pm] : *The MD4 Message Digest Algorithm* - R. Rivest (MIT, RSA Data Security).

August 14, Tuesday

[8:30 am – 9:20 am] : *Invited talk by Whitfield Diffie (BNR)*

SESSION 8: ZERO-KNOWLEDGE
Chair: A. Fiat

[9:25 am – 9:45 am] : *Achieving Zero-knowledge Robustly* - J. Kilian (MIT).
[9:50 am – 10:10 am] : *Hiding Instances in Zero-knowledge Proof Systems* - D. Beaver (Harvard), J. Feigenbaum (AT&T), V. Shoup (AT&T).

MORNING COFFEE BREAK

[10:30 am – 10:50 am] : *Multi Zero-knowledge Interactive Proof Systems* - K. Kurosawa, S. Tsujii (Tokyo Inst. of Tech.).
[10:55 am – 11:15 am] : *Publicly Verifiable Non-interactive Zero-knowledge Proofs* - D. Lapidot, A. Shamir (Weizmann).
[11:20 am – 11:40 am] : *Cryptographic Applications of the Non-interactive Metaproof and Many-prover Systems* - A. De Santis (Salerno), M. Yung (IBM).
[11:45 am – 12:05 am] : *Interactive Proofs with Provable Security Against Passive Adversaries* - J. Kilian (MIT).

LUNCH

SESSION 9: RANDOMNESS
Chair: R. Rivest

[1:45 pm – 2:05 pm] : *On the Universality of the Next Bit Test* - A. Schrift, A. Shamir (Weizmann).
[2:10 pm – 2:30 pm] : *A Universal Statistical Test for Random Bit Generators* - U. Maurer (Swiss Fed. Inst. of Tech.).
[2:35 pm – 2:55 pm] : *On the Impossibility of Private Key Cryptography with Weakly Random Keys* - J. McInnes (Toronto), B. Pinkas (Technion).

SESSION 10: APPLICATIONS
Chair: G. Agnew

[3:00 pm – 3:20 pm] : *How to Time-stamp a Digital Document* - S. Haber, W. Stornetta (Bellcore).

AFTERNOON COFFEE BREAK

[3:45 – 4:05 pm] : *How to Utilize the Randomness of Zero-knowledge Proofs* - T. Okamoto, K. Ohta (NTT).
[4:10 pm – 4:30 pm] : *Fast Software Encryption Functions* - R. Merkle (Xerox).
[4:35 pm – 4:55 pm] : *CORSAIR: A Smart Card for Public Key Cryptosystems* - D. de Waleffe, J. Quisquater (Philips).
[5:00 pm – 5:10 pm] : *On Developing Standard Key Generation Modules (SKGMs) for Low to High Bandwidth Secure Data Communications and Standard Key Management Modules (SKMMs)* - R. Winter (Winter Company).

[5:15 pm – 5:30 pm] : IACR Meeting.

August 15, Wednesday

SESSION 11: DESIGN AND ANALYSIS I
Chair: K. Koyama

[8:35 am – 8:55 am] : *Checkers for RSA / Efficient Checkers for Cryptography* - K. Kompella, L. Adleman (USC).
[9:00 am – 9:20] am : *Complexity Theoretic Issues Concerning Block Ciphers Related to DES* - R. Cleve (Intern. Comp. Sc. Inst.).
[9:25 am – 9:45 am] : *The REDOC-II Cryptosystem* - T. Cusick (SUNY at Buffalo), M. Wood (Cryptech Inc.).
[9:50 am – 10:10 am] : *A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion* - K. Kim, T. Matsumoto, H. Imai (Yokohama).

MORNING COFFEE BREAK
SESSION 12: DESIGN AND ANALYSIS II
Chair: J. Buchmann

[10:30 am – 10:50 am] : *A Comparison of Practical Public Key Cryptosystems Based on Integer Factorization and Discrete Logarithms* - P. van Oorschot (BNR).
[10:55 am – 11:15 am] : *On the Cryptographic Security of Single RSA Digits in a General Base* - B. Jin (Macquaire U).
[11:20 am – 11:40 am] : *Non-linear Parity Circuits and their Cryptographic Applications* - K. Koyama, R. Terada (NTT).
[11:45 am – 12:05 pm] : *Cryptographic Significance of the Carry for Ciphers Based on Integer Addition* - O. Staffelbach (Gretag), W, Meier (HTL).

CONFERENCE ANNOUNCEMENT

EUROCRYPT '91

8th - 11th April 1991
University of Sussex, Brighton, U.K.

A Workshop on the Theory and Applications of Cryptographic Techniques

Sponsored by: the International Association for Cryptologic Research (IACR)

The conference deals with all aspects of the theory and applications of cryptography. It is planned to start on Monday 8th April with lunch and end with lunch on Thursday 11th April. Advance check-in on the Sunday with overnight accomodation will be available.

The meeting will take place at the University of Sussex which is located on the outskirts of the attractive historical coastal resort town of Brighton, in the South Downs. Brighton is the largest town in the county of Sussex and the most popular seaside resort on the South-East coast.

The nearest airport to Brighton is London, Gatwick from which a coach service will be provided.

The many attractions of Brighton include the Royal Pavilion (the Prince Regent's Summer palace), the Lanes, rows of fishermens' cottages converted into antique shops, and numerous restaurants, bistros, pubs and wine bars.

The Organising Committee has already provisionally arranged a very full social programme which will enable delegates to savour the unique delights of Brighton and it's neighbour Hove.

Registration will be handled by the Organising Committee, and the deadline for registration is **22nd February 1991.**

For advance information, please contact the General Chair:

Andrew J Clark, General Chair Eurocrypt '91
c/o Computer Security Limited
Olivier House
18 Marine Parade
BRIGHTON
East Sussex
BN2 1TL
U.K.

Tel: +44-273-672191 (Switchboard)
+44-273-673642 (Booking Line 24hrs)
Fax: +44-273-673928
Tlx: 878195 OPEN G

FIRST CALL FOR PAPERS

EUROCRYPT '91

8th - 11th April 1991
University of Sussex, Brighton, U.K.

A Workshop on the Theory and Applications of Cryptographic Techniques

Sponsored by: the International Association for Cryptologic Research (IACR)

Original papers are solicited on all aspects of the theory and applications of cryptography including symmetric and asymmetric ciphers, authentication, protocols, secure transactions, signatures, sequences and linear complexity, hardware and software topics, security of telecommunications systems and computer networks.

Send 10 copies of an extended abstract of at most 10 double-spaced pages to the Programme Chair (address below).

The abstract should clearly indicate the results achieved, their significance and their relation to other work in the area.

To facilitate blind refereeing, authors are encouraged to supply a separate cover page indicating title and author, and start the next page with title and abstract of the paper.

The deadline for submissions to the conference will be 30th November 1990[1]

Submissions that deviate significantly from these guidelines risk rejection without consideration of their merits.

Proceeding from the conference will be published in Springer Verlag Lecture Notes in Computer Science. Authors of selected papers will be notified before the conference.

Programme Committee:

Donald Davies (Programme Chair)
"Fair Winds"
15 Hawkewood Road
SUNBURY-ON-THAMES
Middlesex
TW6 6HL
U.K.

Tel: (+44)-9327-83854

Thomas Beth, West Germany
Colin Boyd, U.K.
Norbert Cot, France
Viiveke Fåk, Sweden
John Gordon, U.K.
Siegfried Herda, West Germany
Arjen Lenstra, U.S.A.
Tsutomu Matsumoto, Japan
Fred Piper, U.K.
Claus Schnorr, West Germany

[1] In cases of doubt, the postmark date will be taken into account

ASIACRYPT '91

NOVEMBER 11-14, 1991

FUJIYOSHIDA, YAMANASHI, JAPAN

The ASIACRYPT '91 will be held at

The Hotel Highland Resort, Fujiyoshida, Yamanashi, Japan
in
November 11-14, 1991.

Original research papers and technical expository talks are solicited on all practical and theoretical aspects of cryptology. It is anticipated that some talks may also be presented by special invitation of the Program Committee.

For further information, please contact:

Professor Hideki Imai
Division of Electrical and Computer Engineering
YOKOHAMA NATIONAL UNIVERSITY
156 Tokiwadai, Hodogaya, Yokohama, 240 Japan
Phone: +81·45·335·1451×2903
Fax: +81·45·334·3215
E Mail: imai@imailab.dnj.ynu.ac.jp

or,

Professor Tsutomu Matsumoto
Division of Electrical and Computer Engineering
YOKOHAMA NATIONAL UNIVERSITY
Address and Fax are as above.
Phone: +81·45·335·1451×2898
E Mail: matsumoto@mlab.dnj.ynu.ac.jp

Notice Board

This space is new to the newsletter and is provided as a service to our membership. The editor's policy is to present information of interest to the membership of the IACR. Submissions are open to everyone. No paid advertising will be accepted and the editor reserves the right to reject any submissions.

Conference Calendar (bold face indicates IACR sponsored conferences)
CRYPTO'90 - Aug. 11-15, 1990. UC. Santa Barbara, Conference Chair - Sherry McMahan, Cylink, 110 South Wolfe Rd., Sunnyvale, California, USA, 94086.

28th Annual Allerton Conference on Communications, Control and Computing - Oct. 3-5, 1990, Urbana, Illinois, USA., - D. Brown, University of Illinois at Urbana-Champaign, 1101, West Springfield Ave., Urbana, Illinois, 61801.

COMPSEC 90 - Oct. 10-12, 1990. Westminster, London, U.K.

EUROCRYPT'91 - Apr. 8-11, 1991. Univ. of Sussex, Brighton, U.K., Conference Chair - Andy Clark, Computer Security Ltd., Oliver House, 18 Marine Parade, BRIGHTON, East Sussex, BN2 1TL, U.K.

ASIACRYPT'91 - Nov. 11-14, 1991. Japan, Chair - Prof. Tsujii

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

MOUNTAIN VIEW
JUL 9 '90
CALIF.

U.S POSTAGE
.45
METER
F9702002

DR THOMAS A BERSON EXP12/91
ANAGRAM LABORATORIES
PO BOX 791
PALO ALTO CA 94301
USA