The First PQC Standardization Conference
April 11-13, 2018

AGENDA

Pier 66 Hotel & Marina – Panorama Ballroom
Fort Lauderdale, Florida

*Please note: Speakers/times are subject to change without notice.

Wednesday, April 11, 2018

2:00 pm – 4:00 pm	**Registration**
3:00 pm – 3:05 pm	**Opening Remarks** Lily Chen, *NIST*
3:05 pm – 4:30 pm	**Session I** Session Chair: Lily Chen, *NIST*
3:05 – 3:20	**PostQuantum RSA** Presented by: Dan Bernstein, *University of Illinois at Chicago*
3:20 – 3:35	**SIKE** Presented by: David Jao, *University of Waterloo*
3:35 – 3:50	**SPHINCS+** Presented by: Andreas Hülsing, *Eindhoven University of Technology*
3:50 – 4:05	**Gravity-SPHINCS** Presented by: Guillaume Endignoux, *École Polytechnique Fédérale de Lausanne/Kudelski Security*
4:05 – 4:20	**Picnic** Presented by: Greg Zaverucha, *Microsoft*
4:20 – 4:30	**WalnutDSA** Presented by: Derek Atkins, *SecureRF Corporation*
4:30 pm	**Adjourn for the Day**

Thursday, April 12, 2018

8:00 am – 4:30 pm	**Registration**
8:45 am – 9:00 am	**Opening Remarks** Matt Scholl, *NIST*
9:00 am – 9:10 am	**Talk: Estimate all the {NTRU/LWE} Schemes** Rachel Player, *Sorbonne Université*
9:10 am – 10:35 am	**Session II** Session Chair: Gorjan Alagic, *NIST*
9:10 – 9:35	**Crystals-Kyber/Dilithium** Presented by: Peter Schwabe, *Radboud University* Presented by: Vadim Lyubashevsky, *IBM Research – Zurich*
9:35 – 9:50	**FrodoKEM** Presented by: Chris Peikert, *University of Michigan*
9:50 – 10:05	**NewHope** Presented by: Thomas Poeppelmann, *Infineon Technologies*
10:05 – 10:20	**Ding Key Exchange** Presented by: Jintai Ding, *University of Cincinnati*
10:20 – 10:35	**KCL** Presented by: Yunlei Zhao, *Fudan University*
10:35 am – 10:55 am	**Break**
10:55 am – 12:05 pm	**Session III** Session Chair: Jacob Alperin-Sheriff, *NIST*
10:55 – 11:10	**Emblem/R.emblem** Presented by: Minhye Seo, *Korea University*
11:10 – 11:25	**LAC** Presented by: Xianhui Lu, *Chinese Academy of Science*
11:25 – 11:40	**HILA5** Presented by: Markku-Juhani O. Saarinen, *HILA5*
11:40 – 11:55	**Lima** Presented by: Nigel Smart, *KU Leuven & University of Bristol*
11:55 – 12:05	**Lepton** Presented by: Yu-Yu, *Shanghai Jiao Tong University*
12:05 pm – 1:10 pm	**Lunch** *(attendees on their own)*

Thursday, April 12, 2018

1:10 pm – 2:45 pm	**Session IV** Session Chair: Daniel Smith-Tone, *NIST*
1:10 – 1:20	**Giophantus (IEC)** Presented by: Koichiro Akiyama, *Toshiba Corporation*
1:20 – 1:35	**Gui** Presented by: Albrecht Petzoldt, *Université de Versailles*
1:35 – 1:50	**Rainbow** Presented by: Jintai Ding, *University of Cincinnati*
1:50 – 2:05	**HiMQ-3** Presented by: Cheol-Min Park, *National Institute for Mathematical Sciences*
2:05 – 2:20	**LUOV** Presented by: Ward Buellens, *imec-COSIC KU Lueven*
2:20 – 2:35	**MQDSS** Presented by: Joost Rijneveld, *Radboud University*
2:35 – 2:45	**DME** Presented by: Ignacio Luengo, *Universidad Complutense de Madrid*
2:45 pm – 3:05 pm	**Break** *Sponsored by: Microsoft Research*
3:05 pm – 4:30 pm	**Session V** Session Chair: Carl Miller, *NIST*
3:05 – 3:20	**Classic McEliece** Presented by: Tanja Lange, *Technische Universiteit Eindhoven*
3:20 – 3:30	**McNie** Presented by: Jon-Lark Kim, *Sogang University*
3:30 – 3:45	**Three Bears** Presented by: Mike Hamburg, *Rambus Security Division*
3:45 – 4:00	**Titanium** Presented by: Ron Steinfeld, *Monash University*
4:00 – 4:15	**Falcon** Presented by: Thomas Prest, *Thales Communications & Security*
4:15 – 4:30	**qTesla** Presented by: qTesla Team Member
4:30 pm – 5:00 pm	**Open Discussion and Adjourn** Moderator: Daniel Smith-Tone, *NIST*

Friday, April 13, 2018

8:00 am – 4:30 pm	**Registration**
9:00 am – 10:30 am	**Session VI** Session Chair: Ray Perlner, *NIST*
9:00 – 9:15	**BIKE** Presented by: Rafael Misoczki, *Intel*
9:15 – 9:30	**LAKE/LOCKER** Presented by: Adrien Hauteville, *University of Limoges*
9:30 – 9:45	**Ouroboros-R** Presented by: Phillippe Gaborit, *University of Limoges*
9:45 – 10:00	**HQC** Presented by: Jean-Christophe Deneuville, *INSA-CVL Bourges & University of Limoges*
10:00 – 10:15	**RQC** Presented by: Phillippe Gaborit, *University of Limoges*
10:15 – 10:30	**LEDAkem/LEDApkc** Presented by: Marco Baldi, *Università Politecnica Delle Marche* Presented by: Alessandro Barenghi, *Politecnico di Milano*
10:30 am – 10:50 am	**Break**
10:50 am – 12:10 pm	**Session VII** Session Chair: Bill Fefferman, *NIST*
10:50 – 11:05	**Saber** Presented by: Frederik Vercauteren, *COSIC-KU Leven*
11:05 – 11:30	**NTRUEncrypt/pqNTRUsign** Presented by: Zhenfei Zhang, *Onboard Security*
11:30 – 11:45	**NTRU-HRSS-KEM** Presented by: John M. Schank, *University of Waterloo*
11:45 – 12:00	**NTRUprime** Presented by: Christine van Vredendaal, *TU Eindhoven*
12:00 – 12:10	**pqsigRM** Presented by: Jong-Seon No, *Seoul National University*
12:10 pm – 1:15 pm	**Lunch** *(attendees on their own)*
1:15 pm – 2:55 pm	**Session VIII** Session Chair: Jacob Alperin-Sheriff, *NIST*
1:15 – 1:40	**Odd Manhattan/DRS** Presented by: Thomas Plantard, *University of Wollongong*
1:40 – 1:55	**Mersenne-756839** Presented by: Antoine Joux, *Sorbonne Université*
1:55 – 2:10	**Lotus** Presented by: Le Trieu Phong, *National Institute of Information and Communications Technology*
2:10 – 2:25	**Round 2** Presented by: Oscar Garcia-Morchon, *Philips Research*
2:25 – 2:40	**Ramstake** Presented by: Alan Szepieniec, *KU Leuven*
2:40 – 2:55	**Lizard** Presented by: Joohee Lee, *Seoul National University*

Friday, April 13, 2018

2:55 pm – 3:15 pm	**Break**
3:15 pm – 4:50 pm	**Session IX** Session Chair: Dustin Moody, *NIST*
3:15 – 3:30	**Big Quake** Presented by: Alain Couvreur, *Inria & École Polytechnique*
3:30 – 3:45	**QC-MDPC KEM** Presented by: Philip Lafrance, *ISARA Corporation*
3:45 – 4:00	**RLCE** Presented by: Yonggee Wang, *University of North Carolina-Charolotte*
4:00 – 4:15	**NTS-KEM** Presented by: C.J. Tjhai, *PQ Solutions. Ltd.*
4:15 – 4:30	**DAGS** Presented by: Edoardo Persichetti, *Florida Atlantic University*
4:30 – 4:50	**DualModeMS/GeMMS** Presented by: Ludovic Perret, *Sorbonne Université / UPMC / INRIA*
4:50 pm – 5:00 pm	**Closing Remarks and Adjourn** Dustin Moody, *NIST*