Report from Dagstuhl Seminar 16021

Symmetric Cryptography

Edited by

Frederik Armknecht[1], Tetsu Iwata[2], Kaisa Nyberg[3], and Bart Preneel[4]

1 **Universität Mannheim, DE,** armknecht@uni-mannheim.de
2 **Nagoya University, JP,** iwata@cse.nagoya-u.ac.jp
3 **Aalto University, FI,** kaisa.nyberg@aalto.fi
4 **KU Leuven, BE,** bart.preneel@esat.kuleuven.be

Abstract

From January 10–15, 2016, the seminar 16021 in Symmetric Cryptography was held in Schloss Dagstuhl – Leibniz Center for Informatics. It was the fifth in the series of the Dagstuhl seminars "Symmetric Cryptography" held in 2007, 2009, 2012, and 2014.

During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations were given during the seminar. The first section describes the seminar topics and goals in general.

Seminar January 10–15, 2016 – http://www.dagstuhl.de/16021
1998 ACM Subject Classification E.3 Data Encryption, H.2.0 General – Security, Integrity, and Protection, K.6.5 Security and Protection
Keywords and phrases authenticity, block ciphers, confidentiality, cryptanalysis, hash functions, integrity, lightweight cryptography, provable security, stream ciphers
Digital Object Identifier 10.4230/DagRep.6.1.34

1 Executive Summary

Frederik Armknecht
Tetsu Iwata
Kaisa Nyberg
Bart Preneel

One lesson learned from the Snowden leaks is that digital systems can never be fully trusted and hence the security awareness of citizens has increased substantially. Whenever digital data is communicated or stored, it is subject to various attacks. One of the few working countermeasures are the use of cryptography. As Edward Snowden puts it: "*Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.*".[1]

Consequently it holds that although modern cryptography addresses a variety of security challenges, efficiently protecting the enormous amount of daily electronic communication represents a major challenge. Here, symmetric cryptography is especially highly relevant not only for academia, but also for industrial research and applications.

[1] See http://techcrunch.com/2013/06/17/encrypting-your-email-works-says-nsa-whistleblower-edward-snowden/.

Although symmetric cryptography has made enormous progress in the last couple of decades, for several reasons regularly new insights and challenges are evolving. In the past, the AES competition was led by US NIST to standardize a next generation block cipher to replace DES. Similar competitions, such as the eSTREAM and the SHA-3 competition, resulted in new standard algorithms that meet public demands. The outcome of the projects are practically used in our daily lives, and the fundamental understanding of the cryptographic research community of these primitives has been increased significantly.

While this seminar concentrates in general on the design and analysis of symmetric cryptographic primitives, special focus has been put on the following two topics that we explain in more detail below:

1. Authenticated encryption
2. Even-Mansour designs

Authenticated Encryption. Today the central research question is the construction of schemes for *authenticated* encryption. This symmetric primitive efficiently integrates the protection of secrecy and integrity in a single construction. The first wave of solutions resulted in several widely used standards, including CCM and GCM standardized by NIST, and the EAX-prime standardized by ANSI. However, it turns out that these constructions are far from optimum in terms of performance, security, usability, and functionality. For instance a stream of data cannot be protected with CCM, as the length of the entire input has to be known in advance. The security of GCM heavily relies on the existence of data called a nonce, which is supposed to never be repeated. Indeed, the security of GCM is completely lost once the nonce is repeated. While it is easy to state such a mathematical assumption, experience shows that there are many practical cases where realizing this condition is very hard. For instance the nonce may repeat if a crypto device is reset with malice aforethought, or as a consequence of physical attacks on the device. Furthermore, weak keys were identified in GCM, and the security of EAX-prime is questionable.

Thus there is a strong demand for secure and efficient authenticating encryption scheme. As a consequence, the CAESAR project (Competition for Authenticated Encryption: Security, Applicability, and Robustness) has been initiated.[2] The goal of the project is to identify a portfolio of authenticated encryption schemes that (1) offer advantages over GCM/CCM and (2) are suitable for widespread adoption. The deadline of the submission was March 15, 2014, and the project attracted a total of 56 algorithms from 136 designers from all over the world. There are plenty of innovative designs with attractive features, and the final portfolio is planned to be announced at the end of 2017.

This seminar took place in the middle of the CAESAR competition; it is two years from the submission deadline and we have about two years until the announcement of the final portfolio. Therefore, it was a perfect point in time to sum up the research done so far, to exchange ideas and to discuss future directions.

Even-Mansour Designs. Another strong trend in the current symmetric key cryptography is related to the so-called *Even-Mansour designs*. This design paradigm was proposed in 1991 and can be seen as the abstraction of the framework adopted in the design of AES. This general design framework iterates r times the xor of a key and a public permutation. The design framework is highly relevant in practice, and it has been adopted in a variety of recent hash functions, block ciphers, and even in the underlying primitive of several CAESAR submissions. Despite its long history of practical use, the community has so far failed to

[2] See http://competitions.cr.yp.to/caesar.html for details.

develop a complete understanding of its security. From a theoretical viewpoint, the original proposal was accompanied with a proof of security, dealing with the case of $r = 1$ iteration.

Only 20 years after the initial proposal, in 2012, a bound was proven for the security of $r = 2$ iterations. In 2014, the question was solved to cover the general case of r iterations. However, these results only deal with the simple case of distinguishing attack on a single, unknown key setting. Its security in more advanced, yet practically relevant security models, such as the related-key setting or the chosen/known-key setting, is largely unexplored.

Another problem here is that the theoretical analysis assumes that the permutation used therein is ideal and the keys are ideally random, which is not the case for practical constructions. This implies that the theoretical results do not directly translate into the practical constructions, and the security analysis has to be repeated for each constructions.

Summing up, Evan-Mansour designs represent a fruitful and challenging area of research, that hopefully will lead to a fundamental understanding of iterated constructions and ultimately to more efficient and more secure ciphers.

Seminar Program. The seminar program consists of the presentations about the above topics, and relevant areas of symmetric cryptography, including new cryptanalytic techniques and new designs. Furthermore, there were three discussion sessions. In "discussion on attacks," we discussed what constitutes a valid cryptographic attack in light of weak key classes, "discussion on secret agency crypto standards" was about cryptography developed by secret agencies, and there was a discussion session about the ongoing CAESAR project.