Cyber Security - Publications - DTU Orbit (25/03/2018)

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

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. / Kölbl, Stefan; Roy, Amab.
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.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

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

Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-Based Systems. / Chauhan, Muhammad Aufeef; Probst, Christian W.
Publication: Research - peer-review › Book chapter – Annual report year: 2017

Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries. / Elaswad, Othoman; Jensen, Christian D. (Main supervisor).
Publication: Research › Ph.D. thesis – Annual report year: 2017

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

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

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

Do we educate engineers that can engineer? / Nyborg, Mads; Probst, Christian W. Proceedings of the 13th International CDIO Conference. 2017. p. 12. Publication: Research - peer-review › Article in proceedings – Annual report year: 2017


Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. / Li, Wenjuan; Meng, Weizhi; Kwok, Lam-For; IP, Horace H.S. In: Journal of Network and Computer Applications, Vol. 77, 2017, p. 135-145. Publication: Research - peer-review › Journal article – Annual report year: 2017


Evaluating challenge-based trust mechanism in medical smartphone networks: an empirical study. / Meng, Weizhi; Fei, Fei; Li, Wenjuan; Au, Man Ho. Proceedings of 2017 IEEE Global Communications Conference . IEEE, 2017. p. 6 pp. (Globecom 2017 - 2017 Ieee Global Communications Conference). Publication: Research - peer-review › Article in proceedings – Annual report year: 2018


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 indifferentiable compression functions from the PGV compression functions. / Gauravaram, P.; Bagheri, Nasour; Knudsen, Lars Ramkilde.
Conditional differential cryptanalysis of 105 round Grain v1. / Banik, Subhadeep.
In: Cryptography 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

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

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

Introducing E-Government in Developing Countries Analysis of Egyptian e-Government Services. / Elaswad, Othoman; Jensen, Christian D.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks. / Li, Wenjuan ; Meng, Weizhi; Kwok, Lam-For ; Ip, Ho Shing .
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

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

Round Gating for Low Energy Block Ciphers. / Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco; Isobe, Takanori; Hiwatari, Harunaga; Akishita, Toru.
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 › Book chapter – 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: 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
Improved cryptanalysis of the block cipher KASUMI. / Jia, Keting; Li, Leibo; Rechberger, Christian; Chen, Jiazhe; Wang, Xiaoyun.
Publication: Research - peer-review › Conference article – Annual report year: 2013

Improved Impossible Differential Attacks on Large-Block Rijndael. / Wang, Qingju; Gu, Dawu; Rijmen, Vincent; Liu, Ya; Chen, Jiazhe; Bogdanov, Andrey.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

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

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

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; Bædker, 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; Bædker, 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