Advances in Cryptology—CRYPTO '90

Proceedings
CRYPTO '90

A Conference on the Theory and Application of Cryptography

held at the University of California, Santa Barbara,
August 11-15, 1990
through the cooperation of the Computer Science Department

Sponsored by:

International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

General Chair
Sherry McMahan, Cylink

Program Chair
Scott Vanstone, University of Waterloo

Program Committee

Gordon Agnew University of Waterloo
Thomas Berson Anagram Laboratories
Johannes Buchmann Universität des Saarlandes
Yvo Desmedt University of Wisconsin
Amos Fiat Tel-Aviv University
Kenji Koyama NTT Basic Research Lab
Ronald Rivest Massachusetts Institute of Technology
Rainer Rueppel Crypto AG
Marijke De Soete Philips Research Labs
Doug Stinson University of Nebraska
Hugh Williams University of Manitoba
Foreword

Crypto '90 marked the tenth anniversary of the Crypto conferences held at the University of California at Santa Barbara. The conference was held from August 11 to August 15, 1990 and was sponsored by the International Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Department of Computer Science of the University of California at Santa Barbara.

Crypto '90 attracted 227 participants from twenty countries around the world. Roughly 35% of attendees were from academia, 45% from industry and 20% from government. The program was intended to provide a balance between the purely theoretical and the purely practical aspects of cryptography to meet the needs and diversified interests of these various groups.

The overall organization of the conference was superbly handled by the general chairperson Sherry McMahan. All of the outstanding features of Crypto, which we have come to expect over the years, were again present and, in addition to all of this, she did a magnificent job in the preparation of the book of abstracts. This is a crucial part of the program and we owe her a great deal of thanks.

Each year the number and quality of submissions to Crypto has been increasing. This is of course very good for the conference but it does make the task of the program committee more difficult. This year we had 104 papers and abstracts submitted from 18 countries. In anticipation of this larger number, the committee was expanded to twelve members representing seven countries. Having a bigger committee and a wider global representation poses certain problems with communication, but we believe these problems are minute in comparison to the benefits obtained from having each paper scrutinized by more people and by involving a much larger cross-section of the cryptographic community in this process. Each paper was assigned to three committee members who were then responsible for its refereeing. Of the 104 submissions, one was withdrawn, 43 were accepted for presentation and, of these 43, two were merged into one presentation. All papers and abstracts accepted for presentation which contained sufficient detail for the committee to make a reasonably accurate evaluation of the final form of the paper have not been been re-refereed. Rump session contributions and papers accepted for presentation based on abstracts with very little detail have been refereed.

As in other years, Whitfield Diffie kindly agreed to coordinate the Rump Session. We would like to take this opportunity to thank Whit for running this very important aspect of Crypto over the years and for graciously accepting to do it again. In an effort to contain the number of short talks given in this session, a much harder line was adopted this year. Of the 22 abstracts submitted only 12 were accepted for presentation. Of these 12, only 6 were submitted for the proceedings and all of these have gone through a thorough refereeing process.
For this conference there were three invited speakers and each was given fifty minutes to lecture. It was our goal to have topics of current interest, given by noted authorities in the area and presented in a manner which would make the lectures accessible to a large audience of diversified backgrounds. With this in mind we approached Whitfield Diffie (Bell Northern Research), Adi Shamir (Weizmann Institute) and Gus Simmons (Sandia National Laboratories) and all accepted. We thank them for their outstanding presentations and the enthusiasm which they conveyed for the subject.

We would also like to thank Dr. Tatsuaki Okamoto (NTT Tokyo) for the very valuable assistance he provided to us. Dr. Okamoto was on sabbatical leave from NTT and was spending this time (August 1989 – August 1990) at the University of Waterloo. He kindly volunteered his services and made many very important and significant contributions to our efforts with the program.

Finally, we thank the members of the program committee itself for the very fine job they did. Theirs is a task which takes a great deal of time and effort and which receives a disproportionate amount of gratitude. Without a complete commitment by all members, the task would be impossible. We thank each of them for a very thorough and conscientious effort and also for their very deep dedication in making Crypto '90 successful. Many thanks to Gordon Agnew, Thomas Berson, Johannes Buchmann, Yvo Desmedt, Amos Fiat, Kenji Koyama, Ronald Rivest, Rainer Rueppel, Marijke De Soete, Doug Stinson, and Hugh Williams.

Alfred J. Menezes and Scott A. Vanstone
University of Waterloo
December 1990
# Table of Contents

## Session 1: Cryptanalysis
Chair: S. Vanstone

Differential Cryptanalysis of DES-like Cryptosystems (invited talk) .......... 2
  *E. Biham, A. Shamir (Weizmann)*

A Statistical Attack of the Feal-8 Cryptosystem ............................... 22
  *H. Gilbert, G. Chassé (CNET)*

An Improved Linear Syndrome Algorithm in Cryptanalysis with Applications ......................................................... 34
  *K. Zeng (USTC), C.H. Yang (S.W. Louisiana),
   T.R.N. Rao (S.W. Louisiana)*

## Session 2: Protocols
Chair: Y. Desmedt

Quantum Bit Commitment and Coin Tossing Protocols .......................... 49
  *G. Brassard (Montréal), C. Crépeau (Paris)*

Security with Low Communication Overhead ..................................... 62
  *D. Beaver (AT&T), J. Feigenbaum (AT&T), J. Kilian (MIT),
   P. Rogaway (MIT)*

Fair Computation of General Functions in Presence of Immoral Majority 77
  *S. Goldwasser (MIT), L. Levin (Boston)*

One-Way Group Actions .............................................................. 94
  *G. Brassard (Montréal), M. Yung (IBM)*

## Session 3: Algebra and Number Theory
Chair: H. Williams

Solving Large Sparse Linear Systems over Finite Fields .................... 109
  *B.A. LaMacchia, A.M. Odlyzko (AT&T)*

On the Computation of Discrete Logarithms in Class Groups ............... 134
  *J. Buchmann, S. Dülmann (Saarland)*

Matrix Extensions of the RSA Algorithm ....................................... 140
  *C.C. Chuang, J.G. Dunham (SMU)*
Constructing Elliptic Curve Cryptosystems in Characteristic 2 ........... 156

N. Koblitz (Washington)

Session 4: Signatures and Authentication
Chair: D. Stinson

Identification Tokens – or: Solving the Chess Grandmaster Problem .. 169

T. Beth (Karlsruhe), Y. Desmedt (Wisconsin)

Arbitrated Unconditionally Secure Authentication Can Be
Unconditionally Protected against Arbiter’s Attacks .................... 177

Y. Desmedt (Wisconsin), M. Yung (IBM)

Convertible Undeniable Signatures ....................................... 189

J. Boyar (Aarhus), D. Chaum (CWI), I. Damgård (Aarhus),
T. Pedersen (Aarhus)

Unconditionally Secure Digital Signatures .............................. 206

D. Chaum (CWI), S. Roijakkers (Eindhoven)

Session 5: Secret Sharing
Chair: M. De Soete

Geometric Shared Secret and/or Shared Control Schemes (invited talk) 216

G.J. Simmons (Sandia)

Some Improved Bounds on the Information Rate of Perfect Secret
Sharing Schemes .................................................................... 242

E.F. Brickell (Sandia), D.R. Stinson (Nebraska)

Collective Coin Tossing Without Assumptions Nor Broadcasting ...... 253

S. Micali (MIT), T. Rabin (MIT)

Session 6: Key Distribution
Chair: T. Berson

A Key Distribution “Paradox” ............................................... 268

Y. Yacobi (Bellcore)

A Modular Approach to Key Distribution ................................. 274

W. Fumy, M. Munzert (Siemens)
Session 7: Hash Functions
Chair: R. Rueppel

Structural Properties of One-way Hash Functions .......................... 285
  Y. Zheng, T. Matsumoto, H. Imai (Yokohama)

The MD4 Message Digest Algorithm ........................................... 303
  R.L. Rivest (MIT)

Session 8: Zero-Knowledge
Chair: A. Fiat

Achieving Zero-Knowledge Robustly ........................................... 313
  J. Kilian (MIT)

Hiding Instances in Zero-Knowledge Proof Systems ...................... 326
  D. Beaver (AT&T), J. Feigenbaum (AT&T), V. Shoup (Toronto)

Multi-Language Zero-Knowledge Interactive Proof Systems .............. 339
  K. Kurosawa, S. Tsujii (Tokyo Inst. of Tech.)

Publicly Verifiable Non-Interactive Zero-Knowledge Proofs ............ 353
  D. Lapidot, A. Shamir (Weizmann)

Cryptographic Applications of the Non-Interactive Metaproof and
Many-Prover Systems .......................................................... 366
  A. De Santis (Salerno), M. Yung (IBM)

Interactive Proofs with Provable Security Against Honest Verifiers ... 378
  J. Kilian (MIT)

Session 9: Randomness
Chair: R. Rivest

On the Universality of the Next Bit Test .................................. 394
  A.W. Schrift, A. Shamir (Weizmann)

A Universal Statistical Test for Random Bit Generators ............... 409
  U.M. Maurer (Swiss Fed. Inst. of Tech.)

On the Impossibility of Private Key Cryptography with Weakly
Random Keys ................................................................. 421
  J.L. McInnes (Toronto), B. Pinkas (Techion)
Session 10: Applications
Chair: G. Agnew

How to Time-Stamp a Digital Document ........................................... 437
   S. Haber, W.S. Stornetta (Bellcore)

How to Utilize the Randomness of Zero-Knowledge Proofs ....................... 456
   T. Okamoto, K. Ohta (NTT)

Fast Software Encryption Functions ..................................................... 476
   R.C. Merkle (Xerox)

CORSAIR: A Smart Card for Public Key Cryptosystems .............................. 502
   D. de Waleffe, J.J. Quisquater (Philips)

Session 11: Design and Analysis I
Chair: K. Koyama

Fast Checkers for Cryptography ......................................................... 515
   K. Kompella, L. Adleman (USC)

Complexity Theoretic Issues Concerning Block Ciphers Related
to D.E.S. ................................................................................................. 530
   R. Cleve (Calgary)

The REDOC II Cryptosystem ................................................................. 545
   T.W. Cusick (SUNY at Buffalo), M.C. Wood (Cryptech Inc.)

A Recursive Construction Method of S-boxes Satisfying Strict
Avalanche Criterion .................................................................................. 564
   K. Kim, T. Matsumoto, H. Imai (Yokohama)

Session 12: Design and Analysis II
Chair: J. Buchmann

A Comparison of Practical Public Key Cryptosystems Based on Integer
Factorization and Discrete Logarithms ..................................................... 576
   P.C. van Oorschot (BNR)

Nonlinear Parity Circuits and their Cryptographic Applications ............... 582
   K. Koyama, R. Terada (NTT)

Cryptographic Significance of the Carry for Ciphers Based on Integer
Addition ..................................................................................................... 601
   O. Staffelbach (GRETAG), W. Meier (HTL)
Rump Session: Impromptu Talks
Chair: W. Diffie

Computation of Discrete Logarithms in Prime Fields ................. 616
  B.A. LaMacchia, A.M. Odlyzko (AT&T)

Systolic Modular Multiplication ........................................... 619
  S. Even (Bellcore)

Finding Four Million Large Random Primes ............................. 625
  R.L. Rivest (MIT)

The FEAL Cipher Family .................................................... 627
  S. Miyaguchi (NTT)

Discrete-log With Compressible Exponents .............................. 639
  Y. Yacobi (Bellcore)

Author Index ............................................................... 644