Preface

Crypto 2001, the 21st Annual Crypto 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 at Santa Barbara.

The conference received 156 submissions, of which the program committee selected 34 for presentation; one was later withdrawn. These proceedings contain the revised versions of the 33 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

The conference program included two invited lectures. Mark Sherwin spoke on experimental work on quantum computation. Daniel Weitzner spoke on legal and political aspects of cryptography and privacy. The conference program also included its perennial "rump session," chaired by Stuart Haber, featuring short, informal talks on late–breaking research news.

As I try to account for the hours of my life that flew off to oblivion, I realize that most of my time was spent cajoling talented innocents into spending even more time on my behalf. I have accumulated more debts than I can ever hope to repay. As mere statements of thanks are certainly insufficient, consider the rest of this preface my version of Chapter 11.

I would like to first thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto is just a pile of shrimp and chocolate covered strawberries.

I thank David Balenson, the general chair, for shielding me from innumerable logistical headaches, and showing great generosity in supporting my efforts.

Selecting from so many submissions is a daunting task. My deepest thanks go to the members of the program committee, for their knowledge, wisdom, and near-masochistic work ethic. We in turn have relied heavily on the expertise of the many outside reviewers who assisted us in our deliberations. My thanks to all those listed in the following pages, and my thanks and apologies to any I have missed.

I thank Rebecca Wright for hosting the program committee meeting in New York City, AT&T for providing the space, and Sandy Barbu for helping out with the local arrangements. Thanks also go to Ran Canetti, our native culinary guide, for organizing the post–deliberations dinner.

I thank the people who, by their past and continuing work, have greatly streamlined the submission and review process. All but one of the submissions were handled using Chanathip Namprempre's web-based submission software. Reviews were administered using software written by Wim Moreau and Joris Claessens, developed under the guidance of Bart Preneel. With these software packages, they have made the process idiot proof, and practically theorist-proof. My thanks also go to Sam Rebelsky for writing the email-based predecessor of the submission software. He and the other members of the SIGACT Electronic

Publications Board have for many years made program committee chairs' lives much more bearable.

I am grateful to Mihir Bellare, last year's program chair, and Kevin McCurley and Josh Benaloh, my main contacts with the IACR board, for patiently trying to teach me my job.

But, even if I can't really account for what I, personally, was doing, the hours did go somewhere. I thank my boss, Peter Yianilos, for being so supportive of my efforts, and so absurdly forgiving of the time it has taken away from my work. Last, and more importantly, I'd like to thank my family, Dina, Gersh and Pearl, for their support, understanding and love.

June, 2001

Joe Kilian
Program Chair
Crypto 2001