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

Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco / Efficient configurations for block ciphers with unified ENC/DEC paths.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For; IP, Horace H.S. / 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

Meng, Weizhi; Li, Wenjuan; Su, Chunhua; Zhou, Jianying; Lu, Rongxing / 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

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

Jiang, Lijun; Meng, Weizhi; Wang, Michael Yu; Su, Chunhua; Li, Jin-xuan / Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

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

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

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

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

Boura, Christina ; Canteaut, Anne; Knudsen, Lars Ramkilde; Leander, Gregor / Reflection ciphers.
In: Designs, Codes and Cryptography, Vol. 82, 2017, p. 3-25.
Publication: Research - peer-review › Journal article – Annual report year: 2017
Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For / **SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks.**
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Meng, Weizhi; Li, Wenjuan; Kwok, Lam For / **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

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

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

Meng, Weizhi; Au, Man Ho / **Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling.**
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Banik, Subhadeep; Bogdanov, Andrey; Fanni, Tiziana; Sau, Carlo; Raffo, Luigi; Palumbo, Francesca; Regazzoni, Francesco / **Adaptable AES implementation with power-gating support.**
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

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

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

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

Alkhzaimi, Hoda A.; Knudsen, Lars Ramkilde (Supervisor) / **Cryptanalysis of Selected Block Ciphers.**

Publication: Research - peer-review › Article in proceedings – Annual report year: 2017


Publication: Research - peer-review › Article in proceedings – Annual report year: 2017


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 › Article in proceedings – Annual report year: 2015


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 › Journal article – Annual report year: 2015


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


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