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

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

Publications:

**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: 2018

**A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords**
Publication: Research - peer-review › Article in proceedings – 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
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
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: 2016

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
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
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

Twisted Polynomials and Forgery Attacks on GCM
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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

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
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

Towards understanding the known-key security of block ciphers

Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA
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 › Article in proceedings – Annual report year: 2013

Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware
Publication: Research › Article in proceedings – Annual report year: 2013

Improved cryptanalysis of the block cipher KASUMI
Publication: Research › Conference article – Annual report year: 2013

Improved Impossible Differential Attacks on Large-Block Rijndael
Publication: Research › Article in proceedings – Annual report year: 2013

Parallelizable and Authenticated Online Ciphers
Publication: Research › Article in proceedings – Annual report year: 2013

Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers
Publication: Research › Book – Annual report year: 2013

Slender-Set Differential Cryptanalysis
Borghoff, J., Knudsen, L. R., Leander, G. & Thomsen, S. S. 2013 In : Journal of Cryptology. 26, 1, p. 11-38
Publication: Research - peer-review › Journal article – Annual report year: 2013

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

Projects:

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