Submittee: Petr Lisonek
Date Submitted: 2013-11-14 15:28
Title: Selected Areas in Cryptography 2013
Event Type: Conference-Workshop

Location:
IRMACS, Simon Fraser University, Burnaby, BC, Canada

Dates:
August 14-16, 2013

Topic:
Cryptography: Lattices; Discrete logarithms; Stream ciphers and authenticated encryption; Post-quantum cryptography; White-box cryptography; Block ciphers; Elliptic curves, Pairings and RSA; Hash functions and MACs; Side-channel attacks

---

Methodology:
This 2.5-day conference featured 4 invited talks as well as 26 accepted papers, each of which was presented as a talk. The 26 accepted papers were selected from 98 refereed submissions. The program committee had 51 members who also engaged subreviewers in the refereeing process.

Objectives Achieved:
SAC 2013 was the 20th anniversary edition of the Selected Areas in Cryptography conference series. To celebrate the anniversary, the conference was extended from its usual format by an extra half day with two additional invited speakers. The Proceedings of the conference will be published by Springer Verlag in the Lecture Notes in Computer Science series.

Organizers:
Lange, Tanja, Technische Universiteit Eindhoven, The Netherlands // Lauter, Kristin, Microsoft Research, USA // Lisonek, Petr, Simon Fraser University

---

Speakers:
The talks are listed in the order in which they were presented at the conference. Slides for all talks are available at: http://sac2013.irmacs.sfu.ca/ */// * INVITED TALKS: Paulo S. M. L. Barreto (University of Sao Paulo, Brazil), The Realm of the Pairings // Douglas R. Stinson (University of Waterloo, Canada), Key Distribution in Wireless Sensor Networks // Antoine Joux (CryptoExperts and Universite de Versailles Saint-Quentin-en-Yvelines, France), Revisiting Discrete Logarithms in Small/Medium Characteristic Finite Fields // Hugh C. Williams (The Tutte Institute for Mathematics and Computing, Canada), The Tutte Institute for Mathematics and Computing // Anne Canteaut (INRIA Paris-Rocquencourt, France), Similarities between Encryption and Decryption: How far can

we go? *///* ACCEPTED CONTRIBUTED PAPERS: Feng Zhang, Yanbin Pan and Gengran Hu (Chinese Academy of Sciences, China), A Three-Level Sieve Algorithm for the Shortest Vector Problem // Rachid El Bansarkhani and Johannes Buchmann (Technische Universitaet Darmstadt, Germany), Improvement and Efficient Implementation of a Lattice-based Signature Scheme // Thomas Poppelmann and Tim Guneysu (Ruhr-University Bochum, Germany), Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware // Jung Hee Cheon, Taechan Kim and Yong Soo Song (Seoul National University, Korea), A Group Action on Zpx and the Generalized DLP with Auxiliary Inputs // Faruk Gologlu, Robert Granger, Gary McGuire and Jens Zumbraegel (University College Dublin, Ireland), Solving a 6120-bit DLP on a Desktop Computer // Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe and Masakatu Morii (Hiroshima University, Japan and Kobe University, Japan), How to Recover Any Byte of Plaintext on RC4 // Dmitry Khovratovich and Christian Rechberger (University of Luxembourg and Technical University of Denmark, Denmark), The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE // Hongjun Wu and Bart Preneel (Nanyang Technological University, Singapore and KU Leuven, Belgium), AEGIS: A Fast Authenticated Encryption Algorithm // Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen and Bo-Yin Yang (Universit e de Lille, France and National Taiwan University, Taiwan and Technische Universiteit Eindhoven, The Netherlands and Academia Sinica, Taiwan), Fast Exhaustive Search for Quadratic Systems in F2 on FPGAs // Thomas Eisenbarth, Ingo von Maurich and Xin Ye (Worcester Polytechnic Institute, USA and Ruhr University Bochum, Germany), Faster Hash-based Signatures with Bounded Leakage // Cecile Delerablee, Tancrede Lepoint, Pascal Paillier and Matthieu Rivain (CryptoExperts, France and Ecole Normale Superieure, France), White-Box Security Notions for Symmetric Encryption Schemes // Tancrede Lepoint, Matthieu Rivain, Yoni De Mulder, Peter Roelse and Bart Preneel (CryptoExperts, France and Ecole Normale Superieure, France and KU Leuven, Belgium and Irdeto B.V., The Netherlands), Two Attacks on a White-Box AES Implementation // Thierry P. Berger, Marine Minier and Gael Thomas (Universite de Limoges, France and Universite de Lyon, France), Extended Generalized Feistel Networks using Matrix Representation // Ryad Benadjila, Jian Guo, Victor Lomne and Thomas Peyrin (Agence nationale de la securite des systemes d'information, France and Nanyang Technological University, Singapore), Implementing Lightweight Block Ciphers on x86 Architectures // Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen and Baudoin Collard (Technical University of Denmark, Denmark and Shandong University, China and Universite Catholique de Louvain, Belgium), Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA // Sujoy Sinha Roy, Frederik Vercauteren and Ingrid Verbauwhede (KU Leuven, Belgium), High Precision Discrete Gaussian Sampling on FPGAs // Johannes Buchmann, Daniel Cabarcas, Florian Gopfert, Andreas Hulsing and Patrick Weiden (Technische Universitaet Darmstadt, Germany), Discrete Ziggurat: A Time-Memory Trade-off for Sampling from a Gaussian Distribution over the Integers // Yuan Ma, Zongbin Liu, Wuqiong Pan and Jiwu Jing (Chinese Academy of Sciences, China), A high-speed elliptic curve cryptographic processor for generic curves over GF(p) // Joppe W. Bos, Craig Costello and Michael Naehrig (Microsoft Research, USA), Exponentiating in Pairing Groups // Christophe Doche, Daniel Sutantyo (Macquarie University, Australia), Faster Repeated Doublings on Binary Elliptic Curves // Joppe W. Bos, Peter L. Montgomery, Daniel Shumow and Greg Zaverucha (Microsoft Research, USA), Montgomery Multiplication Using Vector Instructions // Yu Sasaki and Lei Wang (NTT Secure Platform Laboratories, Japan and Nanyang Technological University, Singapore), Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5 // Charles Bouillaguet and Bastien Vayssiere (University of Lille, France and University of Versailles, France), Provable Second Preimage Resistance Revisited // Jeremy Jean, Maria Naya-Plasencia and Thomas Peyrin (Ecole Normale Superieure, France and INRIA Paris-Rocquencourt, France and Nanyang Technological University, Singapore), Multiple Limited-Birthday Distinguishers and Applications // Aurelie Bauer, Eliane Jaulmes, Emmanuel Prouff and Justine Wild (French Network and Information Security Agency, France), Horizontal Collision Correlation Attack on Elliptic Curves // David Oswald, Daehyun Strobel, Falk Schellenberg, Timo Kasper and Christof Paar (Ruhr-University Bochum, Germany), When Reverse-Engineering Meets Side-Channel

Analysis--Digital Lockpicking in Practice

Links:
http://sac2013.irmacs.sfu.ca/