Lehrstühle und Professuren

Dokumenttyp: Konferenzbeitrag

Art des Konferenzbeitrags: Vortrag / Präsentation

Autor(en) des Beitrags: Yu, Meng-Day (Mandel) and Hiller, Matthias and Devadas, Srinivas

Titel des Beitrags: Maximum-Likelihood Decoding of Device-Specific Multi-Bit Symbols for Reliable Key Generation

Abstract: We present a PUF key generation scheme that uses the provably optimal method of maximum-likelihood (ML) detection on symbols derived from PUF response bits. Each device forms a noisy, device-specific symbol constellation, based on manufacturing variation. Each detected symbol is a letter in a codeword of an error correction code, resulting in non-binary codewords. We present a three-pronged validation strategy: i. mathematical (deriving an optimal symbol decoder), ii. simulation (comparing against prior approaches), and iii. empirical (using implementation data). We present simulation results demonstrating that for a given PUF noise level and block size (an estimate of helper data size), our new symbol-based ML approach can have orders of magnitude better bit error rates compared to prior schemes such as block coding, repetition coding, and threshold-based pattern matching, especially under high levels of noise due to extreme environmental variation. We demonstrate environmental reliability of a ML symbol-based soft-decision error correction approach in 28nm FPGA silicon,
covering -65°C to 105°C ambient (and including 125°C junction), and with 128-bit key regeneration error probability >-1 ppm.

**Stichworte:**
Physical Unclonable Function, Maximum-Likelihood, Non-Binary Codewords, Soft-Decision, Key Generation

**Dewey Dezimalklassifikation (Liste):**
620 Ingenieurwissenschaften

**Kongress- / Buchtitel:**
IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

**Kongress / Zusatzinformationen:**
Washington, USA

**Jahr:**
2015

**Quartal:**
2. Quartal

**Jahr / Monat:**
2015-05

**Monat:**
May

**Revied:**
ja

**Sprache:**
en

**WWW:**
http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=41204

**Occurences:**
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2015

entries: