Andrey Bogdanov - DTU Orbit (13/01/2018)

Bogdanov, Andrey
anbog@dtu.dk
Department of Applied Mathematics and Computer Science - Associate Professor
Cyber Security

Publications:

Cache timing attacks on recent microarchitectures
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Efficient configurations for block ciphers with unified ENC/DEC paths
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Adaptable AES implementation with power-gating support
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Atomic-AES: A compact implementation of the AES encryption/decryption core
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Exploring Energy Efficiency of Lightweight Block Ciphers
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Fast and Memory-Efficient Key Recovery in Side-Channel Attacks
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Low-area hardware implementations of CLOC, SILC and AES-OTR
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Round Gating for Low Energy Block Ciphers
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Comb to Pipeline: Fast Software Encryption Revisited
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Cryptanalysis of Two Fault Countermeasure Schemes
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Exploring the energy consumption of lightweight blockciphers in FPGA
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Twisted Polynomials and Forgery Attacks on GCM
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

ALE: AES-based lightweight authenticated encryption
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

How to Securely Release Unverified Plaintext in Authenticated Encryption
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Key Recovery Attacks on Recent Authenticated Ciphers
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis
Publication: Research - peer-review › Journal article – Annual report year: 2014

Lightweight cryptography for constrained devices
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015
Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard
Publication: Research - peer-review › Journal article – Annual report year: 2014

On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Route 66: Passively Breaking All GSM Channels
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Towards understanding the known-key security of block ciphers
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Efficient and side-channel resistant authenticated encryption of FPGA bitstreams
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Generalized Feistel networks revisited
Bogdanov, A. & Shibutani, K. 2013 In : Designs, Codes and Cryptography. 66, 3-3, p. 75-97
Publication: Research - peer-review › Journal article – Annual report year: 2013

Improved Impossible Differential Attacks on Large-Block Rijndael
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Parallelizable and Authenticated Online Ciphers
Projects:

Statistical Tools for Cybersecurity
Vejre, P. S., Bogdanov, A. & Knudsen, L. R.
01/02/2016 → 31/01/2019
Project: PhD