Cyber Security - DTU Orbit (10/03/2018)

Cyber Security
Department of Applied Mathematics and Computer Science
Organisational unit: Section

Publications:

- **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 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

- **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
Publication: Research - peer-review › Journal article – Annual report year: 2017

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 Cryptyanalysis
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
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
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
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

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
Publication: Research - peer-review › Journal article – Annual report year: 2014

Lightweight cryptography for constrained devices
Publication: Research - peer-review › Article in proceedings – 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
Parallelizable and Authenticated Online Ciphers

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