Fast Software Encryption 2017

Program

All technical sessions and coffee breaks take place in the Hall D7 at Tokyo International Forum. Lunch is available in the Hall D5.
All talks are 20 minutes including questions unless indicated otherwise.

Sunday 5 March 2017

18:00 - 20:00 **Welcome Reception and Registration**
at the Lounge (G Block, 7th floor), Tokyo International Forum

Monday 6 March 2017

9:00 - **Registration**
9:50 - 10:00 **Welcome Remarks**

Session I - Cryptanalysis: Hash functions (*10:00 - 11:00, Chair: Jian Guo)*

10:00-10:20 **Cryptanalysis of Haraka**
Jérémy Jean
10:20-10:40 **New techniques for trail bounds and application to differential trails in Keccak**
Silvia Mella, Joan Daemen, Gilles Van Assche
10:40-11:00 **SymSum: Symmetric-Sum Distinguishers Against Round Reduced SHA3**
Dhiman Saha, Sukhendu Kuila, Dipanwita Roy Chowdhury

11:00 - 11:30 **Coffee Break** (30 min)

Session II - Invited Talk I (*11:30 - 12:30, Chair: María Naya-Plasencia)*

11:30-12:30 **Innovations in permutation-based encryption and/or authentication**
Imagine there's no block ciphers, it's easy if you try:-)
Joan Daemen (Radboud University, Netherlands and STMicroelectronics, Belgium)

12:30-13:45 **Lunch Break** (75 min)

Session III - Building blocks (*13:45 - 15:35, Chair: Christina Boura)*

13:45-14:05 **Lightweight Diffusion Layer: Importance of Toeplitz Matrices**
Sumanta Sarkar, Habeeb Syed

14:05-14:25 **Direct construction of quasi-involutory recursive-like MDS matrices from 2-cyclic codes**
Victor Cauchois, Pierre Loidreau, Nabil Merkiche

14:25-14:45 **Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices**
Chaoyun Li, Qingju Wang

14:45-15:05 **Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog**
Léo Perrin, Aleksei Udovenko

15:05-15:15 **A Note on 5-bit Quadratic Permutations' Classification** (short talk: 10 minutes)
Dusan Bozilov, Begül Bilgin, Haci Ali Sahin

15:15-15:35 **Analysis of Software Countermeasures for Whitebox Encryption**
Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Martin Bjerregaard Jepsen

15:35-16:05 **Coffee Break** (30 min)

Session IV - Cryptanalysis: Block ciphers (*16:05 - 17:45, Chair: Lei Wang)*

16:05-16:25 **Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs**
Alex Biryukov, Dmitry Khovratovich, Léo Perrin

16:25-16:45 **Practical Key-Recovery Attack on MANTIS5**
Christoph Dobraunig, Maria Eichlseder, Daniel Kales, Florian Mendel

16:45-17:05 **Chosen-Key Distinguishers on 12-Round Feistel-SP and 11-Round Collision Attacks on Its Hashing Modes**
Xiaoyang Dong, Xiaoyun Wang

17:05-17:25 **Meet-in-the-Middle Attacks on Classes of Contracting and Expanding Feistel Constructions**
Jian Guo, Jérémy Jean, Ivica Nikolic, Yu Sasaki

17:25-17:45 **Subspace Trail Cryptanalysis and its Applications to AES**
Lorenzo Grassi, Christian Rechberger, Sondre Rønjom

Tuesday 7 March 2017

9:00- **Registration**

Session V - New designs (*9:30 - 10:50, Chair: Thomas Peyrin)*

9:30-9:50 **Haraka v2 Efficient Short-Input Hashing for Post-Quantum Applications**
Stefan Kölbl, Martin M. Lauridsen, Florian Mendel, Christian Rechberger

9:50-10:10 **The Qarma Block Cipher Family**
Roberto Avanzi

10:10-10:30 **LIZARD - A Lightweight Stream Cipher for Power-constrained Devices**
Matthias Hamann, Matthias Krause, Willi Meier

10:30-10:50 **On Ciphers that Continuously Access the Non-Volatile Key**
Vasily Mikhalev, Frederik Armknecht, Christian Müller

10:50-11:20 **Coffee Break** (30 min)

Session VI - Invited Talk II (*11:20 - 12:20, Chair: Bart Preneel)*

11:20-12:20 **Design, Analysis and Promotion of (Lightweight) Block Ciphers**
Shiho Moriai (NICT, Japan)

12:20-13:35 **Lunch Break** (75 min)

Session VII - Authenticated Encryption: Cryptanalysis (*13:35 - 14:55, Chair: Gaëtan Leurent)*

13:35-13:55 **Cryptanalysis of NORX v2.0**
Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jérémy Jean, Jean-René Reinhard

13:55-14:15 **Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks?**
Colin Chaigneau, Henri Gilbert

14:15-14:35 **Conditional Cube Attack on Round-Reduced ASCON**
Zheng Li, Xiaoyang Dong, Xiaoyun Wang

14:35-14:55 **Cube-like Attack on Round-Reduced Initialization of Ketje Sr**
Xiaoyang Dong, Zheng Li, Xiaoyun Wang, Ling Qin

14:55-15:25 **Coffee Break** (30 min)

Session VIII - Security reductions *(15:25 - 16:45, Chair: Tetsu Iwata)*

15:25-15:45 **Security Analysis of BLAKE2's Modes of Operation**
Atul Luykx, Bart Mennink, Samuel Neves

15:45-16:05 **The Exact Security of PMAC**
Peter Gaži, Krzysztof Pietrzak, Michal Rybár

16:05-16:25 **On the Exact Security of Message Authentication using Pseudorandom Functions**
Ashwin Jha, Avradip Mandal, Mridul Nandi

16:25-16:45 **A Fast Single-Key Two-Level Universal Hash Function**
Debrup Chakraborty, Sebati Ghosh, Palash Sarkar

16:45-17:45 **Rump Session** *(Chair: Carlos Cid)*

19:00-21:00 **Banquet** at The Tokyo Station Hotel (standing buffet style)

Wednesday 8 March 2017

9:00- **Registration**

Session IX - Authenticated encryption: Designs (*9:20 - 10:40, Chair: Anne Canteaut)*

9:20-9:40 **Stronger Security Variants of GCM-SIV**
Tetsu Iwata, Kazuhiko Minematsu

9:40-10:00 **ISAP -- Towards Side-Channel Secure Authenticated Encryption**
Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Thomas Unterluggauer

10:00-10:20 **Linking Online Misuse-Resistant Authenticated Encryption and Blockwise Attack Models**
Guillaume Endignoux, Damian Vizár

10:20-10:40 **OleF: an Inverse-Free Online Cipher. An Online SPRP with an Optimal Inverse-Free Construction**
Ritam Bhaumik, Mridul Nandi

10:40-11:05 **Coffee Break** (25 min)

Session X - Cryptanalysis: Techniques (*11:05 - 12:25, Chair: Thomas Fuhr)*

11:05-11:25 **Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers**
Thorsten Kranz, Gregor Leander, Friedrich Wiemer

11:25-11:45 **Improved Parameter Estimates for Correlation and Capacity Deviates in Linear Cryptanalysis**
Céline Blondeau, Kaisa Nyberg

11:45-12:05 **Quantum Differential and Linear Cryptanalysis**
Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia

12:05-12:25 **The Approximate k-List Problem**
Leif Both, Alexander May

12:25-13:40 **Lunch Break** (75 min)

Session XI - Security Notions (*13:40 - 14:40, Chair: Kazuhiko Minematsu)*

13:40-14:00 **Security Notions for Bidirectional Channels**
Giorgia Azzurra Marson, Bertram Poettering

14:00-14:20 **Security of Symmetric Primitives under Incorrect Usage of Keys**
Pooya Farshim, Claudio Orlandi, Razvan Rosie

14:20-14:40 **SoK: Security Models for Pseudo-Random Number Generators**
Sylvain Ruhault

Session XII - Cryptanalysis: ARX (*14:40 - 15:40, Chair: Yu Sasaki)*

14:40-15:00 **Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha**
Arka Rai Choudhuri, Subhamoy Maitra

15:00-15:20 **Rotational Cryptanalysis in the Presence of Constants**
Tomer Ashur, Yunwen Liu

15:20-15:40 **Optimal Differential Trails in SIMON-like Ciphers**
Zhengbin Liu, Yongqiang Li, Mingsheng Wang

15:40 - 16:05 **Coffee Break** (25 min)

Session XIII - Cryptanalysis: Block ciphers (*16:05 - 17:45, Chair: Shiho Moriai)*

16:05-16:25 **Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs**
Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, Siang Meng Sim

16:25-16:45 **Meet-in-the-Middle Attacks on Reduced-Round Midori64**
Li Lin, Wenling Wu

16:45-17:05 **Multi-key Analysis of Tweakable Even-Mansour with Applications to Minalpher and OPP**
Zhiyuan Guo, Wenling Wu, Renzhang Liu, Liting Zhang

17:05-17:25 **Analysis of AES, SKINNY, and Others with Constraint Programming**
Siwei Sun, David Gerault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, Lei Hu

17:25-17:45 **Cryptanalysis of GOST2**
Tomer Ashur, Achiya Bar-On, Orr Dunkelman