A fog-based privacy-preserving approach for distributed signature-based intrusion detection.

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

Cyber-physical architecture assisted by programmable networking.

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

Detecting insider attacks in medical cyber–physical networks based on behavioral profiling.

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

Editorial of special issue on mobile networks and devices security, privacy and trust.

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

Enhancing Intelligent Alarm Reduction for Distributed Intrusion Detection Systems via Edge Computing.

Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

Evaluating the Impact of Juice Filming Charging Attack in Practical Environments.

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.

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

Improved meet-in-the-middle attacks on reduced-round Piccolo.

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


Publication: Research - peer-review › Journal article – Annual report year: 2018
Meng, Weizhi / **Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling.**
Publication: Communication › Journal article – Annual report year: 2018

Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco; Isobe, Takanori; Hiwatari, Harunaga; Akishita, Toru / **Inverse Gating for Low Energy Encryption.**
Publication: Research - peer-review › Article in proceedings – 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

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: 2018

Yermakov, Oleh Y.; Permyakov, Dmitriy V.; Dmitriev, Pavel A.; Samusev, Anton K.; Iorsh, Ivan V.; Lavrinenko, Andrei V.; Bogdanov, Andrey A.; Zayats, Anatoly V. / **Plasmonic anisotropic metasurfaces: from far-field measurements to near-field properties.**
Publication: Research - peer-review › Article in proceedings – 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

Sahay, Rishikesh; Sepúlveda Estay, Daniel Alberto / **Work Package 2 Report - Cyber resilience for the shipping industry.**
Publication: Research › Report – 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 Aufeef; 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, Othuman; 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

Perno, Jason; Probst, Christian W. / Behavioural Profiling in Cyber-Social Systems.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2018

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.


Boura, Christina; Canteaut, Anne; Knudsen, Lars Ramkilde; Leander, Gregor / Reflection ciphers. In: Designs, Codes and Cryptography, Vol. 82, 2017, p. 3-25.


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.

Banik, Subhadeep; Bogdanov, Andrey; Regazzoni, Francesco / Atomic-AES: A compact implementation of the AES encryption/decryption core.
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
Coron, Jean-Sébastien; Roy, Amab; Vivek, Srinivas / Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures.
Publication: Research - peer-review › Journal article – Annual report year: 2015

Banik, Subhadeep; Jha, Sonu / How Not to Combine RC4 States.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Abdelraheem, Mohamed Ahmed; Alizadeh, Javad; Alkhzaimi, Hoda A.; Aref, Mohammad Reza; Bagheri, Nasour; Gauravaram, Praveen / Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Lauridsen, Martin Mehl; Rechberger, Christian / Linear Distinguishers in the Key-less Setting: Application to PRESENT.
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 › Book chapter – Annual report year: 2015

Ankele, Ralph; Köbl, Stefan; Rechberger, Christian / State-Recovery Analysis of Spritz.
Lamberger, Mario; Mendel, Florian; Schläffer, Martin; Rechberger, Christian; Rijmen, Vincent / The Rebound Attack and Subspace Distinguishers: Application to Whirlpool.

Abdelraheem, Mohamed Ahmed A. M. A.; Beelen, Peter ; Bogdanov, Andrey; Tischhauser, Elmar Wolfgang / Twisted Polynomials and Forgery Attacks on GCM.

Bogdanov, Andrey; Mendel, Florian; Regazzoni, Francesco; Rijmen, Vincent; Tischhauser, Elmar / ALE: AES-based lightweight authenticated encryption.

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.

Banik, Subhadeep; Chattopadhyay, Anupam; Chowdhury, Anusha / Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013.

Andreeva, Elena; Bogdanov, Andrey; Luykx, Atul; Mennink, Bart; Mouha, Nicky; Yasuda, Kan / How to Securely Release Unverified Plaintext in Authenticated Encryption.

Ideguchi, Kota; Tischhauser, Elmar Wolfgang; Preneel, Bart / Internal differential collision attacks on the reduced-round Grøstl-0 hash function.

Bogdanov, Andrey; Dobrindig, 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: 2015

Publication: Research - peer-review › Journal article – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Journal article – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Publication: Research › Patent – 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