

WEWoRC 2011 — Preliminary Program

All technical sessions will take place in Bauhausstraße 11, Lecture Room S15.

Tuesday, July 19:

19:00-20:00: Conference Reception ("Oberlichtsaal", Geschwister-Scholl-Straße 8)

Wednesday, July 20:

08:30—09:20: Check-in

09:20—09:30: Welcome Remarks

09:30—10:30: Session: Cryptanalysis I

- RSA Vulnerabilities with Small Prime Difference
(*Marián Kühnel*)
- Mars Attacks! Revisited!
(*Michael Gorski, Thomas Knapke, Eik List, Stefan Lucks and Jakob Wenzel*)

10:30—11:00: Coffee Break

11:00—12:00 Invited Talk I: The Practice of Cryptography
(*Heike Neumann, NXP Semiconductors*)

12:00—13:45 Lunch Break

13:45—15:45 Session: Foundations of Cryptography I

- Group Homomorphic Encryption and Beyond: Characterizations, Impossibility Results, and Applications
(*Frederik Armknecht, Stefan Katzenbeisser and Andreas Peter*)
- On the role of expander graphs in key predistribution schemes for wireless sensor networks
(*Michelle Kendall and Keith Martin*)
- An Information-Theoretic and Computational Complexity Security Analysis of a Randomized Stream Cipher Model
(*Miodrag J. Mihajjevi and Hideki Imai*)
- The Cryptographic Power of Random Selection
(*Matthias Krause and Matthias Hamann*)

15:45—16:15 Coffee Break

16:15—17:35 Short Paper Session

- Fast parallel keyed hash functions based on chaotic maps (PKHC)
(*Mahmoud M. Maqableh*)
- Block Ciphers Based on Wavelet Decomposition of Splines
(*Alla Levina*)
- New Universal Hash Functions
(*Aysajan Abidin*)
- Cryptanalysis of the Light-Weight Cipher A2U2
(*Mohamed Ahmed Abdelraheem, Julia Borgho, Erik Zenner*)

19:00—20:30 Bauhaus Walk (will start at Geschwister-Scholl-Straße 8)

Thursday, July 21:

09:00—10:30: Session: Cryptanalysis II

- Cryptanalysis of TWIS Block Cipher
(*Onur Kocak and Nese Oztop*)
- Breaking DVB-CSA
(*Erik Tews, Julian Wälde and Michael Weiner*)
- Critical attacks in code-based cryptography
(*Robert Niebuhr*)

10:30—11:00: Coffee Break

11:00—12:00 Session: Foundations of Cryptography II

- A taxonomy of non-cooperatively computable functions
(*Yona Raekow and Konstantin Ziegler*)
- The preimage security of double-block-length compression functions
(*Frederik Armknecht, Ewan Fleischmann, Matthias Krause, Jooyoung Lee, Martijn Stam and John Steinberger*)

12:00—13:45 Lunch Break

13:45—15:45 Session: Efficient Implementations

- Algorithmically determining the optimum polynomial multiplier in GF (2^k)
(*Zoya Dyka and Peter Langendoerfer*)
- Efficient implementation of code-based identification schemes
(*Pierre-Louis Cayrel, Sidi Mohamed El Yousfi Alaoui, Felix Günther, Gerhard*)
- Improved Software Implementation of DES Using CUDA and OpenCL
(*D. Noer, A.P. Engsig-Karup and E. Zenner*)
- Full Lattice Basis Reduction on Graphics Cards
(*Timo Bartkewitz*)

15:45—16:15 Coffee Break

16:15—17:45 Session: New Cryptosystems

- Intractability of a Linear Diophantine Equation Discrete LogProblem (LDEDLP) based Asymmetric Cryptosystem -The AAB Cryptosystem
(*M.R.K.Ariffin and N.A.Abu*)
- Gamma-MAC [H, P] — A new universal MAC scheme
(*Ewan Fleischmann, Christian Forler and Stefan Lucks*)
- A new secure sketch based on the discrete logarithm problem
(*Max Grosse and Stefan Lucks*)

19: 30—Late: Conference Dinner

Friday, July 22:

09:00—10:30: Session on Lightweight Cryptosystems

- A Lightweight Pseudorandom Number Generator For EPC Class 1Gen2 RFID Tags
(*Kalikinkar Mandal, Xinxin Fan, and Guang Gong*)
- Related-key attacks on the full GOST block cipher with 2 or 4 related keys
(*Marina Pudovkina and George Khoruzhenko*)
- On the Security of Hummingbird-2 against Side Channel Cube Attacks
(*Xinxin Fan, Honggang Hu, and Guang Gong*)

10:30—11:00: Coffee Break

11:00—12:00: Invited Talk II: Key Exchange – 35 Years and still Rolling
(*Marc Fischlin, TU Darmstadt*)

12:00—13:30: Final Lunch Break