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

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

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.
Publication: Research - peer-review > Book chapter – Annual report year: 2017


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
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

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; Dobbraunig, 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, Huiaifeng / 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

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

Bilgin, Begul; Bogdanov, Andrey; Knezevic, Miroslav; Mendel, Florian; Wang, Qingju / Fides: LightweightAuthenticated Cipher with Side-Channel Resistance for Constrained Hardware.