A fog-based privacy-preserving approach for distributed signature-based intrusion detection
Wang, Y., Meng, W., Li, W., Li, J., Liu, W-X. & Xiang, Y. 2018 In : Journal of Parallel and Distributed Computing. 122, p. 26-35
Publication: Research - peer-review › Journal article – Annual report year: 2018

CodeTrust: Trusting Software Systems
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Cyber-physical architecture assisted by programmable networking
Publication: Research - peer-review › Journal article – Annual report year: 2018

CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems
Sahay, R., Sepúlveda Estay, D. A., Meng, W., Jensen, C. D. & Barfod, M. B. 2018
Publication: Research - peer-review › Paper – Annual report year: 2018

Detecting insider attacks in medical cyber–physical networks based on behavioral profiling
Publication: Research - peer-review › Journal article – Annual report year: 2018

Enhancing Intelligent Alarm Reduction for Distributed Intrusion Detection Systems via Edge Computing
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Evaluating the Impact of Juice Filming Charging Attack in Practical Environments
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Impossible meet-in-the-middle fault analysis on the LED lightweight cipher in VANETs
Li, W., Rijmen, V., Tao, Z., Wang, Q., Chen, H., Liu, Y., Li, C. & Liu, Y. 2018 In : Science China Information Sciences. 61, 3, 13 p., 032110
Publication: Research - peer-review › Journal article – Annual report year: 2018

Improved meet-in-the-middle attacks on reduced-round Piccolo
Publication: Research - peer-review › Journal article – Annual report year: 2018

Inverse Gating for Low Energy Encryption
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks
Li, W., Meng, W. & Kwok, L. F. 2018 In : Future Internet. 10, 1, 16 p.
Publication: Research - peer-review › Journal article – Annual report year: 2018

JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones
Publication: Research - peer-review › Journal article – Annual report year: 2018
Plasmonic anisotropic metasurfaces: from far-field measurements to near-field properties
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Putting Wings on SPHINCS
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

TouchWB: Touch behavioral user authentication based on web browsing on smartphones
Publication: Research - peer-review › Journal article – Annual report year: 2018

Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks
Publication: Research - peer-review › Journal article – Annual report year: 2018

Towards False Alarm Reduction using Fuzzy If-Then Rules for Medical Cyber Physical Systems
Li, W., Meng, W., Su, C. & Kwok, L. F. 2018 In : *IEEE Access*. 6, p. 6530-6539
Publication: Research - peer-review › Journal article – Annual report year: 2018

When Intrusion Detection Meets Blockchain Technology: A Review
Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y. & Han, J. 2018 In : *IEEE Access*. 6, p. 10179 - 10188
Publication: Research - peer-review › Journal article – Annual report year: 2018

Work Package 2 Report - Cyber resilience for the shipping industry
Publication: Research › Report – Annual report year: 2018

A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks
Publication: Research - peer-review › Journal article – Annual report year: 2017

A brief comparison of Simon and Simeck
Publication: Research - peer-review › Conference article – Annual report year: 2017

A New Structural-Differential Property of 5-Round AES
Publication: Research - peer-review › Conference article – Annual report year: 2017

A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-Based Systems
Publication: Research - peer-review › Book chapter – Annual report year: 2017

Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries
Publication: Research › Ph.D. thesis – Annual report year: 2017

Behavioural Profiling in Cyber-Social Systems
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

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

Design and analysis of cryptographic algorithms
Publication: Research › Ph.D. thesis – Annual report year: 2017

Detecting Malicious Nodes in Medical Smartphone Networks Through Euclidean Distance-Based Behavioral Profiling
Publication: Research - peer-review › Book chapter – Annual report year: 2017

Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks
Publication: Research - peer-review › Journal article – Annual report year: 2017

Do we educate engineers that can engineer?
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

Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model
Publication: Research - peer-review › Journal article – Annual report year: 2017

Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data
Meng, W., Li, W., Su, C., Zhou, J. & Lu, R. 2017 In : IEEE Access. 6, p. 7234 - 7243
Publication: Research - peer-review › Journal article – Annual report year: 2018
Adaptable AES implementation with power-gating support
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

A MAC Mode for Lightweight Block Ciphers
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

Building indifferentiable compression functions from the PGV compression functions
Publication: Research - peer-review › Journal article – Annual report year: 2016

Conditional differential cryptanalysis of 105 round Grain v1
Banik, S. 2016 In *: Cryptography and Communications*. 8, 1, p. 113-137
Publication: Research - peer-review › Journal article – Annual report year: 2016

Cryptanalyzing of Selected Block Ciphers
Publication: Research › Ph.D. thesis – Annual report year: 2016

Design and Analysis of Symmetric Primitives
Publication: Research › Ph.D. thesis – Annual report year: 2016

Feasibility study of context-awareness device Comfort calculation methods and their application to comfort-based access control
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Identity management for e-government Libya as a case study
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Introducing E-Government in Developing Countries Analysis of Egyptian e-Government Services
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016
PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Polytopic Cryptanalysis

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

Secure Refactoring with Java Information Flow

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities

Publication: Research - peer-review › Book chapter – Annual report year: 2017

Towards Formal Analysis of Insider Threats for Auctions

Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows

Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography

Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Ciphers for MPC and FHE

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

Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures
Coron, J-S., Roy, A. & Vivek, S. 2015 In : Journal of Cryptographic Engineering. 5, 2, p. 73-83
Publication: Research - peer-review › Journal article – Annual report year: 2015

How Not to Combine RC4 States
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Linear Distinguishers in the Key-less Setting: Application to PRESENT
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Links among Impossible differential, integral and zero correlation linear cryptanalysis
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Observations on the SIMON Block Cipher Family
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Practical Attacks on AES-like Cryptographic Hash Functions
Publication: Research - peer-review › Book chapter – Annual report year: 2015

Security of the AES with a Secret S-Box
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015
Some Results on Sprout
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Some security results of the RC4+ stream cipher
Banik, S. & Jha, S. 2015 In : Security and Communication Networks. 8, 18, p. 4061-4072
Publication: Research - peer-review › Journal article – Annual report year: 2015

State-Recovery Analysis of Spritz
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

The Rebound Attack and Subspace Distinguishers: Application to Whirlpool
Publication: Research - peer-review › Journal article – 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

Cryptanalysis of SIMON Variants with Connections
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Book – Annual report year: 2015

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

Internal differential collision attacks on the reduced-round Grøstl-0 hash function
Ideguchi, K., Tischhauser, E. W. & Preneel, B. 2014 In : Designs, Codes and Cryptography. 70, 3, p. 251-271
Key Recovery Attacks on Recent Authenticated Ciphers

Lightweight cryptography for constrained devices

Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard

On the Efficacy of Solving LWE by Reduction to Unique-SVP

On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers

On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui’s Algorithm 2

Rotational Rebound Attacks on Reduced Skein

Route 66: Passively Breaking All GSM Channels

The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE

Towards understanding the known-key security of block ciphers

Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA
Dynamic encryption method
Knudsen, L. R. 2013
Publication: Research › Patent – Annual report year: 2013

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

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

Improved cryptanalysis of the block cipher KASUMI
Publication: Research › Conference article – Annual report year: 2013

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

Parallelizable and Authenticated Online Ciphers
Publication: Research › Article in proceedings – Annual report year: 2013

Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers
Publication: Research › Book – Annual report year: 2013

Slender-Set Differential Cryptanalysis
Borghoff, J., Knudsen, L. R., Leander, G. & Thomsen, S. S. 2013 In : Journal of Cryptology. 26, 1, p. 11-38
Publication: Research › Journal article – Annual report year: 2013

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

The range of attraction for light traps catching Culicoides biting midges
Publication: Research › Poster – Annual report year: 2013

The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae)
Publication: Research › Journal article – Annual report year: 2013
Cryptanalysis of Some Lightweight Symmetric Ciphers
Publication: Research › Ph.D. thesis – Annual report year: 2013

Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks
Bogdanov, A., Kavun, E. B., Tischhauser, E. & Yalcin, T. 2012 International Conference on Reconfigurable Computing and FPGAs (ReConFig) 2012, IEEE
Publication: Research › peer-review › Article in proceedings – Annual report year: 2013