Rubio-Hernan, Jose; Sahay, Rishikesh; De Cicco, Luca; Garcia-Alfaro, Joaquin / Cyber-physical architecture assisted by programmable networking. In: Internet Technology Letters, 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. In: Science China Information Sciences, Vol. 61, No. 3, 032110, 2018.


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, Othoman; 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


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 Forging 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

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

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

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