Cyber Security - Publications - DTU Orbit (28/06/2018)

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

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

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

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
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
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: 2018

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
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

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

Crypanalisis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013
Publication: Research - peer-review » Book – Annual report year: 2015

How to Securely Release Unverified Plaintext in Authenticated Encryption
Publication: Research - peer-review » Book – 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
Publication: Research - peer-review » Journal article – Annual report year: 2014

Key Recovery Attacks on Recent Authenticated Ciphers
Publication: Research - peer-review » Book – Annual report year: 2014

Lightweight cryptography for constrained devices
Publication: Research - peer-review » Article in proceedings – Annual report year: 2014

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 » Book – 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 » Book – Annual report year: 2014

On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui’s Algorithm 2
Publication: Research - peer-review » Book – 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 » Book – Annual report year: 2014
SPONGENT: The Design Space of Lightweight Cryptographic Hashing
Publication: Research - peer-review › Journal article – Annual report year: 2013

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

The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae)
Publication: Research - peer-review › 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