PROGRAM EUROCRYPT 2015

MONDAY, April 27th

9:00 Welcome

9:15 Invited Talk: A Privacy Research Roadmap for a National Privacy Research Strategy, Tal Rabin, IBM T.J. Watson Research Center, USA

10:15 Coffee Break

10:40 Random Number Generators R-Track

- Thomas Shrimpton; R. Seth Terashima
- A Formal Treatment of Backdoored Pseudorandom Generators, Yevgeniy Dodis; Chaya Ganesh; Alexander Golovnev; Ari Juels; Thomas Ristenpart

- signatures

- Universal Signature Aggregators, Susan Hohenberger; Venkata Koppula; Brent Waters
- Fully Structure-Preserving Signatures and Shrinking Commitments, Masayuki Abe; Markulf Kohlweiss; Miyako Ohkubo; Mehdi Tibouchi

11:30 Swap

11:35 Number Field Sieve I-Track

- Improving NFS for the discrete logarithm problem in non-prime finite fields, Razvan Barbulescu; Pierrick Gaudry; Aurene Guillevic; François Morain
- The Multiple Number Field Sieve with Conjugation and Generalized, Joux-Lercier Methods; Cécile Pierrot

- Zero-Knowledge Proofs

- Disjunctions for Hash Proof Systems: New Constructions and Applications, Michel Abdalla; Fabrice Benhamouda; David Pointcheval
- Quasi-Adaptive NIZK for Linear Subspaces Revisited, Eike Kiltz; Hoeteck Wee

12:30 Lunch

14:00 Algorithmic Cryptanalysis R-Track

- Better Algorithms for LWE and LWR, Alexandre Duc; Florian Tramèr; Serge Vaudenay
- On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes, Alexander May; Ilya Ozerov

- Leakage-Resilient Cryptography

- Leakage-Resilient Circuits Revisited - Optimal Number of Computing Components without Leak-Free Hardware, Dana Dachman-Soled; Feng-Hao Liu; Hong-Sheng Zhou
- Noisy Leakage Revisited, Stefan Dziembowski; Sebastian Faust; Maciej Skórski

14:55 Symmetric Cryptanalysis I R-Track

- Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE, Itai Dinur
- A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iScream and Zorro, Gregor Leander; Brice Minjaud; Sandre Ramjan

- Garbled Circuits

- Privacy-Free Garbled Circuits with Applications To Efficient Zero-Knowledge, Tore Kasper Frederiksen; Jesper Buus Nielsen; Claudio Orlandi
- Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits using Half Gates, Samee Zahr; Mike Rosulek; David Evans

15:45 Coffee Break

16:15 Symmetric Cryptanalysis II R-Track

- Structural Evaluation by Generalized Integral Property, Yusuke Todo
- Cryptanalysis of SP Networks with Partial Non-Linear Layers, Achiya Bar-On; Itai Dinur; Orr Dunkelman; Nathan Keller; Virginie Lallemand; Boaz Tsaban

- Crypto Currencies

- One-out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin, Jens Groth; Markulf Kohlweiss
- The Bitcoin Backbone Protocol: Analysis and Applications, Juan Garay; Aggelos Kiayias; Nikas Leonardos

TUESDAY, April 28th

9:00 Best paper and honourable mentions

- Cryptanalysis of the Multilinear Maps over the Integers, Jung Hee Cheo; Kyoohyung Han; Changmin Lee; Hansol Ryu; Damien Stehlé
- Robust Authenticated-Encryption: AEZ and the Problem that it Solves, Viet Tung Hoang; Ted Krovetz; Phillip Rogaway
- On the behaviors of affine equivalent Sboxes regarding differential and linear attacks, Anne Canteaut; Joëlle Roué

10:15 Coffee Break

10:40 Hash Functions R-Track

- The Sum Can Be Weaker Than Each Part, Gaëtan Leurent; Lei Wang
- SPHINCS: practical stateless hash-based signatures, Daniel J. Bernstein; Daira Hopwood; Andreas Hülsing; Tanja Lange; Ruben Niederhagen; Louiza Popovchristodoulou; Michael Schneider; Peter Schwabe; Zooko Wilcox O’Hearn

- Secret Sharing

- Function Secret Sharing, Elette Boyle; Niv Gilboa; Yuval Ishai
- Linear Secret Sharing Schemes from Error Correcting Codes and Universal Hash Functions, Ronald Cramer; Ivan Damgaard; Nico Doettling; Serge Fehr; Gabriele Spini

11:30 Swap

11:35 Evaluating Implementations R-Track

- Making Masking Security Proofs Concrete (Or How to Evaluate the Security of any Leaking Device) Alexandre Duc; Sebastian Faust; François-Xavier Standaert
- Ciphers for MPC and FH, Martin Albrecht; Christian Rechberger; Thomas Schneider; Tyge Tiessen; Michael Zohner

- Outsourcing Computations

- Cluster Computing in Zero Knowledge, Alessandro Chiesa; Eran Tromer; Madars Virza
- Hosting Services on an Untrusted Cloud, Dan Boneh; Diya Gupta; Ilya Mironov; Amit Sahai

14:00 Masking R-Track

- Verified Proofs of Higher-Order Masking, Gilles Barthe; Sonia Belaid; François Dupressoir; Pierre-Alain Fouque; Benjamin Grégoire; Pierre-Yves Strub
- Inner Product Masking Revisited, Josep Balasch; Sebastian Faust; Benedikt Gierlichs

- Obfuscation and E-Voting

- How to Obfuscate Programs Directly, Joe Zimmerman
- End-to-End Verifiable Elections in the Standard Model, Aggelos Kiayias; Thomas Zacharias; BingSheng Zhang

18:30 Walking Diner and Rump Session
**WEDNESDAY, April 29th**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:15</td>
<td><strong>Invited talk:</strong> Practical Applications of Homomorphic Encryption, Kristin Lauter, Microsoft Research, USA</td>
</tr>
<tr>
<td>10:15</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:40</td>
<td><strong>R-Track</strong>&lt;br&gt;<strong>I-Track</strong></td>
</tr>
<tr>
<td></td>
<td>Fully Homomorphic Encryption I&lt;br&gt;Fully Homomorphic Encryption over the Integers Revisited, Jung Hee Cheo; &lt;br&gt;Damien Stehle &lt;br&gt;(Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces, Koji Nuida; Kaoru Kurosawa&lt;br&gt;Multi-Party Computations&lt;br&gt;Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data, Shashank Agrawal; Shweta Agrawal; Manoj Prabhakaran &lt;br&gt;Executable Proofs, Input-Size Hiding Secure Computation and a New Ideal World, Melissa Chase; Rafail Ostrovsky; Ivan Visconti</td>
</tr>
<tr>
<td>11:30</td>
<td>Swap</td>
</tr>
<tr>
<td>11:35</td>
<td>Related-Key Attacks&lt;br&gt;KDM-CCA Security from RKA Secure Authenticated Encryption, Xianhui Lu; Bao Li; Dingding Jia&lt;br&gt;Encryption&lt;br&gt;Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation, Dan Boneh; Kevin Lewi; Mariana Raykova; Amit Sahai; Mark Zhandry; Joe Zimmerman &lt;br&gt;Improved Dual System ABE in Prime-Order Groups via Encodings, Jie Chen; Romain Gay; Hoeteck Wee</td>
</tr>
<tr>
<td>12:30</td>
<td>Lunch</td>
</tr>
<tr>
<td>14:00</td>
<td><strong>R-Track</strong>&lt;br&gt;<strong>I-Track</strong></td>
</tr>
<tr>
<td></td>
<td>Fully Homomorphic Encryption II&lt;br&gt;FHEW: Bootstrapping in less than a second, Léo Ducas; Daniele Micciancio&lt;br&gt;Bootstrapping for HElib, Shai Halevi; Victor Shoup&lt;br&gt;Resistant Protocols&lt;br&gt;Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model, Mihir Bellare; Viet Tung Hoang &lt;br&gt;Cryptographic Reverse Firewalls, Ilya Mironov; Noah Stephens-Davidowitz</td>
</tr>
<tr>
<td>14:50</td>
<td>Swap</td>
</tr>
<tr>
<td>15:45</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16:00</td>
<td>IACR membership meeting</td>
</tr>
<tr>
<td>20:00</td>
<td>Banquet</td>
</tr>
</tbody>
</table>

**THURSDAY, April 30th**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:15</td>
<td><strong>Invited talk:</strong> Threshold Implementations, Vincent Rijmen, KU Leuven, Belgium</td>
</tr>
<tr>
<td>10:15</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>10:40</td>
<td><strong>R-Track</strong>&lt;br&gt;<strong>I-Track</strong></td>
</tr>
<tr>
<td></td>
<td>Symmetric Cryptanalysis III&lt;br&gt;Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak&lt;br&gt;Sponge Function, Itai Dinur; Pawel Morawiecki; Josef Pieprzyk; Marian Srebrny; Michal Straus&lt;br&gt;Twisted Polynomials and Forgery Attacks on GCM, Mohamed Ahmed Abdelrahim; Peter Beelen; Andrey Bogdanov; Elmar Tischhauser&lt;br&gt;Quantum Cryptography&lt;br&gt;Non-interactive zero-knowledge proofs in the quantum random oracle model, Dominique Unruh&lt;br&gt;Privacy Amplification in the Isolated Qubits Model, Yi-Kai Liu</td>
</tr>
<tr>
<td>11:30</td>
<td>Swap</td>
</tr>
<tr>
<td>11:35</td>
<td>Lattices&lt;br&gt;Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices, Vadim Lyubashevsky; Thomas Prest&lt;br&gt;Discrete Logarithms&lt;br&gt;Generic Hardness of the Multiple Discrete Logarithm Problem, Aaram Yun</td>
</tr>
<tr>
<td>12:00</td>
<td>Lunch</td>
</tr>
</tbody>
</table>