Lehrstuhl für Sicherheit
in der Informationstechnik

6. April 2017

BA, IP, FP:

Implementation of third-round CAESAR-Candiates

The currently ongoing “Competition for Authenticated Encryption: Security, Applicability, and Robustness” (CAESAR) is a competition to find a portfolio of next-generation authenticated ciphers. Competitions have a long tradition in the cryptographic community and have been used to select other cryptographic functions such as stream ciphers, the Secure Hash Algorithm 3 (SHA-3) and most important the Advanced Encryption Standard (AES). Public competitions became popular because mutual evaluation serves to focus the cryptographic community’s efforts and to stimulate research. In addition, backdoor theories are avoided, and the acceptance of standards is sped up.

Currently the remaining 15 CAESAR candidates are evaluate. There are four different classes of ciphers:

1. Block-cipher-based (AES-OTR, AEZ, JAMBU, COLM, OCB, CLOC and SILC, Deoxys)
2. Sponge-based (NORX, Ketje, Keyak, Ascon)
3. Stream-cipher-based (ACORN)
4. Dedicated ciphers (AEGIS, Tiaoxin, MORUS)

Your tasks are:

- Implementation of (different) third-round CAESAR-candidates.
- Evaluation of their performance.

As knowledge in cryptography is **not** required, the topic is very well suited for (integrated) system designers who want to get in touch with cryptography.

Requirements:

- Very good VHDL skills.
- Basic knowledge of FPGAs.

If you are interested, please send your application to:
Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Michael Tempelmeier
Arcisstraße 21
80333 München
oder per Email: michael.tempelmeier@tum.de

Visit us on the internet at: http://www.sec.ei.tum.de/