Cyber Security - Publications - DTU Orbit (20/04/2018)

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

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

Putting Wings on SPHINCS
Publication: Research - peer-review › Article in proceedings – 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

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 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 › Conference article – 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

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

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

Evaluating challenge-based trust mechanism in medical smartphone networks: an empirical study
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Exploring Effect of Location Number on Map-Based Graphical Password Authentication
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

From Higher-Order Differentials to Polytopic Cryptanalyis
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Harvesting Smartphone Privacy Through Enhanced Juice Filming Charging Attacks
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

JFCGuard: Detecting juice filing charging attack via processor usage analysis on smartphones
Publication: Research - peer-review › Journal article – Annual report year: 2017

Modeling and Verification of Insider Threats Using Logical Analysis
Publication: Research - peer-review › Journal article – Annual report year: 2017

Reflection ciphers
Boura, C., Canteaut, A., Knudsen, L. R. & Leander, G. 2017 In : Designs, Codes and Cryptography. 82, p. 3-25
Publication: Research - peer-review › Journal article – 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 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

Crytpanalysis 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: 2017

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
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 Efficacy of Solving LWE by Reduction to Unique-SVP
Publication: Research › peer-review › Article in proceedings – 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

Rotational Rebound Attacks on Reduced Skein
Publication: Research › peer-review › Journal article – Annual report year: 2014

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: 2013

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

The range of attraction for light traps catching Culicoides biting midges
Publication: Research - peer-review › Journal article – Annual report year: 2013

Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks
Publication: Research › Ph.D. thesis – Annual report year: 2013