Abstract:
Silicon Physical Unclonable Functions (PUFs) produce a sequence of response bits from chip-unique manufacturing variations. Since the response bits are physically derived, there is noise present. To generate bit-exact cryptographic keys, error correction algorithms are used. The error correction is typically split into small processing blocks to reduce implementation complexity. The reliability of PUF responses varies from bit to bit but there has been very little work so far that mathematically analyzes the effect of the block size on the reliability of PUF response sequences. We use the information theoretical concept of typicality to show that the probability of drawing an unreliable sequence decreases exponentially with the block size.
We present Differential Sequence Coding (DSC) that scales efficiently across larger block sizes without having the super-linear increase in decoding complexity of prior approaches. It scans the entire PUF response sequentially and then only operates on one single, maximally reliable, block to generate the cryptographic key. Our sample FPGA implementation with a convolutional code is designed for a popular SRAM PUF.
scenario. It generates a 128 bit key for an average input bit error probability of 15% with an output bit error probability of 6.14*10^{-9} and only uses 974 PUF and 1; 108 helper data bits. There are 36% less PUF bits and 71% less helper data bits than the best previous individual results in both criteria without increasing the implementation size of the key generation module noticeably.

**Stichworte:** Physical Unclonable Function (PUF), Syndrome Coding, Error Correction, Differential Sequence Coding (DSC), Typicality, Convolutional Code, FPGA.

**Dewey Dezimalklassifikation neu:**

620 Ingenieurwissenschaften

**Zeitschriftentitel:**

IEEE Transactions on Information Forensics and Security

**Jahr:**

2016

**Jahr / Monat:**

2016-09

**Quartal:**

3. Quartal

**Monat:**

Sep

**Heft / Issue:**

Volume: 11 Issue: 9

**Seiten:**

pages: 2065-2076

**Nachgewiesen in:**

Scopus

**Reviewed:**

ja

**Sprache:**

en

**Volltext / DOI:**

http://doi.org/10.1109/TIFS.2016.2573766

**WWW:**

https://signalprocessingsociety.org/publications-resources/ieee-transactions-information-forensics-and-security

**Occurences:**

- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)

- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

**entries:**