10^{th} Central European Conference on Cryptology

Programme

Thursday, 10 June.

9:00 - 9:10 **Openning**

9:10 - 10:00 Simon Blackburn
Group theory and cryptography

10:00 - 10:10 **Break**

10:00 - 10:35 Pavol Zajac
Algebraic cryptanalysis in practice

10:45 - 11:15 **Coffee break**

11:15 - 11:35 Sugata Gangopadhyay, Brajesh Kumar Singh
On second-order nonlinearities of some $\mathcal{D}_0$ type bent functions

11:35 - 11:55 Smile Markovski, Aleksandra Mileva, Vesna Dimitrova
Quasigroup String Transformations and Block Cipher Design

11:55 - 12:15 Vadym Fedyukovych
Committing with partial knowledge of group order

12:15 - 12:30 **Break**

12:30 - 12:50 János Folláth
Notes on a Family of Preimage-Resistant Functions

12:50 - 13:10 Michal Rjaško
Combining properties of cryptographic hash functions

13:15 - 15:00 **Lunch**

15:00 - 15:20 Viktoria Toth
The extension of collision and avalanche effect to pseudorandom k-ary sequences

15:20 - 15:40 Katalin Gyarmati
On binary lattices

15:40 - 16:00 Andrea Huszti
Security definitions for electronic exam systems

16:00 - 16:30 **Coffee break**

16:30 - 16:50 Marina Pudovkina
Differential attack on one family of block ciphers based on the SPN structure

16:50 - 17:10 Piotr Mroczkowski, Janusz Szmidt
The cube attack on stream cipher Trivium and quadraticity tests

17:10 - 18:10 **Poster session**

18:15 - 19:00 **Dinner**

Friday, 11 June.

9:00 - 9:50 Jerzy Kaczorowski
L-function and cryptography

9:50 - 10:00 **Break**

10:10 - 10:45 Martin Hlaváč
Attacking RSA-CRT with Montgomery, from Schindler to Fourier

10:35 - 11:05 **Coffee break**

11:05 - 11:25 Maciej Grześkowiak
Algorithm for generating primes p and q such that q divides $p^4 \pm p^3 + p^2 \pm p + 1$

11:25 - 11:45 Sedat Akleylek, Murat Cenk, Ferruh Özbudak
A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication

11:45 - 12:05 Urszula Romanczuk, Vasyl Ustimenko
On the similarity of two pairs of matrices and key exchange protocols

12:05 - 12:25 Vasyl Ustimenko, Aneta Wróblewska
On the key exchange via cubical polynomials

12:45 - **Bus to Poznań**

14:00 - **Lunch** (Faculty of Mathematics and Computer Science, Adam Mickiewicz University)

15:30 - 16:30 Marek Grajek
Roots of Victory

17:00 - 19:00 **Poznań - Old Town**

20:00 - 22:00 **Party - bonfire**

Saturday, 12 June.

9:00 - 9:20 Michal Rjaško, Martin Stanek
Attacking M&M Collective Signature Scheme

9:20 - 9:40 Konrad Durnoga
Applications of the Deniable Encryption Scheme

9:40 - 10:00 László Csirmaz, Péter Ligeti, Gábor Tardos
On infinite secret sharing schemes

10:00 - 10:10 **Break**

10:10 - 10:30 Krzysztof Chmiel, Anna Grocholewska-Czuryło, Janusz Stokłosa
Scalable involutional PP-1 block cipher for limited resources

10:30 - 10:50 Bernadin Ibrahimpašić
LUC vs KMOV

10:50 - 11:20 **Coffee break**

11:20 - 11:55 László Mérai
Pseudorandom binary sequences from elliptic curves

11:55 - 12:30 Krystian Matusiewicz
Groestl - a SHA-3 candidate

12:30 - 12:40 **Closing**

13:00 - **Lunch**