

Preface

Crypto 2004, the 24th 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 program committee accepted 33 papers for presentation at the conference. These were selected from a total of 211 submissions. Each paper received at least three independent reviews. The selection process included a Web-based discussion phase, and a one-day program committee meeting at New York University.

These proceedings include updated versions of the 33 accepted papers. The authors had a few weeks to revise them, aided by comments from the reviewers. However, the revisions were not subjected to any editorial review.

The conference program included two invited lectures. Victor Shoup's invited talk was a survey on chosen ciphertext security in public-key encryption. Susan Landau's invited talk was entitled "Security, Liberty, and Electronic Communications". Her extended abstract is included in these proceedings.

We continued the tradition of a Rump Session, chaired by Stuart Haber. Those presentations (always short, often serious) are not included here.

I would like to thank everyone who contributed to the success of this conference. First and foremost, the global cryptographic community submitted their scientific work for our consideration. The members of the Program Committee worked hard throughout, and did an excellent job. Many external reviewers contributed their time and expertise to aid our decision-making. James Hughes, the General Chair, was supportive in a number of ways. Dan Boneh and Victor Shoup gave valuable advice. Yevgeniy Dodis hosted the PC meeting at NYU.

It would have been hard to manage this task without the Web-based submission server (developed by Chanathip Namprempre, under the guidance of Mihir Bellare) and review server (developed by Wim Moreau and Joris Claessens, under the guidance of Bart Preneel). Terri Knight kept these servers running smoothly, and helped with the preparation of these proceedings.

June 2004

Matt Franklin