## Eurocrypt 2019 Affiliated Events

### Program Overview

**Saturday (1/2) May 18, 2019**

<table>
<thead>
<tr>
<th>Time</th>
<th>CBC (room A02)</th>
<th>CrossFyre (room A03)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 – 09:00</td>
<td>Registration</td>
<td></td>
</tr>
<tr>
<td>09:00 – 10:30</td>
<td><strong>Invited talk</strong></td>
<td><strong>Session B</strong></td>
</tr>
<tr>
<td></td>
<td><strong>McTiny: McEliece for tiny network servers (Dan Bernstein)</strong></td>
<td>On the Privacy-Preserving V2G Payment Scheme P6V2G and Scenario Specific Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rebecca Schwerdt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yet another Holy Grail in crypto: (efficient) zero-knowledge proofs for lattice problems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cecilia Boschini</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privado: Privacy-Preserving Group-Based Advertising in Online Social Networks using Multiple Independent Providers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sanaz Taheri Boshrooyeh</td>
</tr>
<tr>
<td>10:30 – 11:00</td>
<td><strong>Paper presentations</strong></td>
<td><strong>Session C</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 – 12:30</td>
<td><strong>Coffee Break</strong></td>
<td><strong>Keynote</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Quantum Resistant Public Key Encryption Scheme HermitianRLCE</strong></td>
<td>Stronger Lower Bounds for Online ORAM</td>
</tr>
<tr>
<td></td>
<td>G. Matthews, Y. Wang</td>
<td>Veronika Slívová</td>
</tr>
<tr>
<td></td>
<td><strong>Design of LEDAkem and LEDApkc instances with tight parameters and bounded decryption failure rate</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>M. Baldi, A. Barenghi, F. Chiaraluce, G. Petosi, P. Santini</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Introducing arithmetic failures to accelerate QC-MDPC code-based cryptography</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A. Guimarães, E. Borin, D. F. Aranha</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DAGS Reloaded: Revisiting Dyadic Key Encapsulation</strong></td>
<td></td>
</tr>
<tr>
<td>12:30 – 14:00</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>14:00 – 15:30</td>
<td><strong>Contributed talks</strong></td>
<td><strong>Session D</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>How to combine Reed-Muller and Goppa codes in McEliece type cryptosystem</strong></td>
<td>Algebraic construction of lattices in the Ring-LWE problem</td>
</tr>
<tr>
<td></td>
<td>I. Dumer, G. Kabatiansky, E. Knouk</td>
<td>Jheyne Ortiz</td>
</tr>
<tr>
<td></td>
<td><strong>Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes</strong></td>
<td>More efficient updatable zk-SNARKs</td>
</tr>
<tr>
<td></td>
<td>T. Debris-Alazard, N. Sendrier, J.-P. Tillich</td>
<td>Arantxa Zapico</td>
</tr>
<tr>
<td></td>
<td><strong>New McEliece cryptosystem using Reed-Solomon codes over an extension field</strong></td>
<td>Applied post-quantum cryptography for embedded systems</td>
</tr>
<tr>
<td></td>
<td>K. Khathuria, J. Rosenthal, V. Weger</td>
<td>Soundes Marzougui</td>
</tr>
<tr>
<td></td>
<td><strong>Loong: new IND-CCA-secure code-based public-key schemes</strong></td>
<td>Anomaly Detection of IOT Nodes using Power Signature</td>
</tr>
<tr>
<td></td>
<td>L.-P. Wang</td>
<td>Maria Ashraf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Towards Cognitive Obfuscation – Analyzing Human Factors to Impede Hardware Reverse Engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Carina Wiesen</td>
</tr>
<tr>
<td>15:30 – 16:00</td>
<td><strong>Coffee Break</strong></td>
<td></td>
</tr>
<tr>
<td>16:00 – 17:30</td>
<td><strong>Working and discussion session</strong></td>
<td><strong>Session E</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Efficient and Proactive Long-Term Secure Secret Sharing-based Storage Systems</strong></td>
<td>Efficient and Proactive Long-Term Secure Secret Sharing-based Storage Systems</td>
</tr>
<tr>
<td></td>
<td>Giulia Traverso</td>
<td>Giulia Traverso</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(last updated: 2019-05-18)
## Program Overview
### Saturday (2/2)  
May 18, 2019

<table>
<thead>
<tr>
<th>Time</th>
<th>PENCIL (room A01)</th>
<th>WhibOx (room A5)</th>
<th>WSM (room A4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 – 08:50</td>
<td>Registration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 08:50 – 10:30 | **Keynote 1 – A Consensus Taxonomy in the Blockchain Era (Juan Garay)**  
Afgjort – A Semi-Synchronous Finality Layer for Blockchains  
B. Mags, J. Bius Nielsen, D. Tschudi  
Pixel: Multi-Signatures for Consensus  
M. Drijvers, S. Gorbunov, G. Neven, H. Wee  
A Framework for Anonymous Lottery-Based Protocols in the Proof-of-Stake Setting  
F. Baldimtsi, V. Rajeev Madathil, A. Scafuro, L. Zhou  
White-box designs  
White-box cryptography: between academia and industry (Part 1)  
Andrey Bogdanov  
White-box cryptography: between academia and industry (Part 2)  
Andrey Bogdanov  
<< starts 09:00 >>  
Secure messaging, MLS and Wire  
Raphael Robert  
Definitional Foundations of Ratcheting and their Impact on Practice  
Paul Rooster |                                                           |                                                           |                                                       |
|               |                                                           |                                                           |                                                       |
| 10:30 – 11:00 | Coffee Break                                               |                                                           |                                                       |
| 11:00 – 12:30 | **Keynote 2 (Charles Hoskinson)**  
Asymmetric Distributed Trust  
C. Cachin, B. Tackmann  
Publicly Verifiable Proofs from Blockchains and the Attacks of the Clones in Proof-of-Stake Blockchains  
A. Scafuro, L. Siniscalchi, I. Visconti  
Timed Signatures and Zero-Knowledge Proofs - Timestamping in the Blockchain Era  
A. Abadi, M. Ciampi, A. Kiyalias, V. Zikas  
White-box designs  
White-box and asymmetrically hard crypto design  
Alex Biryukov  
New encodings for white-box implementations  
Adrian Ranaa  
Encryption is not enough - using mix-networks for anonymous messaging  
Aria Pirozhkova  
Messaging Layer Security: Past, Present, and Future  
Richard Barnes |                                                           |                                                       |                                                       |
| 12:30 – 14:00 | Lunch                                                      |                                                           |                                                       |
| 14:00 – 15:30 | **Keynote 3 – Why should I believe that? (Jens Groth)**  
Fully Homomorphic NIZK and NIWI Proofs  
P. Ananth, A. Deshpande, Y. Kalai, A. Lysyanskaya  
Zether: Towards Privacy in a Smart Contract World  
S. Blümer, S. Agrawal, M. Zanaini, G. Boneh  
ZEXE: Enabling Decentralized Private Computation  
S. Bowe, A. Chiesa, M. Green, I. Miers, P. Münch, H. Wu  
Attacks on white-box cryptography  
Grey-box attacks, four years later  
Philipp Toffen  
A DFA attack on white-box implementations of AES with external encodings  
Alessandro Amadori  
On the Security and Insecurity of TreeKEM  
Yevgeny Dodis  
Message Franking: Invisible Salamanders, Encryption, and AMFs  
Paul Grubbs |                                                       |                                                       |                                                       |
| 15:30 – 16:00 | Coffee Break                                               |                                                           |                                                       |
| 16:00 – 17:30 | On QA-NIZK in the BPK Model  
P. Abdulmaleki, H. Lipmaa, J. Siim, M. Zajac  
Verifiable MPC and DLT  
P. Schoenmakers, T. Segers  
Attacks on white-box cryptography  
DCA attacks against internally encoded white-box implementations  
Junwei Wang  
Security assessment of WhibOx 2017 candidates  
Alexander Treff  
A Proper Security Level for Postcompromise Secure Messaging  
Serge Vaudenay |                                                       |                                                       |                                                       |

(last updated: 2019-05-18)
<table>
<thead>
<tr>
<th>Time</th>
<th>CBC (room A02)</th>
<th>QuAC (room A03)</th>
<th>SPY (room A01)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 – 09:00</td>
<td>Registration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00 – 10:30</td>
<td><strong>Invited talk</strong> <em>(Ray Perlner)</em></td>
<td>Quantum Search Beyond Grover</td>
<td>&quot;If Technology Allows For It&quot; – the current debate on the usage of surveillance software by the German police</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stacey Jeffery</td>
<td>Marie Bröckling</td>
</tr>
<tr>
<td>10:30 – 11:00</td>
<td>Coffee Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 – 12:30</td>
<td><strong>Paper presentations</strong></td>
<td>Quantum Algorithms for Optimization over Finite Fields and Applications in Cryptanalysis</td>
<td>Corporate surveillance of everyday life – How companies use personal data against people</td>
</tr>
<tr>
<td></td>
<td>Practical Algebraic Attack on DAGS</td>
<td></td>
<td>Wolfe Christl</td>
</tr>
<tr>
<td></td>
<td>M. Bardet, M. Bertin, A. Couvreur, A. Otmani</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes</td>
<td></td>
<td>The European Intelligence Oversight Network: a quest for better control instruments</td>
</tr>
<tr>
<td></td>
<td>P. Santini, M. Battaglioni, F. Chiaraluce, M. Baldi</td>
<td></td>
<td>Thorsten Wetzing</td>
</tr>
<tr>
<td></td>
<td>On IND-CCA1 Security of Randomized McEliece Encryption in the Standard Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>F. A. Farro, K. Morezov</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weak Keys in the Faure-Loidreau Cryptosystem</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T. Jerkovits, H. Bartz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30 – 14:00</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00 – 15:30</td>
<td><strong>Contributed talks</strong></td>
<td>New Algorithms for Quantum Symmetric Cryptanalysis</td>
<td>Silicon Valley and China</td>
</tr>
<tr>
<td></td>
<td>Generalization of the ball-collision algorithm</td>
<td>Andre Schrottenloher</td>
<td>Ryan Gallagher</td>
</tr>
<tr>
<td></td>
<td>V. Weger, C. Interlando, K. Khathurthu, N. Rohrer, J. Rosenthal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backflip: An Improved QC-MDPC Bit-Flipping Decoder</td>
<td>Non-Asymptotic Quantum Resource Estimation</td>
<td>Secret Sharing for Journalists and Whistleblowers</td>
</tr>
<tr>
<td></td>
<td>N. Sendrier, V. Vasseur</td>
<td>Vlad Gheorghiu</td>
<td>Phil Rogaway</td>
</tr>
<tr>
<td></td>
<td>Implementation of Code-based KEMs submitted to NIST on Optical Communication Systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>J. Y. Cho</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ternary Syndrome Decoding for Large Weights</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R. Bricout, A. Chailloux, T. Debris-Alazard, M. Lequesne</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30 – 16:00</td>
<td>Coffee Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00 – 17:30</td>
<td><strong>Working and discussion session</strong></td>
<td>Quantum Hidden Shift Algorithms 2.0</td>
<td>Hunting Political Bots on Twitter – Joining Captain Ahab</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Greg Kuperberg</td>
<td>Orr Dunkelman</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mix-networks against mass surveillance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ana Piotrowska</td>
</tr>
</tbody>
</table>

(last updated: 2019-05-18)
### OPACity (room A4)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:30 – 09:00</td>
<td>Registration</td>
</tr>
<tr>
<td>09:00 – 10:30</td>
<td><strong>Theory (joint session in room A5)</strong></td>
</tr>
<tr>
<td></td>
<td>– Foundations of program obfuscation</td>
</tr>
<tr>
<td></td>
<td>– Obfuscation from LWE proofs, attacks, candidates</td>
</tr>
<tr>
<td>10:30 – 11:00</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>11:00 – 12:30</td>
<td><strong>Theory (joint session in room A5)</strong></td>
</tr>
<tr>
<td></td>
<td>– White-box crypto and obfuscation: relations and attacks</td>
</tr>
<tr>
<td>12:30 – 14:00</td>
<td>Lunch</td>
</tr>
<tr>
<td>14:00 – 15:30</td>
<td>Tools and Demos</td>
</tr>
<tr>
<td></td>
<td>– Optimize your binary tracing: an example with an ECDSA implementation</td>
</tr>
<tr>
<td></td>
<td>– Exploring different faulting techniques for stressing white-box crypto</td>
</tr>
<tr>
<td>15:30 – 16:00</td>
<td>Coffee Break</td>
</tr>
<tr>
<td>16:00 – 17:30</td>
<td>Hands-on</td>
</tr>
</tbody>
</table>

### WhibOX (room A5)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00 – 10:30</td>
<td>Initial lecture</td>
</tr>
<tr>
<td></td>
<td>– Cas Cremers</td>
</tr>
</tbody>
</table>

### Tamarin Tutorial (TPT) (room A2)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30 – 11:00</td>
<td>Hands-on</td>
</tr>
</tbody>
</table>

(last updated: 2019-05-18)