Cyber Security - Publications - DTU Orbit (28/06/2018)
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

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

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 › Journal article – Annual report year: 2017

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

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

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

Publication: Research - peer-review › Journal article – Annual report year: 2017
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

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

Publication: Research - peer-review › Journal article – Annual report year: 2017

Publication: Research - peer-review › Journal article – Annual report year: 2017

Publication: Research - peer-review › Journal article – Annual report year: 2017

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. 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 › 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 › Book chapter – 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

Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

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; Sanadhya, 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

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

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

Bogdanov, Andrey; Tischhauser, Elmar / On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Khovratovich, Dmitry; Nikolić, Ivica; Rechberger, Christian / Rotational Rebound Attacks on Reduced Skein.
Publication: Research - peer-review › Journal article – Annual report year: 2014

Vejre, Philip S.; Bogdanov, Andrey / Route 66: Passively Breaking All GSM Channels.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Khovratovich, Dmitry; Rechberger, Christian / The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Andreeva, Elena; Bogdanov, Andrey; Mennink, Bart / Towards understanding the known-key security of block ciphers.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Bogdanov, Andrey; Geng, Huizheng; Wang, Meiqin; Wen, Long; Collard, Baudoin / Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

Knudsen, Lars Ramkilde (Inventor) / Dynamic encryption method.
Publication: Research › Patent – Annual report year: 2013

Bogdanov, Andrey; Moradi, Amir; Yalcin, Tolga / Efficient and side-channel resistant authenticated encryption of FPGA bitstreams.
Proceedings of 2012 International Conference on Reconfigurable Computing and FPGAs (ReConFig). IEEE, 2013.
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Bilgin, Begul; Bogdanov, Andrey; Knezevic, Miroslav; Mendel, Florian; Wang, Qingju / Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware.
Jia, Keting; Li, Leibo; Rechberger, Christian; Chen, Jiazhe; Wang, Xiaoyun / Improved cryptanalysis of the block cipher KASUMI.
Publication: Research - peer-review › Conference article – Annual report year: 2013

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, Atil; Mennink, Bart; Tischhauser, Elmar Wolfgang; Yasuda, Kan / Parallelizable and Authenticated Online Ciphers.
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

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