07381 Executive Summary
Cryptography
— Dagstuhl Seminar —

J. Blömer[1], D. Boneh[2], R. Cramer[3] and U. Maurer[4]

[1] Univ. Paderborn, DE
[2] Stanford University, US
dabo@cs.stanford.edu
[3] CWI - Amsterdam, NL
cramer@cwi.nl
[4] ETH Zürich, CH
maurer@inf.ethz.ch

Keywords. Cryptography, information security, public-key cryptography, cryptographic protocols, security proofs.

1 Introduction and Motivation

Cryptography is of paramount importance for information security. Cryptographic primitives are the core building blocks for constructing secure systems. The last three decades have seen tremendous progress in cryptography and the field has substantially matured. Major achievements include the proposal of adequate security definitions, of new cryptographic schemes, and of security proofs for these schemes, relative to the security definition. As a consequence, cryptography has shifted from an ad-hoc discipline with many interesting tricks and ideas to a mathematically rigorous science. Despite this progress many essential problems in cryptography still remain open and new areas and topics arise constantly. The field is more lively than ever before.

While the number of scientific conferences focusing on cryptography is increasing, most of these meetings have a broad focus, and due to a growing interest by practitioners, the number of non-expert attendees has increased. As a result, it becomes more difficult to discuss the details of the advancement of the field, as well as to identify promising innovative trends. Therefore, the aim of the seminar was to provide an opportunity for key cryptographers to meet, to interact, to focus on the scientific foundation of cryptography, to spot the emerging new areas, and to work on them. Applications were also covered but the emphasis was on the conceptual framework that allows the use of appropriate models, amenable to mathematical reasoning.

2 Participation, Organization, and Atmosphere

The seminar brought together about 40 leading cryptographers from all over the world. Almost all participants gave a presentation about their recent research

and also about future research plans they have, encouraging others to join in. In many cases the choice of the subject for the talk was targeted to the unique list of participants. The presentations were highly interactive and led to lively discussions, well into the evenings and nights. A number of new collaborations were initiated at the seminar. Overall, the seminar was a great success, as is also documented by the feedback given by the participants on the questionnaires.

3 Summary of Topics

The topics covered in the seminar spanned most areas of cryptography, in one way or another, both in terms of the types of schemes (public-key cryptography, symmetric cryptography, hash functions and other cryptographic functions, multi-party protocols, etc.) and in terms of the mathematical methods and techniques used (algebra, number theory, elliptic curves, probability theory, information theory, combinatorics, quantum theory, etc.). The range of applications addressed in the various talks was broad, ranging from secure communication, key management, authentication, digital signatures and payment systems to e-voting and Internet security.

While the initial plan had been to focus more exclusively on public-key cryptography, it turned out that this sub-topic branches out into many other areas of cryptography and therefore the organizers decided to expand the scope, emphasizing quality rather than close adherence to public-key cryptography. This decision turned out to be a wise one.

What was common to almost all the talks is that rigorous mathematical proofs for the security of the presented schemes were given. In fact, a central topic of many of the talks were proof methodologies for various contexts.