Dagstuhl Seminar 07021
"Seminar on Symmetric Cryptography"
07.01.07 - 12.01.07

Executive Summary

Eli Biham[1], Helena Handschuh[2], Stefan Lucks[3], Vincent Rijmen[4]

[1]Technion, Haifa, Israel
[2]Spansion, France
[3]University of Mannheim, Germany**
[4]Graz University of Technology, Austria

Introduction and Motivation

Cryptography provides techniques for secure communication in adversarial environments. Cryptographic primitives are *symmetric*, if both the sender and the receiver of a message are using the same secret key, as in the case of block and stream ciphers and message authentication codes. Another type of symmetric primitives are cryptographic hash functions, where neither sender nor receiver need to know a secret key at all. In contrast to this, cryptographic primitives are asymmetric, if sender and receiver are using different keys, typically a "public" and a "private" one.

Symmetric Cryptography deals with designing and analysing

- symmetric primitives (block and stream ciphers, message authentication codes and hash functions), and
- cryptographic protocols employing these primitives.

Since symmetric cryptosystems are much more efficient in practice 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 by transmitting a cipher key with asymmetric techniques while symmetrically encrypting the payload data under the cipher key.

** on the leave to Bauhaus-University Weimar, Germany

Dagstuhl Seminar Proceedings 07021
Symmetric Cryptography
http://drops.dagstuhl.de/opus/volltexte/2007/1020

Participation and Program

The Seminar brought together about 35 researchers from industry and academia. Most of the participants came from different European countries, but quite a few also came from America and Asia. Almost all the participants gave a presentation. Most of them gave a "regular" talk of 30 to 50 minutes (including discussion time), some gave a "rump session" talk, and a few even gave two presentations, a regular one and another at the rump session.

The institution of a "rump session" for short talks on recent results, fresh ideas and open problems has a long tradition at cryptographic workshops and conferences. At the Seminar, the "rump session" was on Thursday evening. Each "rump session" talk was limited to at most ten minutes.

Topics and Focus Areas

The Seminar topics (stream ciphers, message authentication, hash functions, provable security, algebraic attacks, lightweight cryptography, ...) were various, but closely related and interleaved. All these topics received their share of interest, but two areas caught more attention than others:

1. The design and analysis of hash functions.
2. The security of stream ciphers against nonstandard "repeated initial value" attacks.[1]

The participant's interest in the first area is rather unsurprising. In 2004 and 2005, the cryptanalysis of *hash functions* has made a big leap forward. Attacks against hash functions in wide practical use, such as MD5 and SHA-1, have been published. There is an urgent need for new practical hash functions. Quite a few talks and many discussions dealt with advancing the theory and practice of hash function design, including the study of hash function attacks.

The excitement for the second area mirrors very recent research advances in research in Symmetric Cryptography. At the Seminar, further progress was made.

[1] Modern stream ciphers usually operate dependent on an "initial vlaue" (IV) or a "nonce". In contrast to the key, the IV is not secret, and may even be chosen by the adversary – but the requirement is to use a *different* IV for each new encryption. "Repeated IV" attacks assume the adversary to circumvent this requirement, thus widening the established thead model for stream ciphers.

Advances and Outlook

Most presentations at the seminar dealt with very recent results on Symmetric Cryptography – unpublished research which either had been submitted to one of the leading conferences in the area, or is designated to be submitted soon. Some participants also presented their research in progress, promising but not mature enough for publication. We anticipate that most of the presentations at the Seminar will ultimatively lead to peer-reviewed publications.

The atmosphere at the Seminar was very inspiring and stimulating. Participants reacted on other participants' open problems, and collaborations where initiated. Some progress made by our participants during the course of the Seminar and *already presented at the Seminar*:

- As a reaction on Greg Rose's presentation of a new stream cipher called "Shannon", *Alexander Maximov* presented some "repeated IV" attacks at the rump session.
- Following some discussions (during the days of the Seminar) with Alexander Maximov and others, *Greg Rose* confirmed the attack at the rump session and explained which design choices lead to the weakness.
- Inspired by Bart Preneel's talk on a "repeated IV" attack against the stream cipher "Phelix", *Doug Whiting* (one of the authors of Phelix), presented a tweak for Phelix at the rump session. The tweak defends against the weakness exploited by Preneel.
- After Elena Andreeva's talk on the RMC hash function design and its generalised security properties, it was observed that the HAIFA hash iteration mode can be instantiated with compression functions that satisfy the extra conditions required for RMC. If one does so, the RMC proof of security by Andreeva and her co-authors is applicable to the HAIFA mode as well, i.e., HAIFA satisfies the generalised RMC security properties. *Orr Dunkelman* (one of the authors of HAIFA) presented this observation at the rump session.
- In a quickly-scheduled regular talk on Friday morning, *Ralph-Philipp Weinmann* and *Ulrich Kühn* presented the idea of using algebraic attack techniques for a rather unusal kind of block cipher analysis: The adversary is allowed to control plaintexts *and keys*. The adversary's goal is to find out unknown parts of the block cipher specification (namely, a description of the secret S-box). This collaboration was initiated by a discussion at the Seminar.

Again, we anticipate that some – and perhaps all – these presentations will eventually lead to peer-reviewed publications.