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

A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks
Meng, W., Li, W., Xiang, Y. & Choo, K. K. R. 2017 In : Journal of Network and Computer Applications. 78, p. 162-169
Publication: Research - peer-review › Journal article – Annual report year: 2017

A brief comparison of Simon and Simeck
Kölbl, S. & Roy, A. 2017 In : Lecture Notes in Computer Science. 10098, p. 69-88
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

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
SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Towards effective and robust list-based packet filter for signature-based network intrusion detection: an engineering approach
Meng, W., Li, W. & Kwok, L-F. 2017 In : Transactions - Hong Kong Institution of Engineers. 24, 4, p. 204-215 12 p.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments
Meng, W., Li, W. & Kwok, L-F. 2017 In : IEEE Transactions on Network and Service Management. 14, 1, p. 233 - 245
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling
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

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 indistinguishable 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

Cryptanalysis 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
Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013


How to Securely Release Unverified Plaintext in Authenticated Encryption

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

The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE
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

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 - 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

Improved cryptanalysis of the block cipher KASUMI
Publication: Research - peer-review › Conference 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

Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers
Slender-Set Differential Cryptanalysis
Borghoff, J., Knudsen, L. R., Leander, G. & Thomsen, S. S. 2013 In : Journal of Cryptology. 26, 1, p. 11-38

SPONGENT: The Design Space of Lightweight Cryptographic Hashing

The range of attraction for light traps catching Culicoides biting midges

The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae)

Cryptanalysis of Some Lightweight Symmetric Ciphers

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

Projects:

Cyber Resilience for the Shipping industry
01/09/2017 → 31/08/2019
Project