The Second PQC Standardization Conference
August 22-24, 2019

AGENDA

University of California, Santa Barbara
Corwin Pavilion

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

Thursday, August 22, 2019	
12:00 pm – 2:00 pm	**Badge Pick Up for pre-registered attendees only** *Lagoon Plaza*
2:00 pm – 5:00 pm	**Badge Pick Up and on-site registration** *Corwin Pavilion Lobby*
2:00 pm – 2:30 pm	**Welcome** Lily Chen, *NIST* **NIST Opening Remarks** Dustin Moody, *NIST*
2:30 pm – 3:30 pm	**Session I: Accepted Papers** Session Chair: Angela Robinson, *NIST*
2:30 – 2:50	**Measuring TLS key exchange with post-quantum KEM** Presented by: Nick Sullivan, *Cloudflare*
2:50 – 3:10	**Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH** Presented by: Douglas Stebila, *University of Waterloo*
3:10 – 3:30	**Implementing and Benchmarking Seven Round 2 Lattice-Based Key Encapsulation Mechanisms Using Software/Hardware Codesign Approach** Presented by: Kris Gaj, *George Mason University*
3:30 pm – 4:00 pm	**Break**
4:00 pm – 5:00 pm	**Session II: Industry Panel** Moderator: John Kelsey, *NIST* ***Panelists:*** Matt Campagna, *Amazon Web Services* Scott Fluhrer, *Cisco* Brian LaMacchia, *Microsoft* Nataraj (Raj) Nagaratnam, *IBM* Nick Sullivan, *Cloudflare*

Friday, August 23, 2019

8:00 am – 5:00 pm	**Badge Pick Up and on-site registration** *Corwin Pavilion Lobby*
8:30 am – 9:45 am	**Session III: : Round 2 Team Updates** Session Chair: Dustin Moody, *NIST*
8:30 – 8:45	**CRYSTALS-Dilithium** Presented by: Vadim Lyubashevsky, *IBM Research Zurich*
8:45 – 9:00	**qTesla** Presented by: Patrick Longa, *Microsoft Research*
9:00 – 9:15	**Falcon** Presented by: Thomas Prest, *PQShield*
9:15 – 9:30	**Picnic** Presented by: Greg Zaverucha, *Microsoft*
9:30 – 9:45	**Sphincs+** Presented by: Andreas Hülsing, *Eindhoven University of Technology*
9:45 am – 10:15 am	**Break**
10:15 am – 11:55 am	**Session IV: Accepted Papers** Session Chair: Carl Miller, *NIST*
10:15 – 10:35	**Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures** Presented by: Yilei Chen, *Visa Research*
10:35 – 10:55	**Simple, Fast and Constant-Time Gaussian Sampling over the Integers for Falcon** Presented by: Melissa Rossi, *Thales & École normale supérieure*
10:55 – 11:15	**Sharing the LUOV: Threshold Post-Quantum Signatures** Presented by: Daniele Cozzo, *KU Leuven*
11:15 – 11:35	**New Attacks on Lifted Unbalanced Oil Vinegar** Presented by: Jintai Ding, *Univesrity of Cincinnati*
11:35 – 11:55	**Visualizing size-security tradeoffs for lattice-based encryption** Presented by: Daniel J. Bernstein, *University of Illinois at Chicago*
11:55 am – 1:15 pm	**Lunch** *(De La Guerra Commons or UCEN Food Court)* for those staying off campus, tickets can be purchased in the lobby of De La Guerra Commons

Friday, August 23, 2019

1:15 pm – 2:15 pm	**Session V: Round 2 Team Updates** Session Chair: Daniel Smith-Tone, *NIST*
1:15 – 1:30	**LUOV** Presented by: Ward Beullens, *KU Leuven*
1:30 – 1:45	**Rainbow** Presented by: Jintai Ding, *University of Cincinnati*
1:45 – 2:00	**GeMMS** Presented by: Ludovic Perret, *Cryptonext*
2:00 – 2:15	**MQDSS** Presented by: Andreas Hülsing, *Eindhoven University of Technology*
2:15 pm – 2:45 pm	**Break**
2:45 pm – 3:45 pm	**Session VI: Accepted Papers** Session Chair: Rene Peralta, *NIST*
2:45 – 3:05	**Comparing proofs of security for lattice-based encryption** Presented by: Daniel J. Bernstein, *University of Illinois at Chicago*
3:05 – 3:25	**Tighter proofs of CCA security in the quantum random oracle model** Presented by: Mike Hamburg, *Rambus Security Division*
3:25 – 3:45	**On non-tightness of security reductions for key encapsulation mechanism in the quantum random oracle model** ****Will be presented via video**** Presented by: Haodong Jiang, *Chinese Academy of Sciences*
3:45 pm – 4:45 pm	**Session VII: Round 2 Team Updates** Session Chair: Quynh Dang, *NIST*
3:45 – 4:00	**FrodoKEM** Presented by: Chris Peikert, *University of Michigan*
4:00 – 4:15	**CRYSTALS-Kyber** Presented by: Peter Schwabe, *Radboud University*
4:15 – 4:30	**Saber** Presented by: Jan-Pieter D'Anvers, *KU Leuven*
4:30 – 4:45	**SIKE** Presented by: David Jao, *University of Waterloo*

Saturday, August 24, 2019

8:00 am – 12:00 pm	**Badge Pick Up and on-site registration** *Corwin Pavilion Lobby*
8:30 am – 10:00 am	**Session VIII: Round 2 Team Updates** Session Chair: Yi-Kai Liu, *NIST*
8:30 – 8:45	**Classic McEliece** Presented by: Edoardo Persichetti, *Florida Atlantic University*
8:45 – 9:00	**BIKE** Presented by: Rafael Misoczki, *Intel*
9:00 – 9:15	**HQC** Presented by: Philippe Gaborit, *University of Limoges*
9:15 – 9:30	**ROLLO** Presented by: Philippe Gaborit, *University of Limoges*
9:30 – 9:45	**RQC** Presented by: Loic Bidoux, *Worldine*
9:45 – 10:00	**LEDAcrypt** Presented by: Alessandro Barenghi, *Politecnico di Milano*
10:00 am – 10:30 am	**Break**
10:30 am – 12:30 pm	**Session IX: Accepted Papers** Session Chair: Daniel Apon, *NIST*
10:30 – 10:50	**A Lightweight Implementation of NTRUEncrypt for 8-bit AVR Microcontrollers** Presented by: Johann Großschädl, *University of Luxembourg*
10:50 – 11:10	**Optimised Lattice-Based Key Encapsulation in Hardware** Presented by: James Howe, *PQShield*
11:10 – 11:30	**Feasibility and Performance of PQC Algorithms on Microcontrollers** Presented by: Jens-Peter Kaps, *George Mason University*
11:30 – 11:50	**Energy Consumption of Round 2 Submissions for NIST PQC Standards** Presented by: Crystal Roma, *University of Waterloo*
11:50 – 12:10	**A Hardware Evaluation Study of NIST Post-Quantum Cryptographic Signature schemes** Presented by: Deepraj Soni, *New York University*
12:10 – 12:30	**pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4** Presented by: Matthias T. Kannwischer, *Radboud University*
12:30 pm – 1:45 pm	**Lunch** *(De La Guerra Commons)* for those staying off campus, tickets can be purchased in the lobby of De La Guerra Commons

Saturday, August 24, 2019

1:45 pm – 3:15 pm	**Session X: Round 2 Team Updates** Session Chair: Ray Perlner, *NIST*
1:45 – 2:00	**NTRU** Presented by: John Schanck, *University of Waterloo*
2:00 – 2:15	**NTRUPrime** Presented by: Daniel J. Bernstein, *University of Illinois at Chicago*
2:15 – 2:30	**Three Bears** Presented by: Mike Hamburg, *Rambus Security Division*
2:30 – 2:45	**LAC** Presented by: Zhenfei Zhang, *Algorand*
2:45 – 3:00	**New Hope** Presented by: Thomas Poeppelmann, *Infineon Technologies AG*
3:00 – 3:15	**Round5** Presented by: Markku-Juhani O. Saarinen, *PQShield* Oscar Garcia-Morchon, *Philips Research*
3:15 pm – 4:00 pm	**Next Steps/Open Problems/Adjourn** Yi-Kai Liu, *NIST*

Sleeping Rooms are in Santa Rosa and Anacapa Halls
Meeting Room: Corwin Pavilion

NO BADGE PICK UP WEDNESDAY
Badge pick up will start at noon on Thursday

Interactive Campus Map: https://map.ucsb.edu/