Cyber Security - Publications - DTU Orbit (14/06/2018)

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

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
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 › 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: 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 Cryptanalysis
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 filming 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

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

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
Ciphers for MPC and FHE

Comb to Pipeline: Fast Software Encryption Revisited

Cryptanalysis of Two Fault Countermeasure Schemes

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

How Not to Combine RC4 States

Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48

Linear Distinguishers in the Key-less Setting: Application to PRESENT

Links among impossible differential, integral and zero correlation linear cryptanalysis

Observations on the SIMON Block Cipher Family

Practical Attacks on AES-like Cryptographic Hash Functions
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: 2015

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