Cryptographic Engineering Research Group Presents

ECE Departmental Seminar

The CAESAR-API in the Real World

Tuesday, May 8th, 2018
3:00 pm — 4:00 pm
Engineering Building, Room 3507

Speaker: Michael Tempelmeier
Technical University of Munich

Abstract:

In 2013 the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) was started. It aims at determining a portfolio of ciphers for authenticated encryption that has advantages over AES-GCM in terms of performance, security, and ease of implementation. This competition, for the first time, provides a standardized hardware API, which allows a fair comparison of hardware implementations. However, the community still lacks a common platform to automatically test hardware implementations, confirm implementation claims, and benchmark performance figures on real hardware in terms of runtime, area, power and energy consumption. In this work, we present a common platform using the CAESAR-API in a Xilinx Zynq-7000 System on Chip (SoC) with ARM processors and an AXI interface. This reflects a typical real world usage scenario for hardware-accelerators and thus extends the work for a fair comparison of hardware implementations in three dimensions: first the API is evaluated on a real SoC, which shows, e.g. the performance of the API. Second, it provides a hardware platform to test the proposed implementations of the candidates easily. This can be used by future designers, as we will provide it as open source hardware. Finally, we ran all published hardware implementations of the current 3rd-round candidates during which we identified several implementation weaknesses, e.g. presumably unintended latches in the design, hence emphasizing the importance of testing hardware proposals on real hardware.

Biography:

Michael Tempelmeier is currently a PhD candidate at the Technical University of Munich. He received his Master's degree in electrical engineering from the Technical University of Munich in 2014. Since then his research focuses on (secure) hardware implementations, benchmarking of CAESAR candidates, and hardware/software codesign of authenticated encryption.