Evaluating the Impact of Juice Filming Charging Attack in Practical Environments. / Meng, Weizhi; Lee, Wang; Liu, Zhe; Su, Chunhua; Li, Yan.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Improved meet-in-the-middle attacks on reduced-round Piccolo. / Liu, Ya; Cheng, Liang; Liu, Zhiqiang; Li, Wei; Wang, Qingiu; Gu, Dawu.
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, Wenjuan; Meng, Weizhi; Kwok, Lam For.
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, Wenjuan; Meng, Weizhi; Su, Chunhua; Kwok, Lam For.
Publication: Research - peer-review › Journal article – Annual report year: 2018

When Intrusion Detection Meets Blockchain Technology: A Review. / Meng, Weizhi; Tischhauser, Elmar Wolfgang; Wang, Qingiu; Wang, Yu; Han, Jinguang.
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, Weizhi; Li, Wenjuan; Xiang, Yang; Choo, Kim Kwang Raymond.
Publication: Research - peer-review › Journal article – Annual report year: 2017

A brief comparison of Simon and Simeck. / Kölbl, Stefan; Roy, Arnab.
Publication: Research - peer-review › Conference article – Annual report year: 2017

A New Structural-Differential Property of 5-Round AES. / Grassi, Lorenzo; Rechberger, Christian; Ronjom, Sondre.
Publication: Research - peer-review › Conference article – Annual report year: 2018

A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords. / Meng, Weizhi; Li, Wenjuan; Lee, Wang; Jiang, Lijun; Zhou, Jianying.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing. / Wang, Yu; Xie, Lin; Li, Wenjuan; Meng, Weizhi; Li, Jin.
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. / Chauhan, Muhammad Aufee; Probst, Christian W.
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. / Elaswad, Othman; Jensen, Christian D. (Main supervisor).
Publication: Research › Ph.D. thesis – Annual report year: 2017

Cache timing attacks on recent microarchitectures. / Andreou, Alexandres; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Design and analysis of cryptographic algorithms. / Kölbl, Stefan; Rechberger, Christian (Main supervisor); Knudsen, Lars Ramkilde (Supervisor).
Publication: Research › Ph.D. thesis – Annual report year: 2017

Detecting Malicious Nodes in Medical Smartphone Networks Through Euclidean Distance-Based Behavioral Profiling. / Meng, Weizhi; Li, Wenjuan; Wang, Yu; Au, Man.
Publication: Research - peer-review › Book chapter – Annual report year: 2017

Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks. / Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For; IP, Horace H.S.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Do we educate engineers that can engineer? / Nyborg, Mads; Probst, Christian W.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Efficient configurations for block ciphers with unified ENC/DEC paths. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco.
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. / Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For; IP, Horace H.S.
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, Weizhi; Li, Wenjuan; Su, Chunhua; Zhou, Jianying; Lu, Rongxing.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Evaluating challenge-based trust mechanism in medical smartphone networks: an empirical study. / Meng, Weizhi; Fei, Fei; Li, Wenjuan; Au, Man Ho.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Exploring Effect of Location Number on Map-Based Graphical Password Authentication. / Meng, Weizhi; Lee, Wang; Au, Man Ho; Liu, Zhe.
Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study. / Jiang, Lijun; Meng, Weizhi; Wang, Michael Yu; Su, Chunhua; Li, Jin-xuan.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

From Higher-Order Differentials to Polytopic Cryptanalysis. / Tiessen, Tyge.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Harvesting Smartphone Privacy Through Enhanced Juice Filming Charging Attacks. / Meng, Weizhi; Fei, Fei; Li, Wenjuan; Au, Man Ho.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones. / Meng, Weizhi; Jiang, Lijun; Wang, Yu; Li, Jin; Zhang, Jun; Xiang, Yang.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Modeling and Verification of Insider Threats Using Logical Analysis. / Kammuller, Florian; Probst, Christian W.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Reflection ciphers. / Boura, Christina; Canteaut, Anne; Knudsen, Lars Ramkilde; Leander, Gregor.
In: Designs, Codes and Cryptography, Vol. 82, 2017, 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. / Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For.
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, Weizhi; Li, Wenjuan; Kwok, Lam For.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments. / Meng, Weizhi; Li, Wenjuan; Kwok, Lam-For.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones. / Meng, Weizhi; Li, Wenjuan; Kwok, Lam For; Choo, Kim Kwang Raymond.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling. / Meng, Weizhi; Au, Man Ho.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Adaptable AES implementation with power-gating support. / Banik, Subhadeep; Bogdanov, Andrey; Fanni, Tiziana; Sau, Carlo; Raffo, Luigi; Palumbo, Francesca; Regazzoni, Francesco.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

A MAC Mode for Lightweight Block Ciphers. / Luykx, Atul; Preneel, Bart; Tischhauser, Elmar Wolfgang; Yasuda, Kan.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Atomic-AES: A compact implementation of the AES encryption/decryption core. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Building indifferentiable compression functions from the PGV compression functions. / Gauravaram, P.; Bagheri, Nasour; Knudsen, Lars Ramkilde.
Publication: Research - peer-review › Journal article – Annual report year: 2016

Conditional differential cryptanalysis of 105 round Grain v1. / Banik, Subhadeep.
In: Cryptography and Communications, Vol. 8, No. 1, 2016, p. 113-137.
Publication: Research - peer-review › Journal article – Annual report year: 2016

Cryptanalysis of Selected Block Ciphers. / Alkhzaimi, Hoda A.; Knudsen, Lars Ramkilde (Supervisor).
Publication: Research › Ph.D. thesis – Annual report year: 2016

Design and Analysis of Symmetric Primitives. / Lauridsen, Martin Mehl; Rechberger, Christian (Supervisor); Knudsen, Lars Ramkilde (Supervisor).
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. / Guo, Jingjing; Jensen, Christian D.; Ma, Jianfeng.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Identity management for e-government Libya as a case study. / Elaswad, Othoman; Jensen, Christian D.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Introducing E-Government in Developing Countries Analysis of Egyptian e-Government Services. / Elaswad, Othoman; Jensen, Christian D.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. / Albrecht, Martin; Grassi, Lorenzo; Rechberger, Christian; Roy, Arnab; Tiessen, Tyge.
PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks. / Li, Wenjuan; Meng, Weizhi; Kwok, Lam-Fo; Ip, Ho Shing.

Polytopic Cryptanalysis. / Tiessen, Tyge.

Round Gating for Low Energy Block Ciphers. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco; Isobe, Takanori; Hiwatari, Harunaga; Akishita, Toru.

Secure Refactoring with Java Information Flow. / Helke, Steffen; Kammüniidler, Florian; Probst, Christian W.

Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities. / Jiang, Lijun; Meng, Weizhi.

Towards Formal Analysis of Insider Threats for Auctions. / Kammueller, Florian; Kerber, Manfred; Probst, Christian W.

Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness. / Bogdanov, Andrey; Isobe, Takanori; Tischhauser, Elmar Wolfgang.

Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows. / Beierle, Christof; Jovanovic, Philipp; Lauridsen, Martin Mehl; Leander, Gregor; Rechberger, Christian.

APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography. / Andreeva, Elena; Bilgin, Begül; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Mouha, Nicky; Yasuda, Kan.

Ciphers for MPC and FHE. / R. Albrecht, Martin; Rechberger, Christian; Schneider, Thomas; Tiessen, Tyge; Zohner, Michael.
Some Results on Sprout. / Banik, Subhadeep.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Some security results of the RC4+ stream cipher. / Banik, Subhadeep; Jha, Sonu.
Publication: Research - peer-review › Journal article – Annual report year: 2015

State-Recovery Analysis of Spritz. / Ankele, Ralph; Kölbl, Stefan; Rechberger, Christian.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. / Lamberger, Mario; Mendel, Florian; Schlaffer, Martin; Rechberger, Christian; Rijmen, Vincent.
Publication: Research - peer-review › Journal article – Annual report year: 2015

Twisted Polynomials and Forgery Attacks on GCM. / Abdelraheem, Mohamed Ahmed A. M. A.; Beelen, Peter ; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

ALE: AES-based lightweight authenticated encryption. / Bogdanov, Andrey; Mendel, Florian; Regazzoni, Francesco; Rijmen, Vincent; Tischhauser, Elmar.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Cryptanalysis of SIMON Variants with Connections. / Alizadeh, Javad; Alkhzaimi, Hoda A.; Aref, Mohammad Reza; Bagheri, Nasour; Gauravaram, Praveen; Kumar, Abhishek; Lauridsen, Martin Mehl; Sanadhya, Somitra Kumar.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013. / Banik, Subhadeep; Chattopadhyay, Anupam; Chowdhury, Anusha.
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. / Andreeva, Elena; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Mouha, Nicky; Yasuda, Kan.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014
Internal differential collision attacks on the reduced-round Grøstl-0 hash function. / Ideguchi, Kota; Tischhauser, Elmar Wolfgang; Preneel, Bart.
Publication: Research - peer-review › Journal article – Annual report year: 2014

Key Recovery Attacks on Recent Authenticated Ciphers. / Bogdanov, Andrey; Dobranić, Christoph; Eichlseder, Maria; Lauridsen, Martin Mehl; Mendel, Florian; Schläffer, Martin; Tischhauser, Elmar Wolfgang.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Lightweight cryptography for constrained devices. / Alippi, Cesare; Bogdanov, Andrey; Regazzoni, Francesco.
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. / Wen, Long; Wang, Meiqin; Bogdanov, Andrey; Chen, HuaiFeng.
Publication: Research - peer-review › Journal article – Annual report year: 2014

On the Efficacy of Solving LWE by Reduction to Unique-SVP. / Albrecht, Martin Roland; Fitzpatrick, Robert; Göpfert, Florian.
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. / Blondeau, Celine; Bogdanov, Andrey; Wang, Meiqin.
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. / Bogdanov, Andrey; Tischhauser, Elmar.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Rotational Rebound Attacks on Reduced Skein. / Khovratovich, Dmitry; Nikolić, Ivica; Rechberger, Christian.
Publication: Research - peer-review › Journal article – Annual report year: 2014

Route 66: Passively Breaking All GSM Channels. / Vejre, Philip S.; Bogdanov, Andrey.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE. / Khovratovich, Dmitry; Rechberger, Christian.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Towards understanding the known-key security of block ciphers. / Andreeva, Elena; Bogdanov, Andrey; Mennink, Bart.