Cyber Security - Publications - DTU Orbit (13/04/2018)
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

Liu, Ya; Cheng, Liang; Liu, 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

Li, Wenjuan; Meng, Weizhi; 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

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

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

Wang, Yu; Xie, Lin; Li, Wenjuan; Meng, Weizhi; Li, Jin / A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

Chauhan, Muhammad Aueef; Probst, Christian W. / Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-Based Systems.
Publication: Research - peer-review › Book chapter – Annual report year: 2017
Elaswad, Othoman; Jensen, Christian D. (Main supervisor) / Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries. 
Publication: Research › Ph.D. thesis – Annual report year: 2017

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

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

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

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. / Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks. 
Publication: Research - peer-review › Journal article – Annual report year: 2017

Meng, Weizhi; Li, Wenjuan; Su, Chunhua; Zhou, Jianying; Lu, Rongxing / 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; 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: 2017

Meng, Weizhi; Lee, Wang; Au, Man Ho; Liu, Zhe / Exploring Effect of Location Number on Map-Based Graphical Password Authentication. 
Banik, Subhadeep; Bogdanov, Andrey; Fanni, Tiziana; Sau, Carlo; Raffo, Luigi; Palumbo, Francesca; Regazzoni, Francesco / Adaptable AES implementation with power-gating support. Proceedings of the ACM International Conference on Computing Frontiers (CF '16). Association for Computing Machinery, 2016. p. 331-334.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Publication: Research - peer-review › Journal article – Annual report year: 2016

Publication: Research - peer-review › Journal article – Annual report year: 2016

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

Lauridsen, Martin Mehl; Rechberger, Christian (Supervisor); Knudsen, Lars Ramkilde (Supervisor) / Design and Analysis of Symmetric Primitives. Kgs. Lyngby : Technical University of Denmark (DTU), 2016. 213 p. (DTU Compute PHD-2015; No. 382).
Publication: Research › Ph.D. thesis – Annual report year: 2016

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

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For; Ip, Ho Shing / PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks.

Tiessen, Tyge / Polytopic Cryptanalysis.

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

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

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

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

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

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

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

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

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

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

Lamberger, Mario; Mendel, Florian; Schläffer, Martin; Rechberger, Christian; Rijmen, Vincent / The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. 
Publication: Research - peer-review › Journal article – 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; Sanadha, Somitra Kumar / Cryptanalysis of SIMON Variants with Connections. 
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Banik, Subhadeep; Chattopadhyay, Anupam; Chowdhury, Anusha / Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013. 
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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

Andreeva, Elena; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Mouha, Nicky; Yasuda, Kan / How to Securely Release Unverified Plaintext in Authenticated Encryption. 
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014
Græsbøll, Kaare; Kirkeby, Carsten; Bødker, Rene; Stockmarr, Anders; Christiansen, Lasse Engbo; Lind, Peter / The range of attraction for light traps catching Culicoides biting midges. 2013. Poster session presented at EDENext Annual Meeting, Barcelona, Spain. Publication: Research - peer-review › Poster – Annual report year: 2013

Kirkeby, Carsten; Græsbøll, Kaare; Stockmarr, Anders; Christiansen, Lasse Engbo; Bødker, Rene / The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae). In: Parasites & Vectors, Vol. 6, No. 67, 2013. Publication: Research - peer-review › Journal article – Annual report year: 2013

Abdelraheem, Mohamed Ahmed Awadelkareem Mohamed Ahmed; Knudsen, Lars Ramkilde (Main supervisor); Zenner, Erik (Supervisor); Leander, Gregor (Supervisor) / Cryptanalysis of Some Lightweight Symmetric Ciphers. Kgs. Lyngby: Technical University of Denmark (DTU), 2012. 123 p. Publication: Research › Ph.D. thesis – Annual report year: 2013

Bogdanov, Andrey; Kavun, Elif Bilge; Tischhauser, Elmar; Yalcin, Tolga / Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks. International Conference on Reconfigurable Computing and FPGAs (ReConFig) 2012. IEEE, 2012. Publication: Research - peer-review › Article in proceedings – Annual report year: 2013