Zagreb, Croatia, June 24 – 26, 2020
20th Central European Conference on Cryptology

Program

The conference is held at Hotel Westin, Izidora Kršnjavoga 1, Zagreb. All talks take place in the room Maksimir, at ground floor on the right.

Wednesday, June 24, 2020

9:00 - 9:30	Registration
9:30 - 9:45	Opening and Announcements
9:45 - 10:35	Lilya Budaghyan: *Optimal cryptographic functions solving hard mathematical problems*
10:40 - 11:00	Hayder Hashim, Alexandra Molnár, Szabolcs Tengely: *Cryptanalysis of ITRU*
11:05 - 11:30	coffee break
11:30 - 11:55	Gennady Khalimov, Yevgen Kotukh, Svitlana Khalimova: *Encryption scheme based on the extension of automorphism group of the Hermitian function field*
12:00 - 12:20	Liliya Kraleva, Raluca Posteuca, Vincent Rijmen: *Cryptanalysis of the permutation based algorithm SpoC*
12:30 - 14:00	lunch
14:00 - 14:45	Nicolas T. Courtois, Marek Grajek: *On weak rotors, latin squares, linear algebraic representations, invariant differentials and cryptanalysis of Enigma*
14:50 - 15:10	Lyudmila Kovalchuk, Mariia Rodinko, Roman Oliynykov: *Security of Poseidon hash function against linear and differential attacks with respect to field operations*
15:15 - 15:45	coffee break
15:45 - 16:15	Laszlo Csirmaz: *Multipartite secret sharing revisited*
16:20 - 16:30	Anatolii Bessalov, Lyudmila Kovalchuk, Nataliia Kuchynska, Oleksandr Telizhenko: *Algorithm for short messages encryption on twisted Edward curves*

Thursday, June 25, 2020

9:00 - 9:50	Marcin Pawłowski: *Quantum random number generators*
9:55 - 10:10	Ádám Vécsi, Attila Pethő: *Formal language Identity-based Cryptography*
10:15 - 10:40	Clemens Heuberger, Dunja Pucher: *An algorithm for optimal joint expansion with odd digits*
10:45 - 11:15	coffee-break
11:15 - 11:40	Nicolas T. Courtois, Matteo Abbondati, Aidan Patrick: *On reducing annihilation degree inside nonlinear invariant attacks on T-310 and DES*
11:45 - 12:10	Pavol Zajac, Alena Bednarikova: *Experimental algebraic differential cryptanalysis of SPN*
12:20	conference photo
12:30 - 14:00	lunch
14:00 - 15:00	Elena Andreeva: *Forkciphers: New cryptographic primitives*
15:05 - 15:30	István András Seres, Péter Burcsi: *A note on Low Order assumptions in RSA groups*
15:35 - 15:55	coffee break
15:55 - 16:15	Krisztián Dsupin, Szabolcs Tengely: *Discrete logarithm problem in some families of sandpile groups*
16:20 - 16:30	Victor Ruzhentsev: *Comparative analysis of ARX transformations*
16:35 - 16:55	Bohdan Kovalenko, Anton Kudin: *Evaluation and minimization of kleptography risks in cryptographic algorithms*
17:15 - 19:00	city sightseeing
19:00	conference dinner

Friday, June 26, 2020

9:00 - 10:00	Florian Mendel: *Authenticated Encryption*
10:05 - 10:25	Andreas Klinger, Stefan Wüller, Giulia Traverso, Ulrike Meyer: *Hierarchical and dynamic threshold Paillier cryptosystem without trusted dealer*
10:30 - 10:55	Reni Banov: *Computing minimal DNF of Boolean functions for digital implementations*
11:00 - 11:20	coffee-break
11:20 - 11:35	Peter Švec, Roderik Ploszek: *A review of encryption schemes used in modern ransomware*
11:40 - 11:55	Peter Špaček, Pavol Sobota: *Musipher: Hiding information in music composition*
12:00 - 12:30	rump session and CECC 2021 announcement
12:40 - 14:00	lunch