Workshop on Cybersecurity in a Post-Quantum World
Accepted Presentations

Post-quantum Authenticated Key Exchange from Ideal Lattices
Jiang Zhang, Zhenfang Zhang, Jintai Ding, Michael Snook, Ozgur Dagdelen

Gui: Revisiting Multivariate Digital Signature Schemes based on HFEv-
Albrecht Petzoldt, Ming-Sheng Chen, Jintai Ding, Bo-Yin Yang

QC-MDPC-McEliece: A public-key code-based encryption scheme
Nicolas Sendrier, Jean-Pierre Tillich, Rafael Misoczki, Paulo Barreto

Rank based Cryptography: a credible post-quantum alternative to classical crypto
Phillipe Gaborit, Olivier Ruatta, Julien Schrek, Jean-Pierre Tillich, Gilles Zemor

Practical Lattice-based Digital Signature Schemes
James Howe, Thomas Poppelmann, Maire O'Neill, Elizabeth O'Sullivan, Tim Guneysu

Post-quantum key exchange for the TLS protocol from RLWE problem
Joppe Bos, Craig Costello, Michael Naehrig, Douglas Stebila

Post-Quantum Secure Onion Routing (Future Anonymity in Today's Budget)
Satrajit Ghosh, Aniket Kate

A quantum-safe circuit-extension handshake for Tor
John Schanck, William Whyte, Zhenfei Zhang

Hash-based Signatures: An outline for a new standard
Andreas Hulsing, Stefan-Lukas Gazdag, Denis Butin, Johannes Buchmann

SPHINCS: practical stateless hash-based signatures
Daniel Bernstein, Daira Hopwood, Andreas Hulsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox-O'Hearn

Let Live and Let Die - Handling the state of Hash-based signatures
Stefan-Lukas Gazdag, Denis Butin, Johannes Buchmann

Evaluating Post-Quantum Asymmetric Cryptographic Algorithm Candidates
Dan Shumow, Tolga Acar, Josh Benaloh, Craig Costello

Failure is not an option: Standardization issues for Post-Quantum key Agreement
Daniel Kirkwood, Bradley Lackey, John McVey, Mark Motley, David Tuller

PQCrypto project in the EU
Tanja Lange

MQ Challenge: Hardness Evaluation of Solving MQ problems
Takanori Yasusa, Xavier Dahan, Yun-Ju Huang, Tsuyoshi Takagi, Kouichi Sakurai

Renaissance of Pre-computation in a Post-Quantum World
Aydin Aysu, Patrick Schaumont

Trapdoor simulation of quantum algorithms
Tung Chou, Daniel Bernstein

Grobner Bases Techniques in Post-Quantum Cryptography
Jean-Charles Faugere, Danilo Gligoroski, Ludovic Perret, Simona Samardjiska

DTLS-HIMMO: Efficiently Securing PQ world with a fully-collusion resistant KPS
Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, Jose Luis Torre-Arce

A New Code Based Public Key Encryption and Signature Scheme based on List Decoding
Danilo Gligoroski, Simona Samardjiska, Hakon Jacobsen, Sergey Bezzateev

PANEL: **Shoring up the Infrastructure: A strategy for Standardizing Hash Signatures**
panelists: *Andreas Hulsing, David McGrew, Aziz Mohaisen, Russ Housley*

PANEL: **Key Management for Quantum-safe Cryptography**
panelists: *Robert Griffin, Elizabeth O'Sullivan, Sean Parkinson, Gregoire Ribordy, William Whyte*