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: 2016

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
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
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

SPONGENT: The Design Space of Lightweight Cryptographic Hashing
Publication: Research - peer-review › Journal article – Annual report year: 2013

Beyond the Limits of DPA: Combined Side-Channel Collision Attacks
Publication: Research - peer-review › Journal article – Annual report year: 2012

Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Integral and Multidimensional Linear Distinguishers with Correlation Zero
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations (Extended Abstract)
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

On security arguments of the second round SHA-3 candidates
Publication: Research - peer-review › Journal article – Annual report year: 2012

Publication: Research - peer-review › Book – Annual report year: 2012

The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers
Publication: Research - peer-review › Journal article – Annual report year: 2012

Zero correlation linear cryptanalysis with reduced data complexity
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN
Publication: Research - peer-review › Conference article – Annual report year: 2011

Analysis of 3-line generalized Feistel networks with double SD-functions
Publication: Research - peer-review › Conference article – Annual report year: 2011

Biclique cryptanalysis of the full AES
Publication: Research - peer-review › Journal article – Annual report year: 2011

Double SP-Functions: Enhanced Generalized Feistel Networks: Extended Abstract
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Spongent: A lightweight hash function
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011
Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs
Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

On the differential and linear efficiency of balanced Feistel networks
Publication: Research - peer-review › Journal article – Annual report year: 2010

Algebraic methods in side-channel collision attacks and practical collision detection
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Fast Multivariate Signature Generation in Hardware: The Case of Rainbow
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Hash functions and RFID tags: Mind the gap
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Linear slide attacks on the KeeLoq block cipher
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Multiple-Differential Side-Channel Collision Attacks on AES
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Projects:

Statistical Tools for Cybersecurity
Project: PhD