Cyber Security - Research outputs - DTU Orbit (28/07/2019)


Sukham, Johneph ; Takayama, Osamu ; Mahmoodi, Maryam ; Sychev, Stanislav ; Bogdanov, Andrey ; Tavassoli, Seyed Hassan ; Lavrinienko, Andrei V ; Malureanu, Radu. / Investigation of effective media applicability for ultrathin multilayer structures. In: Nanoscale. 2019 ; Vol. 11, No. 26. pp. 12582-12588.


Singh, Saurabh ; Ra, In-Ho ; Meng, Weizhi ; Kaur, Maninder ; Cho, Gi Hwan. / SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. In: International Journal of Distributed Sensor Networks. 2019 ; Vol. 15, No. 4.


Walla, Frederik ; Bürkle, Florian ; Sinev, Ivan ; Wiecha, Matthias M. ; Mecklenbeck, Nicolas ; Ladutenko, Konstantin ; Malureanu, Radu ; Komissarenko, Filipp ; Lavrinenko, Andrei ; Bogdanov, Andrey ; Soltani, Amin ; Roskos, Hartmut G. / Near-Field Observation of Guided-Mode Resonances on a Metasurface via Dielectric Nanosphere Excitation. In: ACS Photonics. 2018 ; Vol. 5, No. 11. pp. 4238-4243.


Rubio-Hernan, Jose ; Sahay, Rishikesh ; De Cicco, Luca ; Garcia-Alfaro, Joaquin. / Cyber-physical architecture assisted by programmable networking. In: Internet Technology Letters. 2018 ; Vol. 1, No. 4.


Dmitry, Pidgayko ; Sinev, Ivan ; Permyakov, Dmitry ; Samusev, Anton ; Sychev, Stanislav ; Bogdanov, Andrey ; Lavrinenko, Andrey ; Rutckaia, Viktoria; Schilling, Joerg. / Direct imaging of isofrequency contours in all-dielectric optical metasurface. In: Journal of Physics: Conference Series. 2018 ; Vol. 1092, No. 1.


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. 2018 ; Vol. 61, No. 3.


Liu, Ya ; Cheng, Liang ; Liu, Zhiqiang ; Li, Wei ; Wang, Qingju ; Gu, Dawu. / Improved meet-in-the-middle attacks on reduced-round Piccolo. In: Science China Information Sciences. 2018 ; Vol. 61, No. 3.


Isobe, Takanori (Inventor) ; Bogdanov, Andrey (Inventor). / Encryption device, encryption method, decryption device, and decryption method. IPC No.: G09C1/00; H04L9/00; H04L9/06. Patent No.: US2017294148 . Oct 12, 2017.


Bour, Christina ; Canteaut, Anne ; Knudsen, Lars Ramkilde ; Leander, Gregor. / Reflection ciphers. In: Designs, Codes and Cryptography. 2017 ; Vol. 82. pp. 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. pp. 331-334


Coron, Jean-Sébastien ; Roy, Arnab ; Vivek, Srinivas. / Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures. In: Journal of Cryptographic Engineering. 2015 ; Vol. 5, No. 2. pp. 73-83.


Bogdanov, Andrey ; Dobbraug, Christoph ; Eichlseder, Maria ; Lauridsen, Martin Mehl ; Mendel, Florian ; Schläffer, Martin ; Tischhauser, Elmar Wolfgang. / Key Recovery Attacks on Recent Authenticated Ciphers. 3rd International Conference on Cryptology and Information Security in Latin America. Springer, 2014. pp. 274-287 (Lecture Notes in Computer Science, Vol. 8895).


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.


Græsbøll, Kaare; Kirkeby, Carsten; Bedker, Rene; Stockmarr, Anders; Christiansen, Lasse Engbo; Lind, Peter. / *The range of attraction for light traps catching Culicoides biting midges*. Poster session presented at EDENext Annual Meeting, Barcelona, Spain. 1 p.

Kirkeby, Carsten; Græsbøll, Kaare; Stockmarr, Anders; Christiansen, Lasse Engbo; Bedker, Rene. / *The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae)*. In: Parasites & Vectors. 2013; Vol. 6, No. 1.

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.