

Relating Cryptography and Cryptographic Protocols: A Panel

Andre Scedrov, Moderator
University of Pennsylvania
Department of Mathematics
Philadelphia, PA 19104–6395, USA
scedrov@cis.upenn.edu

1. Participants

- **Ran Canetti, IBM Yorktown**
- **Joshua Guttman, MITRE**
- **David Wagner, Univ. of California, Berkeley**
- **Michael Waidner, IBM Zurich**

2. Overview

Cryptographic protocol analysis, including foundational research as well as automated tools, is often based on a model of adversary capabilities that appears to have developed from positions taken by Needham and Schroeder [6] and a model presented by Dolev and Yao [3]. In this idealized setting, a protocol adversary is allowed to nondeterministically choose among possible actions. Messages are composed of indivisible abstract values, not sequences of bits, and encryption is modeled in an idealized way. Adversary may only send messages comprised of data it “knows” as the result of overhearing previous messages.

Basic assumptions of this model provide an idealized setting in which protocol analysis becomes relatively tractable. However, actual protocols use actual cryptosystems that may have their own weaknesses, or might employ probabilistic techniques not expressed in the idealized model. Recently there have been several research efforts to relate the idealized model to cryptographic techniques and the computational model based on probabilistic polynomial-time computation, including [1, 2, 4, 5, 7, 8]. The panel will include a discussion of these and related approaches, as well as a few practical examples that shed light on the sorts of failure modes that a successful theory of cryptographic protocol security might try to capture.

References

- [1] M. Abadi and P. Rogaway. Reconciling two views of cryptography (The computational soundness of formal encryption). In *IFIP International Conference on Theoretical Computer Science*, Sendai, Japan, 2000. Full paper to appear in *J. of Cryptology*.
- [2] R. Canetti. A unified framework for analyzing security of protocols. Cryptology ePrint Archive: Report 2000/067; see <http://eprint.iacr.org/2000/067/>, 2000.
- [3] D. Dolev and A. Yao. On the security of public-key protocols. In *Proc. 22nd Annual IEEE Symp. Foundations of Computer Science*, pages 350–357, 1981.
- [4] P. Lincoln, M. Mitchell, J. Mitchell, and A. Scedrov. A probabilistic poly-time framework for protocol analysis. In M. Reiter, editor, *Proc. 5-th ACM Conference on Computer and Communications Security*, pages 112–121, San Francisco, California, 1998. ACM Press.
- [5] J. Mitchell, A. Ramanathan, A. Scedrov, and V. Teague. A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols. Manuscript, 2001.
- [6] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.
- [7] B. Pfitzmann, M. Schunter, and M. Waidner. Cryptographic security of reactive systems. In S. Schneider and P. Ryan, editors, *Workshop on secure architectures and information flow*, Royal Holloway, University of London, December 1999, 2000. Electronic Notes in Theoretical Computer Science, vol. 32.
- [8] B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In *7-th ACM Conference on Computer and Communications Security, Athens, November 2000*, pages 245–254. ACM Press, 2000. Preliminary version: IBM Research Report RZ 3234 (# 93280) 06/12/00, IBM Research Division, Zürich, June 2000.