Travel Report

Xiaojie Zhu

October 31, 2017

1 CHES Introduction

CHES is the short name of the conference on cryptographic hardware and embedded system. This year, it was held from 25 til 28 of September in Taiwan. The accepted topics includes cryptographic implementations, attacks against implementations and countermeasures, tools and methodologies, Interactions between cryptographic theory and implementation issues and some applications, e.g., hardware IP protection and anti-counterfeiting, automotive security and trusted computing platforms.

2 Content from the conference

The first day, there are four tutorials for two topics. The first is the *Post-quantum cryptography for embedded systems*. The second is the *side channel live*. Both topics are quite popular recently as they are kind of new attacks of existing systems.

The second day, we have four sessions. The first session is side channel analysis. It includes four papers. The first is *a side-channel assisted cryptanalytic attack against QcBits*. The second is the *Improved blind side-channel analysis by exploitation of joint distribution of leakages*. The third is the *convolution neural networks with data augmentation against jitter-based countermeasures -profiling attacks without pre-processing* and the last one is the *cacheZoom: How SGX amplies the power of cache attack*. There are only three papers in the second session, *McBits revisited*, *High-speed key encapsulating from NTRU*, and *FPGA-based key generator for the niederreiter cryptosystem using binary goppa codes*. The session three is emerging attacks. There are only two papers, but one of them is the best paper. The best paper is the *nanfocused x-ray beam to reprogram secure circuits* and another one is *novel bypass attack and bdd-based tradeoff analysis against all known logic locking attacks*. Both papers are very interesting, which provide a novel way to analysis the security weakness in the circuit.

In the second day there are three sessions. The first is the related block cipher and protocol design. The first paper is *blockcipher-based authenticated encryption:how small can we go?*. The second paper is the *Gimili:a cross-platform permutation*. The third is

Gift:a small present. The last is the *making password authenticated key exchange suitable for resource-constrained industrial control devices*. The second session is security evaluation. The first is *back to massey: impressively fast, scalable, and tight security evaluation tools*. The second is *fast leakage assessment*. The third session is the FPGA security. As the popularity of FPGA, more and more researches focus on the chip. This results that increasing vulnerabilities are found. The first paper is *Your Rails cannot hide from localized em:how dual-rail logic fails on FPGAs*. The second is *how to break secure boot on FPGA socs through malicious hardware*.

In the last day, there are four sessions and eleven papers. The first session is the emerging attack which is the second part of last day. It includes three papers. The first one is the *illusion and dazzle: adversarial optical channel exploits against lidars for automotive applications*. The second is *hacking in the blind:(almost) invisible runtime user interface attacks*. The third is the *on the security of carrier phase-based ranging*. The second session is side-channel analysis. The first paper is the *a systematic approach to the side channel analysis of ECC implementations with worst-case horizontal attack*. The second is the *single-trace side-channel attack on masked lattice-based encryption*. The third paper is *sliding right into disaster:left-to-right sliding windows leak*. The third session is the encoding techniques. The first paper is *faster homomorphic function evaluation using non-integral base encoding*. The second paper is *hiding secrecy leakage in leaky helper data*. The last session is efficient implementation. The first paper is *very high order masking: efficient implementation and security evaluation*. The second paper is *present runs fast: efficient and secure implementation in software*. The third is *fourQ on embeded devices with strong countermeasures against side-channel attacks*. The last is *bit-sliding: a generic technique for bit-serial implementations of SPN-based primitives-applications to aes, present and skinny*.

Figure 1: picture taken from conference