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
Inverse Gating for Low Energy Encryption. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco; Isobe, Takanori; Hiwatari, Harunaga; Akishita, Toru.
Publication: Research - peer-review › Article in proceedings – 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

JFGuard: 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 › Journal article – Annual report year: 2018

Plasmonic anisotropic metasurfaces: from far-field measurements to near-field properties. / Yermakov, Oleh Y.; Permyakov, Dmitry V.; Dmitriev, Pavel A.; Samusev, Anton K.; Iorsh, Ivan V.; Lavrinenko, Andrei V.; Bogdanov, Andrey A.; Zayats, Anatoly V.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Putting Wings on SPHINCS. / Kölbl, Stefan.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

TouchWB : Touch behavioral user authentication based on web browsing on smartphones. / Meng, Weizhi; Wang, Yu; Wong, Duncan S.; Wen, Sheng; Xiang, Yang.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. / Meng, Weizhi; Choo, Kim-Kwang Raymond; Furnell, Steven; Vasilakos, Athanasios V.; Probst, Christian W.
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, Wenjuang; 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, Qingu; Wang, Yu; Han, Jinguang.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Publication: Research › Report – 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
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: 2018
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
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 indiffferentiable 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).
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.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks. / Li, Wenjuan ; Meng, Weizhi; Kwok, Lam-For ; Ip, Ho Shing .
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Polytopic Cryptanalysis. / Tiessen, Tyge.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Round Gating for Low Energy Block Ciphers. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesc; Isobe, Takanori; Hiwatari, Harunaga; Akishita, Toru.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Secure Refactoring with Java Information Flow. / Helke, Steffen; Kammünielt kler, Florian; Probst, Christian W.
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. / Jiang, Lijun; Meng, Weizhi.
Publication: Research - peer-review › Book chapter – Annual report year: 2017

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014


Publication: Research - peer-review › Article in proceedings – Annual report year: 2015


Publication: Research - peer-review › Article in proceedings – Annual report year: 2015


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


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; Dobroinig, Christoph; Eichlseder, Maria; Lauridsen, Martin Mehl; Mendel, Florian; Schläffer, Martin; Tischhauser, Elmar Wolfgang. 3rd International Conference on Cryptology and Information Security in Latin America. Springer, 2014. p. 274-287 (Lecture Notes in Computer Science, Vol. 8895).

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014


Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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


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.