Cyber Security - Publications - DTU Orbit (11/05/2018)
Rubio-Hernan, Jose; Sahay, Rishikesh; De Cicco, Luca; Garcia-Alfaro, Joaquin / Cyber-physical architecture assisted by programmable networking.
Publication: Research - peer-review › Journal article – Annual report year: 2018

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

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

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

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

Li, Wenjuan; Meng, Weizhi; Su, Chunhua; Kwok, Lam For / Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks.
Publication: Research - peer-review › Journal article – Annual report year: 2018

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

Li, Wenjuan; Meng, Weizhi; Su, Chunhua; Kwok, Lam For / Towards False Alarm Reduction using Fuzzy If-Then Rules for Medical Cyber Physical Systems.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Meng, Weizhi; Tischhauser, Elmar Wolfgang; Wang, Qingju; Wang, Yu; Han, Jinguang / When Intrusion Detection Meets Blockchain Technology: A Review.
Publication: Research - peer-review › Journal article – Annual report year: 2018

Meng, Weizhi; Li, Wenjuan; Xiang, Yang; Choo, Kim Kwang Raymond / A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks.
Publication: Research - peer-review › Journal article – Annual report year: 2017

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

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

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

Meng, Weizhi; Li, Wenjuan ; Lee, Wang; Jiang, Lijun; Zhou, Jianying / A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords.
Wang, Yu; Xie, Lin; Li, Wenjuan; Meng, Weizhi; Li, Jin / A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing.

Chauhan, Muhammad Aufeef; Probst, Christian W. / Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-Based Systems.

Elaswad, Othoman; Jensen, Christian D. (Main supervisor) / Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries.

Andreou, Alexandres; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang / Cache timing attacks on recent microarchitectures.

Kölbl, Stefan; Rechberger, Christian (Main supervisor); Knudsen, Lars Ramkilde (Supervisor) / Design and analysis of cryptographic algorithms.

Meng, Weizhi; Li, Wenjuan; Wang, Yu; Au, Man / Detecting Malicious Nodes in Medical Smartphone Networks Through Euclidean Distance-Based Behavioral Profiling.

Li, Wenjuan; Meng, Weizhi; Kwo, Lam-For; IP, Horace H.S. / Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks.

Nybørg, Mads; Probst, Christian W. / Do we educate engineers that can engineer?

Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco / Efficient configurations for block ciphers with unified ENC/DEC paths.

Li, Wenjuan; Meng, Weizhi; Kwo, Lam-For; IP, Horace H.S. / Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model.
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: 2018

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

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

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 R.; 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

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 › Ph.D. thesis – Annual report year: 2016

Lauridsen, Martin Mehli; Rechberger, Christian (Supervisor); Knudsen, Lars Ramkilde (Supervisor) / Design and Analysis of Symmetric Primitives.
Publication: Research › Ph.D. thesis – Annual report year: 2016

Guo, Jingjing; Jensen, Christian D.; Ma, Jianfeng / Feasibility study of context-awareness device Comfort calculation methods and their application to comfort-based access control.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Kölbl, Stefan; Leander, Gregor; Tiessen, Tyge / Observations on the SIMON Block Cipher Family.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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

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

Banik, Subhadeep / Some Results on Sprout.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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

Abdelraheem, Mohamed Ahmed A. M. A.; Beelen, Peter ; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang / Twisted Polynomials and Forgery Attacks on GCM.
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.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

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


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


