PREFACE

The Crypto '95 conference was 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, Santa Barbara. It took place at the University of California, Santa Barbara, from August 27-31, 1995. This was the fifteenth annual Crypto conference; all have been held at UCSB. For the second time, proceedings were available at the conference. The General Chair, Stafford Tavares, was responsible for local organization and registration.

The Program Committee considered 151 papers and selected 36 for presentation. There were also two invited talks. Robert Morris, Sr. gave a talk on "Ways of Losing Information," which included some non-cryptographic means of leaking secrets that are often overlooked by cryptographers. The second talk, "Cryptography - Myths and Realities," was given by Adi Shamir, this year's IACR Distinguished Lecturer. Shamir is the second person to receive this honor, the first having been Gus Simmons at Crypto '94.

These proceedings contain revised versions of the 36 contributed talks. Each paper was sent to at least three members of the program committee for comments. Revisions were not checked on their scientific aspects. Some authors will write final versions of their papers for publication in refereed journals. Of course, the authors bear full responsibility for the contents of their papers.

I am very grateful to the members of the Program Committee for their hard work and the difficult task of selecting one quarter of the submitted papers. Following recent traditions, the submissions were anonymous; and each program committee member could be the author of at most one accepted paper.

We thank the following referees and external experts for their help on various papers: Philippe Béguin, Mihir Bellare, Charles Bennett, Gilles Brassard, Florent Chabaud, Chris Charnes, Yair Frankel, Atsushi Fujioka, Thomas Hardjono, Philippe Hoogvorst, Nobuyuki Imoto, Toshiya Itoh, Sushil Jajodia, Lars Knudsen, Paul Kocher, Mitsuru Matsui, Tsutomu Matsumoto, David M'Raihi, Yi Mu, Rafail Ostrovsky, Eiji Okamoto, Tatsuaki Okamoto, David Pointcheval, Rei Safavi-Naini, Kouichi Sakurai, Jennifer Seberry, Hiroki Shizuya, Dan Simon, Othmar Staffelbach, Jacques Stern, Moti Yung and Xian-Mo Zhang. I apologize for any omissions.

I thank Baruch Schieber and Prabhakar Raghavan for help with software and LaTeX; Barbara White and Peg Cargiulo for secretarial help; and Yvo Desmedt, Jimmy Upton and Peter Landrock for advice on the mechanics.

Finally, thanks go to all who submitted papers for Crypto '95. The success of the conference depends on the quality of its submissions. I am also thankful for all the authors, who cooperated by delivering their final copy to me in a timely fashion for the proceedings.

Don Coppersmith
Program Chair, Crypto '95
IBM Research Division, Yorktown Heights, New York, USA
June, 1995

CRYPTO '95

University of California, Santa Barbara
August 27-31, 1995

Sponsored by the

International Association for Cryptologic Research

in cooperation with the

IEEE Computer Society Technical Committee
on Security and Privacy

and the

Computer Science Department,
University of California, Santa Barbara

General Chair

Stafford Tavares, Queen's University, Canada

Program Chair

Don Coppersmith, IBM T.J. Watson Research Center, USA

Program Committee

Ross Anderson	Cambridge University, UK
Ernest Brickell	Sandia National Laboratories, USA
Hugo Krawczyk	IBM T.J. Watson Research Center, USA
Susan Langford	Stanford University, USA
Kevin McCurley	Sandia National Laboratories, USA
Willi Meier	HTL Brugg-Windisch, Switzerland
Moni Naor	Weizmann Institute of Science, Israel
Andrew Odlyzko	AT&T Bell Laboratories, USA
Kazuo Ohta	NTT Laboratories, Japan
Josef Pieprzyk	University of Wollongong, Australia
Jean-Jacques Quisquater	UCL-MathRIZK, Belgium
Alan Sherman	Univ. of Maryland Baltimore County, USA
Scott Vanstone	University of Waterloo, Canada
Serge Vaudenay	Ecole Normale Supérieure, France