Cyber Security - Publications - DTU Orbit (11/05/2018)

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

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

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

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

Towards False Alarm Reduction using Fuzzy If-Then Rules for Medical Cyber Physical Systems. / Li, Wenjuan; 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, Qingju; Wang, Yu; Han, Jinguang.
Publication: Research - peer-review › Journal article – 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

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

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

A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords. / Meng, Weizhi; Li, Wenjuan; Lee, Wang; Jiang, Lijun; Zhou, Jianying.
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: 2018

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; Li, 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

JFCGuard: 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: 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 indiffrerentiable 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: Cryptology 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).
Publication: Research › Ph.D. thesis – Annual report year: 2016

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


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

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

The range of attraction for light traps catching Culicoides biting midges. / Græsbøll, Kaare; Kirkeby, Carsten; Bødker, Rene; Stockmarr, Anders; Christiansen, Lasse Engbo; Lind, Peter.
2013. Poster session presented at EDENext Annual Meeting, Barcelona, Spain.
Publication: Research - peer-review › Poster – Annual report year: 2013

The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae). / Kirkeby, Carsten; Græsbøll, Kaare; Stockmarr, Anders; Christiansen, Lasse Engbo; Bødker, Rene.
Publication: Research - peer-review › Journal article – Annual report year: 2013

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

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