Dagstuhl Seminar 09031
"Seminar on Symmetric Cryptography"
– Executive Summary –

Helena Handschuh[1], Stefan Lucks[2], Bart Preneel[3], Phil Rogaway[4]

[1]Spansion, France
[2]Bauhaus-University Weimar, Germany
[3]Katholieke Universiteit Leuven, Belgium
[4]University of California Davis, USA

Topics

Cryptography is the science that studies secure communication in adversarial environments. Symmetric Cryptography deals with two cases:

- either sender and receiver share the same secret key, as for encryption and message authentication;
- or neither sender nor receiver use any key at all, as, e.g., in the case of cryptographic hash functions.

Specifically, Symmetric Cryptography deals with symmetric primitives (block and stream ciphers, message authentication codes and hash functions), and complex cryptosystems and cryptographic protocols employing these primitives. Since symmetric cryptosystems are one to two orders of magnitude more efficient than asymmetric systems, most security applications use symmetric cryptography to ensure the privacy, the authenticity and the integrity of sensitive data. Even most applications of public-key cryptography are actually working in a *hybrid* way, separating an asymmetric protocol layer for key transmission or key agreement from secure payload transmission by symmetric techniques.

Presentations

The seminar brought together about 40 researchers from industry and academia, leading experts as well as exceptionally talented junior researchers. Most of the presentations did concentrate on one of the following three research directions:

1. studying the design and analysis of *stream ciphers*;

Dagstuhl Seminar Proceedings 09031
Symmetric Cryptography
http://drops.dagstuhl.de/opus/volltexte/2009/1959

2. presenting and attacking recent proposals for *cryptographic hash functions*; and
3. advancing the field of complex symmetric cryptosystems and protocols and their *provable security*.

The great interest in stream ciphers relates to the recently terminated eSTREAM project, under the umbrella of the European Network of Excellence ECRYPT. This initiative has brought remarkable advances in stream cipher design, a.o. by recommending a portfolio of 8 stream ciphers which are believed to be promising for further study. The cryptanalysis of hash functions has made a quantum leap in recent years. As a result, the National Institute of Standards and Technologies (NIST, USA) initiated a competition for a new hash function standard "SHA-3". The list of SHA-3 first-round candidates and their submission documents have been published about one month ahead of the Dagstuhl seminar. That was just enough time for the seminar participants to gain some first insights into strengths and weaknesses of some of the candidates. This constellation was ideal for the Dagstuhl seminar, as it lead to a fruitful exchange of ideas for cryptanalysing SHA-3 candidates, and to intense discussions about the relevance of several weaknesses. Provable security is based on the idea of formally specifying the security requirements a cryptosystem should satisfy, and formally proving that these security requirements are met if certain assumptions hold. In recent years, the research community in Symmetric Cryptography had shown a growing interest in provable security; in the SHA-3 competition, provable security plays an essential role to study the relation between the security of the building blocks and the hash function itself.

Discussion

In an *open discussion session*, many questions where raised, regarding the state of the art in Symmetric Cryptography in general, how the field has evolved in the past and how it will likely evolve in the future, how the community would like it to evolve, whether the research community actually concentrates on the right questions, and so on. One major issue, which raised substantial interest among the participants was the following:

> There is a broad range of abstract techniques to study the security of symmetric primitives, such as Differential Cryptanalysis, Linear Cryptanalysis, Algebraic Attacks and so on. But in many cases, a

researcher who is trying to apply these techniques needs tools (typically software), e.g., to compute the difference distribution table of a cipher, a round function or an S-box or to find the best linear or differential characteristic of an iterated cipher. It turns out however that each researcher or each group of researchers develops such tools on their own from scratch.

The general agreement was that the research community would benefit from establishing a culture of tool reuse, by encouraging researchers to share not only their ideas, but also the software they developed for the purpose of analyzing cryptosystems.

Summary

Research in Symmetric Cryptography is quickly evolving. The seminar was the second of its kind, the first one took place in 2007. We observe a steadily increasing interest in Symmetric Cryptography, as well as a growing practical demand for symmetric algorithms and protocols.

The seminar was very successful in discussing recent results and sharing new ideas. Furthermore, it inspired the participants to consider how Symmetric Cryptography has evolved in the past, and how they would like it to evolve in the future. The hospitality and support of the Dagstuhl team did contribute significantly to the success of the seminar.