Day 1 - October 7

>> 7h45 OPENING REMARKS

>> 8h00 -9h30: QUANTUM ALGORITHMS

MODERATOR: TBD

Tight Bounds for Simon's Algorithm
Xavier Bonnetain

Constructions for Quantum Indistinguishability Obfuscation
Raza Ali Kazmi; Raza Ali Kazmi

On Forging SPHINCS + -Haraka Signatures on a Fault-tolerant Quantum Computer
Robin Berger; Marcel Tiepelt

>> 9h30- 10h00: BREAK

>> 10h00 -11h00: INVITED TALK

Luca De Feo, ¿What’s next for isogeny based cryptography?

>> 11h00- 11h30: BREAK

>> 11h30 -13h30: POST-QUANTUM CRYPTOGRAPHY

MODERATOR: TBD

Post-Quantum Key-Blinding for Authentication in Anonymity Networks
Edward Eaton; Douglas Stebila; Roy Stracovsky

Implementing and measuring KEMTLS
Sofía Celi; Armando Faz-Hernández; Goutam Tamvada; Luke Valenta; Thom Wiggers; Bas Westerbaan; Christopher Wood

A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples in PQC Candidates
Mojtaba Bisheh-Niasar; Reza Azarderakhsh; Mehran Mozaffari-Kermani

Attribute-Based Access Control for Inner Product Functional Encryption from LWE
Tapas Pal; Ratna Dutta
Day 2 - October 8

>> 7h30 - 9h30: CRYPTANALYSIS AND SIDE-CHANNEL ANALYSIS I

MODERATOR: TBD

Classical Attacks on a Variant of the RSA Cryptosystem
Abderrahmane Nitaj; Muhammad Rezal Bin Kamel Ariffin; Nurul Nur Hanisah Adenan; Nur Azman Abu

Improved attacks against key reuse in learning with errors key exchange
Nina Bindel; Douglas Stebila; Shannon Veitch

Differential-ML Distinguisher: Machine Learning based Generic Extension for Differential Cryptanalysis 10
Tarun Yadav; Manoj Kumar

Train or Adapt a Deeply Learned Profile 11
Christophe Genevey-Metat; Annelie Heuser; Benoit Gérard

>> 9h30 - 10h00: BREAK

>> 10h00 - 11h00: INVITED TALK

Shweta Agrawal, Recent Progress and Challenges in Lattice Based Cryptography

>> 11h00 - 11h30: BREAK

>> 11h30 - 13h00: CRYPTANALYSIS AND SIDE-CHANNEL II

MODERATOR: TBD

Autocorrelations of vectorial Boolean functions
Anne Canteaut; Lukas Kölsch; Chao Li; Chunlei Li; Kangquan Li; Longjiang Qu; Friedrich Wiemer

Automatic Search for Bit-based Division Property
Shibam Ghosh; Orr Dunkelman

Highly Secure Leakage-resilient TBC-based Authenticated Encryption
Eik List

>> 14h00 - 15h00: Virtual tour to a traditional Colombian Coffee farm
Day 3 - October 9

>> 6h00-7h00: Waking up in the Colombian Coffee Region

>> 7h00 -8h30: DISTRIBUTED CRYPTOGRAPHIC PROTOCOLS I

MODERATOR: TBD

Weight-Based Nakamoto-Style Blockchains
Simon Holmgaard Kamp; Bernardo Magri; Christian Matt; Jesper Buus Nielsen; Søren Eller Thomsen; Daniel Tschudi

LOVE a Pairing
Diego F. Aranha; Elena Pagnin; Francisco Rodríguez-Henríquez

Implementing Secure Reporting of Sexual Misconduct - Revisiting WhoToo
Alejandro Hevia; Ilana Mergudich-Thal

>> 8h30 - 9h00: BREAK

>> 9h00 -10h00: DISTRIBUTED CRYPTOGRAPHIC PROTOCOLS II

Stronger Notions and a More Efficient Construction of Threshold Ring Signatures
Alexander Munch-Hansen; Claudio Orlandi; Sophia Yakoubov

Improved Threshold Signatures, Proactive Secret Sharing and Input Certification from LSS Isomorphisms
Diego Aranha; Anders Dalskov; Daniel Escudero; Claudio Orlandi

>> 10h00 -11h00: INVITED TALK

Dan Boneh, Recent Developments in Based Cryptography

>> 11h00- 11h30: BREAK
>> 11h30 - 13h00: MULTIPARTY COMPUTATION

MODERATOR: TBD

**Full-Threshold Actively-Secure Multiparty Arithmetic Circuit Garbling**
Eleftheria Makri; Tim Wood

**The Cost of IEEE Arithmetic in Secure Computation**
David Archer; Shahla Atapoor; Nigel P. Smart

**Honest Majority MPC with Abort with Minimal Online Communication**
Anders Dalskov; Daniel Escudero

Organized by:

In cooperation with:

Sponsor: