Preface

Crypto 2000 is the Twentieth Annual Crypto conference. It is sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara.

The conference received 120 submissions, and the program committee selected 32 of these for presentation. Extended abstracts of revised versions of these papers are in these proceedings. The authors bear full responsibility for the contents of their papers.

The conference program includes two invited lectures. Don Coppersmith's presentation "The development of DES" records his involvement with one of the most important cryptographic developments ever, namely the Data Encryption Standard, and is particularly apt given the imminent selection of the Advanced Encryption Standard. Martin Abadi's presentation "Taming the Adversary" is about bridging the gap between useful but perhaps simplistic threat abstractions and rigorous adversarial models, or perhaps, even more generally, between viewpoints of the security and cryptography communities. An abstract corresponding to Martin's talk is included in these proceedings.

The conference program also includes its traditional "rump session" of short, informal or impromptu presentations, chaired this time by Stuart Haber. These presentations are not reflected in these proceedings.

An electronic submission process was available and recommended, but for the first time used a web interface rather than email. (Perhaps as a result, there were no hardcopy submissions.) The submission review process had three phases. In the first phase, program committee members compiled reports (assisted at their discretion by sub-referees of their choice, but without interaction with other program committee members) and entered them, via web forms, into web-review software running at UCSD. In the second phase, committee members used the software to browse each other's reports, discuss, and update their own reports. Lastly there was a program committee meeting to discuss the difficult cases.

I am extremely grateful to the program committee members for their enormous investment of time, effort and adrenaline in the difficult and delicate process of review and selection. (A list of program committee members and sub-referees they invoked can be found in succeeding pages of this volume.) I also thank the authors of submitted papers - in equal measure regardless of whether their papers were accepted or not - for their submissions. It is the work of this body of researchers that makes this conference possible.

I thank Rebecca Wright for hosting the program committee meeting at the AT&T building in New York City and managing the local arrangements, and Ran Canetti for organizing the post-PC-meeting dinner with his characteristic gastronomic and oenophilic flair.
The web-review software we used was written for Eurocrypt 2000 by Wim Moreau and Joris Claessens under the direction of Eurocrypt 2000 program chair Bart Preneel, and I thank them for allowing us to deploy their useful and colorful tool.

I am most grateful to Chanathip Namprempre (aka. Meaw) who provided systems, logistical and moral support for the entire Crypto 2000 process. She wrote the software for the web-based submissions, adapted and ran the web-review software at UCSD, and compiled the final abstracts into the proceedings you see here. She types faster than I speak.

I am grateful to Hugo Krawczyk for his insight and advice, provided over a long period of time with his usual combination of honesty and charm, and to him and other past program committee chairs, most notably Michael Wiener and Bart Preneel, for replies to the host of questions I posed during the process. In addition I received useful advice from many members of our community including Silvio Micali, Tal Rabin, Ron Rivest, Phil Rogaway and Adi Shamir. Finally thanks to Matt Franklin who as general chair was in charge of the local organization and finances, and, on the IACR side, to Christian Cachin, Kevin McCurley, and Paul Van Oorschot.

Chairing a Crypto program committee is a learning process. I have come to appreciate even more than before the quality and variety of work in our field, and I hope the papers in this volume contribute further to its development.

Mihir Bellare
Program Chair, Crypto 2000
San Diego, June 2000
CRYPTO 2000

August 20–24, 2000, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair
Matthew Franklin, Xerox Palo Alto Research Center, USA

Program Chair
Mihir Bellare, University of California, San Diego, USA

Program Committee
Alex Biryukov ......................... Weizmann Institute of Science, Israel
Dan Boneh .............................. Stanford University, USA
Christian Cachin ........................ IBM Research, Switzerland
Ran Canetti .............................. IBM Research, USA
Ronald Cramer .......................... ETH Zurich, Switzerland
Yair Frankel .............................. CertCo, USA
Shai Halevi .............................. IBM Research, USA
Arjen Lenstra ............................ Citibank, USA
Mitsuru Matsui ........................... Mitsubishi Electric Corporation, Japan
Paul Van Oorschot ........................ Entrust Technologies, Canada
Bart Preneel .............................. Katholieke Universiteit Leuven, Belgium
Phillip Rogaway .......................... University of California, Davis, USA
Victor Shoup ............................. IBM Zurich, Switzerland
Jessica Staddon ........................... Bell Labs Research, Palo Alto, USA
Jacques Stern ............................. Ecole Normale Supérieure, France
Doug Stinson .............................. University of Waterloo, Canada
Salil Vadhan .............................. Massachusetts Institute of Technology, USA
David Wagner ............................. University of California, Berkeley, USA
Rebecca Wright ............................ AT&T Laboratories Research, USA

Advisory members
Michael Wiener (Crypto 1999 program chair) ........................ Entrust Technologies, Canada
Joe Kilian (Crypto 2001 program chair) ........................... Intermemory, USA
Sub-Referees

Table of Contents

XTR and NTRU
The XTR public key system ............................................. 1
   Arjen K. Lenstra, Eric R. Verheul
A Chosen-Ciphertext Attack against NTRU ......................... 21
   Éliane Jaulmes, Antoine Joux

Privacy for databases
Privacy Preserving Data Mining .................................... 37
   Yehuda Lindell, Benny Pinkas
Reducing the Servers Computation in Private Information Retrieval: PIR
   with Preprocessing ............................................. 56
   Amos Beimel, Yuval Ishai, Tal Malkin

Secure distributed computation and applications
Parallel Reducibility for Information-Theoretically Secure Computation ... 75
   Yengeniy Dodis, Silvio Micali
Optimistic Fair Secure Computation ................................ 94
   Christian Cachin, Jan Camenisch
A Cryptographic Solution to a Game Theoretic Problem ............. 113
   Yengeniy Dodis, Shai Halevi, Tal Rabin

Algebraic cryptosystems
Differential Fault Attacks on Elliptic Curve Cryptosystems ........ 131
   Ingrid Biehl, Bernd Meyer, Volker Müller
Quantum Public-Key Cryptosystems .................................. 147
   Tatsuaki Okamoto, Keisuke Tanaka, Shigenori Uchiyama
New Public-key Cryptosystem Using Braid Groups .................. 166
   Ki Hyoun Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park

Message authentication
Key recovery and forgery attacks on the MacDES MAC algorithm .... 184
   Don Coppersmith, Lars R. Knudsen, Chris J. Mitchell
CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions 197
John Black, Phillip Rogaway

L-collision Attacks against Randomized MACs .......................... 216
Michael Semanko

Digital signatures
On the exact security of Full Domain Hash .......................... 229
Jean-Sébastien Coron

Timed Commitments .................................................. 237
Dan Boneh, Moti Yung

A Practical and Provably Secure Coalition-Resistant Group Signature Scheme 256
Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik

Provably Secure Partially Blind Signatures .......................... 272
Masayuki Abe and Tatsuaki Okamoto

Cryptanalysis
Weaknesses in the SL_{2}(\mathbb{F}_{2^n}) Hashing Scheme ............ 288
Rainer Steinwandt, Markus Grassl, Willi Geiselmann, Thomas Beth

Fast Correlation Attacks Through Reconstruction of Linear Polynomials 302
Thomas Johansson and Fredrik Jönsson

Traitor tracing and broadcast encryption
Sequential Traitor Tracing ........................................ 318
Reihaneh Safavi-Naini and Yejing Wang

Long-Lived Broadcast Encryption .................................. 335
Juan A. Garay, Jessica Staddon, Avishai Wool

Invited talk
Taming the Adversary ............................................... 354
Martin Abadi

Symmetric encryption
The Security of All-Or-Nothing Encryption: Protecting Against Exhaustive Key Search .......................... 360
Anand Desai

On the Round Security of Symmetric-Key Cryptographic Primitives 377
Zulfikar Ramzan, Leonid Reyzin
New Paradigms for Constructing Symmetric Encryption Schemes Secure
Against Chosen-Ciphertext Attack ........................................ 395
Anand Desai

To Commit or not to Commit

Efficient Non-Malleable Commitment Schemes ............................ 414
Marc Fischlin and Roger Fischlin

Improved Non-Committing Encryption Schemes based on a General Complex-
ity Assumption ..................................................................... 433
Ivan Damgård, Jesper Buus Nielsen

Protocols

A note on the round-complexity of Concurrent Zero-Knowledge ........ 452
Alon Rosen

An Improved Pseudo-Random Generator Based on Discrete Log ........ 470
Rosario Gennaro

Linking Classical and Quantum Key Agreement: Is There “Bound Infor-
mation”? .............................................................................. 483
Nicolas Gisin, Stefan Wolf

Stream ciphers and boolean functions

Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers . . . 502
Muxiang Zhang, Agnes Chan

Nonlinearity Bounds and Constructions of Resilient Boolean Functions . . 516
Palash Sarkar, Subhamoy Maitra

Almost Independent and Weakly Biased Arrays: Efficient Constructions
and Cryptologic Applications .................................................... 534
Jürgen Bierbrauer, Holger Schellwat

Author Index ........................................................................... 546