A fog-based privacy-preserving approach for distributed signature-based intrusion detection. / Wang, Yu; Meng, Weizhi; Li, Wenjuan; Li, Jin; Liu, Wai-Xi; Xiang, Yang.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Cyber-physical architecture assisted by programmable networking. / Rubio-Hernan, Jose; Sahay, Rishikesh; De Cicco, Luca; Garcia-Alfaro, Joaquin.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Publication: Research - peer-review › Paper – Annual report year: 2018

Detecting insider attacks in medical cyber-physical networks based on behavioral profiling. / Meng, Weizhi; Li, Wenjuan; Wang, Yu; Au, Man Ho.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Editorial of special issue on mobile networks and devices security, privacy and trust. / Meng, Weizhi; Liu, Zhe; Castiglione, Aniello; Au, Man Ho.
Publication: Research - peer-review › Editorial – Annual report year: 2018

Enhancing Intelligent Alarm Reduction for Distributed Intrusion Detection Systems via Edge Computing. / Meng, Weizhi; Wang, Yu; Li, Wenjuan; Liu, Zhe; Li, Jin; Probst, Christian W.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

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

Impossible meet-in-the-middle fault analysis on the LED lightweight cipher in VANETs. / Li, Wei; Rijmen, Vincent; Tao, Zhi; Wang, Qingju; Chen, Hua; Liu, Yunwen; Li, Chaoyun; Liu, Ya.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Improved meet-in-the-middle attacks on reduced-round Piccolo. / Liu, Ya; Cheng, Liang; Liu, Zhiqiang; Li, Wei; Wang, Qingju; Gu, Dawu.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling. / Meng, Weizhi.
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 Aufeef; 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, Othoman; Jensen, Christian D. (Main supervisor).
Publication: Research › Ph.D. thesis – Annual report year: 2017

Behavioural Profiling in Cyber-Social Systems. / Perno, Jason; Probst, Christian W.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

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.
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.
(2017 IEEE International Symposium on Hardware Oriented Security and Trust (host)).
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: 2017

Exploring Effect of Location Number on Map-Based Graphical Password Authentication. / Meng, Weizhi; Lee, Wang; Au, Man Ho; Liu, Zhe.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

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

Linear Cryptanalysis of DES with Asymmetries. / Bogdanov, Andrey; Vejre, Philip Søgaard.
Modeling and Verification of Insider Threats Using Logical Analysis. / Kammuller, Florian; Probst, Christian W.
Publication: Research - peer-review › Journal article – Annual report year: 2017

Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. / Chase, Melissa; Derler, David; Golfdeder, Steven; Orlandi, Claudio; Ramacher, Sebastian; Rechberger, Christian; Slamanig, Daniel; Zaverucha, Greg.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

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.
Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. / Coron, Jean-Sébastien; Roy, Arnab; Vivek, Srinivas.
Publication: Research - peer-review › Journal article – Annual report year: 2015

How Not to Combine RC4 States. / Banik, Subhadeep; Jha, Sonu.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48. / Abdelraheem, Mohamed Ahmed; Alizadeh, Javad; Alkhzaimi, Hoda A.; Aref, Mohammad Reza; Bagheri, Nasour; Gauravaram, Praveen.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Linear Distinguishers in the Key-less Setting: Application to PRESENT. / Lauridsen, Martin Mehl; Rechberger, Christian.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Links among impossible differential, integral and zero correlation linear cryptanalysis. / Sun, Bing; Liu, Zhiqiang; Rijmen, Vincent; Li, Ruilin; Cheng, Lei; Wang, Qingju; Alkhzaimi, Hoda A.; Li, Chao.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Observations on the SIMON Block Cipher Family. / Kölbl, Stefan; Leander, Gregor; Tiessen, Tyge.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Practical Attacks on AES-like Cryptographic Hash Functions. / Kölbl, Stefan; Rechberger, Christian.
Publication: Research - peer-review › Book chapter – Annual report year: 2015

Security of the AES with a Secret S-Box. / Tiessen, Tyge; Knudsen, Lars Ramkilde; Kölbl, Stefan; Lauridsen, Martin Mehl.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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.
**The Rebound Attack and Subspace Distinguishers: Application to Whirlpool.** / Lamberger, Mario; Mendel, Florian; Schläffer, Martin; Rechberger, Christian; Rijmen, Vincent.

**Twisted Polynomials and Forgery Attacks on GCM.** / Abdelraheem, Mohamed Ahmed A. M. A.; Beelen, Peter; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang.

**ALE: AES-based lightweight authenticated encryption.** / Bogdanov, Andrey; Mendel, Florian; Regazzoni, Francesco; Rijmen, Vincent; Tischhauser, Elmar.

**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.

**Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013.** / Banik, Subhadeep; Chattopadhyay, Anupam; Chowdhury, Anusha.


**How to Securely Release Unverified Plaintext in Authenticated Encryption.** / Andreeva, Elena; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Mouha, Nicky; Yasuda, Kan.

**Internal differential collision attacks on the reduced-round Grøstl-0 hash function.** / Ideguchi, Kota; Tischhauser, Elmar Wolfgang; Preneel, Bart.

**Key Recovery Attacks on Recent Authenticated Ciphers.** / Bogdanov, Andrey; Dobrindig, Christoph; Eichlseder, Maria; Lauridsen, Martin Mehl; Mendel, Florian; Schläffer, Martin; Tischhauser, Elmar Wolfgang.