Dokumenttyp: Konferenzbeitrag
Art des Konferenzbeitrags: Vortrag / Präsentation
Autor(en) des Beitrags: Hiller, Matthias and Rodrigues Lima, Leandro and Sigl, Georg
Titel des Beitrags: Seesaw: An Area-Optimized FPGA Viterbi Decoder for PUFs
Abstract: Physical Unclonable Functions PUFs are popular security primitives to provide cryptographic keys on FPGAs. However, PUFs require error correction to create reliable cryptographic keys. This work presents a highly optimized Viterbi decoder, adapted to the constraints of PUFs on FPGAs, primarily area but also low power. Our Seesaw architecture contains two block RAMs that are connected through a custom low-area data path. As main result, alternating data access patterns reduce the complexity of the data handling in the Viterbi decoder. Instead of translating through the entire trellis, we introduce a method that only operates on the last state. The new access pattern permits to store the intermediate results in block RAM and leads to a compact overall footprint with low register count. Synthesis results for one legacy and one state-of-the-art FPGA, and a comparison to state-of-the-art implementations demonstrate the efficiency of our new Seesaw architecture. Our decoder requires only 65 FPGA slices and 2 block RAMs to carry out the entire Viterbi decoding for a popular (2, 1, [7]) convolutional code.

Stichworte:
Physical Unclonable Functions (PUFs), Error Correction, Convolutional Code, Viterbi Algorithm, VLSI, FPGA

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
EUROMICRO Conference on Digital System Design (DSD) 2014

Kongress / Zusatzinformationen:
Verona, Italy
Jahr:
2014
Quartal:
3. Quartal
Jahr / Monat:
2014-08
Monat:
Aug
Revied:
ja
Sprache:
en
WWW:
http://esd.scienze.univr.it/dsd-seaa-2014/?page_id=22

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2014

Entries: