08491 Executive Summary Theoretical Foundations of Practical Information Security — Dagstuhl Seminar —

Ran Canetti[1], Shafi Goldwasser[2], Günter Müller[3], and Rainer Steinwandt[4]

[1] Tel-Aviv University, Tel-Aviv, Israel
canetti@tau.ac.il
[2] Massachusetts Institute of Technology, Cambridge, USA and
Weizmann Institute of Science, Rehovot, Israel
[3] University of Freiburg, Freiburg, Germany
mueller@iig.uni-freiburg.de
[4] Florida Atlantic University, Boca Raton, USA
rsteinwa@fau.edu

Introduction and Motivation

Designing, building, and operating secure information processing systems is a complex task, and the only scientific way to address the diverse challenges arising throughout the life-cycle of security criticial systems is to consolidate and increase the knowledge of the theoretical foundations of practical security problems. To this aim, the mutual exchange of ideas across individual security research communities can be extraordinary beneficial. Accordingly, the motivation of this Dagstuhl seminar was the integration of different research areas with the common goal of providing an integral theoretical basis that is needed for the design of secure information processing systems.

Coping with the full spectrum of challenges in information security is far beyond the scope of a single seminar, and thus participants were selected from a number of different, but still related, fields, so that a common scientific language or similarity of theoretical tools can facilitate an efficient exchange of ideas. Ideally, the seminar would help in identifying possibilities of cross-fertilization among seemingly different research directions within information security.

In addition to senior experts from academics, an effort was made to include participants with experience in industry, and also to include young researchers in the field who had already demonstrated a strong research potential.

Atmosphere, Organization, and Participation

It is fair to say that the seminar brought together some of the world experts on theoretical foundations of information security. The organizers are indebted for excellent presentations that were delivered by participants at this Dagstuhl

Dagstuhl Seminar Proceedings 08491
Theoretical Foundations of Practical Information Security
http://drops.dagstuhl.de/opus/volltexte/2009/1893

seminar. More than 30 participants from several countries came together, and the additional flexibility offered by a Dagstuhl seminar in comparison to traditional conferences turned out to be of invaluable help:

Talks of different lengths were scheduled, and lively technical discussions during talks where the norm. This resulted in various program changes and the scheduling of additional talks. The possibility to discuss results in technical depth when needed was of great benefit and together with the infrastructure offered by Schloss Dagstuhl resulted in an extremely fruitful reasearch atmosphere with rather long working hours. Feedback of seminar participants to the organizers was extremely positive, and it is no exaggeration to consider this Dagstuhl seminar as a world class research meeting.

Summary of Topics

Owing to the nature of the workshop, the topics presented covered quite different subjects of information security. Because of the significance of cryptographic techniques, it is not surprising that many talks made use the the technical machinery offered by research on theoretical foundations of cryptography. These talks were supplemented by presentations on several other aspects of information security and privacy.

Given the topic of the workshop, it is not surprising that presentations often focused on theoretical models and provable constructions. However, the techniques used in different presentations varied greatly, therewith giving seminar participants the possibility of experiencing techniques not typically encountered in their own line of research. This type of crossing the boundaries of individual subareas of research on the theoretical foundations of information security was hoped for in the organization of this seminar and greatly added to the diversity of the discussions.

Acknowledgment

The organizers are indebted to all participants for making this Dagstuhl seminar a great success. Moreover, it is our pleasure to thank the team of Schloss Dagstuhl for providing an excellent research environment for this seminar. Their efficient help and endless patience in dealing with requests and deviations from the time schedule is greatly appreciated.