Cyber Security - Publications - DTU Orbit (08/06/2018)

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

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

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

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

Meng, Weizhi; Choo, Kim-Kwang Raymond; Furnell, Steven; Vasilakos, Athanasios V.; Probst, Christian W. / Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined 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
Publication: Research - peer-review › Conference article – Annual report year: 2017

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

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 › Book chapter – Annual report year: 2017

Publication: Research › Ph.D. thesis – Annual report year: 2017

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. Kgs. Lyngby : Technical University of Denmark (DTU), 2017. 272 p. (DTU Compute PHD-2016; No. 434).
Publication: Research › Ph.D. thesis – Annual report year: 2017

Publication: Research - peer-review › Book chapter – Annual report year: 2017

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 › Article in proceedings – 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

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. / Modelling 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 › Ph.D. thesis – Annual report year: 2016
Lauridsen, Martin Mehl; 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

Elaswad, Othoman; Jensen, Christian D. / Identity management for e-government Libya as a case study.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

Albrecht, Martin; Grassi, Lorenzo; Rechberger, Christian; Roy, Arnab; Tiessen, Tyge / MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity.
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.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

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

Helke, Steffen; Kammüüniidt kller, Florian; Probst, Christian W. / Secure Refactoring with Java Information Flow.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Jiang, Lijun; Meng, Weizhi / Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities.
Publication: Research - peer-review › Book chapter – Annual report year: 2017


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; Sanadghy, 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: 2014

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

Ideguchi, Kota; Tischhauser, Elmar Wolfgang; Preneel, Bart / Internal differential collision attacks on the reduced-round Grøstl-0 hash function.
Publication: Research - peer-review › Journal article – Annual report year: 2014

Bogdanov, Andrey; Dobraunig, Christoph; Eichlseder, Maria; Lauridsen, Martin Mehl; Mendel, Florian; Schläffer, Martin; Tischhauser, Elmar Wolfgang / Key Recovery Attacks on Recent Authenticated Ciphers.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Alippi, Cesare; Bogdanov, Andrey; Regazzoni, Francesco / Lightweight cryptography for constrained devices.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Wen, Long; Wang, Meiqin; Bogdanov, Andrey; Chen, HuaiFeng / Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard.
Publication: Research - peer-review › Journal article – Annual report year: 2014

Albrecht, Martin Roland; Fitzpatrick, Robert; Göpfert, Florian / On the Efficacy of Solving LWE by Reduction to Unique-SVP.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Blondeau, Celine; Bogdanov, Andrey; Wang, Meiqin / On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers.
Wang, Qingju; Gu, Dawu; Rijmen, Vincent; Liu, Ya; Chen, Jiazhe; Bogdanov, Andrey / **Improved Impossible Differential Attacks on Large-Block Rijndael.**
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Andreeva, Elena; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Tischhauser, Elmar Wolfgang; Yasuda, Kan / **Parallelizable and Authenticated Online Ciphers.**
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Knudsen, Lars Ramkilde (Editor); Wu, Huapeng (Editor) / **Selected Areas in Cryptography : 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers.**
Publication: Research › Book – Annual report year: 2013

Borghoff, Julia; Knudsen, Lars Ramkilde; Leander, Gregor; Thomsen, Søren Steffen / **Slender-Set Differential Cryptanalysis.**
Publication: Research - peer-review › Journal article – Annual report year: 2013

Bogdanov, Andrey; Knezevic, Miroslav; Leander, Gregor; Toz, Deniz; Varici, Kerem; Verbauwhede, Ingrid / **SPONGENT: The Design Space of Lightweight Cryptographic Hashing.**
Publication: Research - peer-review › Journal article – Annual report year: 2013

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).**
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.**
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