WartaCrypt'04

Preliminary programme

Thursday, 1 July.

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

9:10 - 10:00 **Gerhard Frey**
A First Step Towards Computations in Brauer Groups and Applications to data Security

10:00 - 10:30 **Coffee break**

10:30 - 10:50 **Wolfgang Lempken, Tran van Trung**
On Minimal Logarithmic Signatures for Finite Groups

10:50 - 11:10 **Tanja Lange**
Mathematical Countermeasures Against Side-Channel Attacks on ECC/HECC

11:10 - 11:30 **Katalin Gyarmati**
Inequalities Between Pseudorandom Measures

11:30 - 11:45 **Coffee break**

11:45 - 12:05 **María Isabel Gonzales Vasco, Rainer Steinwandt**
Chosen Ciphertext Attacks as Common Vulnerability of Some Group - and Polynomial - Based Encryption Schemes

12:05 - 12:25 **Marcin Gomułkiewicz, Mirosław Kutyłowski, Paweł Wlaź**
Fault Cryptanalysis for Breaking A5/1

12:25 - 12:45 **Otokar Grosek, Spyros S. Magliveras**
Is Rijndael Really Independent on the Field Polynomial?

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

15:00 - 15:50 **Mirosław Kutyłowski**
Rapid Mixing in Cryptographic protocols

15:50 - 16:30 **Coffee break**

16:30 - 16:50 **Jarosław Byrka**
Efficient User Removal in Broadcast Channel with Symmetric Encryption

16:50 - 17:10 **Dennis Hofheinz, Jörn Müller-Quade, Rainer Steinwandt**
On Modeling IND - CCA Security in Cryptographic Protocols

17:10 - 17:30 **Michał Ren**
Efficiency Considerations In Unconditionally Secure Communication by Public Discussion

19:00 - 21:00 **Party - bonfire**

Friday, 2 July.

9:00 - 9:50 **Stefan Dziembowski**
Introduction to the Bounded-Storage Model

9:50 - 10:30 **Coffee break**

10:30 - 10:50 **Laszlo Csirmaz, Gyula O.H. Katona**
On a model of identification

10:50 - 11:10 **Andrzej Grudka, Antoni Wojcik**
Quantum information splitting.

11:10 - 11:30 **Krzysztof Gołofit**
Efficient Hardware Implementation of Elliptic Curve Cryptosystems

11:30 - 11:45 **Coffee break**

11:45 - 12:05 **Dominic Bucerzan, Marius Gheorghita**
Henkos - a New Stream Cipher: Performance Analysis

12:05 - 12:25 **Zoltán Csajbók, József Ködmön**
The Implementation Of A New One-Way Function Based On Norm Form Equations In Java

12:25 - 12:45 **Jean-Camille Birget, Spyros S. Magliveras, Michal Sramka**
Wagner-Magyarik-like Public-Key Cryptosystem

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

15:00 - 15:20 **Tobias Straub**
How to Strengthen Certificate Enrollment

15:20 - 15:40 **Joanna Bissinger**
Watermarking Travelling Salseman Problem Solution

15:40 - 16:00 **Marcin Gogolewski, Mirosław Kutyłowski, Tomasz Łuczak**
Distributed Time-Stamping Boomerang Onions

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

16:30 - 16:50 **Lenka Fibíková**
Random Oracle Model and Analysis of Primitives of Cryptographic Scheme

16:50 - 17:10 **Krzysztof Nowak**
The Second Algorithm for Checking Normality of Boolean Functions

18:00 - **Dinner**

Saturday, 3 July.

9:00 - 9:20 **Łukasz Nitschke**
Interactive Key Generation Protocols

9:20 - 9:40 **Włodzimierz Chocianowicz, Jerzy Pejas**
Chaos In Cryptography

9:40 - 10:20 **Coffee break**

10:20 - 10:40 **Kamil Kulesza, Zbigniew Kotulski, Konrad Kulesza**
On mobile agents resistance to traffic analysis

10:40 - 11:00 **Marcin Serweciński**
Classification of boolean functions with respect to linear equivalence

12:00 - **Lunch**