The 3rd Yanqi Lake International PQC Standardization and Application Workshop

Conference Date: July 7th-8th, 2023(GMT+8, Beijing Time)
Conference Venue: Liaoning Hall A, 8th Floor, Liaoning International Hotel, North 4th Ring Road West Road, Haidian District, Beijing, China.

	July 7th, 2023	
TIME	**CONFERENCE PROGRAMME**	**HOST**
7:50-8:50	**Registration**	
8:50-9:00	**Welcome Address** Jintai Ding	**Jintai Ding**
9:00-10:15	**NIST New PQC Signature Round (Online)** Dustin Moody, *National Institute of Standards and Technology*	
10:15-10:30	**Tea Break**	
10:30-11:15	**PQC Migration: AWS perspective (Online)** Matthew Campagna, *Amazon Web Services*	**Hong Xiang**
11:15-12:00	**UOV and TUOV, A New Provable Secure Signature** Jintai Ding, *Yau Mathematical Sciences Center, Tsinghua University & Yanqi Lake Beijing Institute of Mathematical Sciences and Applications*	
12:00-13:15	**Lunch Buffet** Shenganhui Buffet Restaurant, 1st Floor, Liaoning International Hotel	
13:15-13:45	**Challenges and Solutions to Post-Quantum Secure Messaging（Online）** Shuichi Katsumata, *PQShield Ltd & AIST*	**Chengdong Tao**
13:45-14:15	**QR-UOV** Hiroki Furue, *University of Tokyo*	
14:15-14:45	**SNOVA(Online)** Lih-Chung Wang, *National Dong Hwa University*	
14:45-15:30	**VOX and PROV(Online)** Jacques Patarin, *University of Versailles* Benoît Cogliati, *CISPA Helmholtz Center for Information Security*	
15:30-15:45	**Tea Break**	
15:45-16:30	**Migration to PQC: The road never taken (Online)** Jihoon Cho, *Samsung SDS*	**Xianhui Lu**
16:30-17:00	**Implementing UOV（Online）** Ming-Shing Chen, *Academia Sinica*	

17:00-17:30	**PQC Standardization in Korea** Kwanjo Kim, *Korea Advanced Institute of Science & Technology*	
17:30-18:00	**Quantum-safe PKI for the German administration(Online)** Kaveh Bashiri, *Federal Office for Information Security, BSI, Germany*	
18:00-20:30	**Dinner** Shenyang Hall, 7th Floor, Liaoning International Hotel	

July 8th, 2023

TIME	CONFERENCE PROGRAMME	PRESENTER
09:00-09:30	**Advances in Quantum-Resistant Cryptography and Standardization** Xianhui Lu, *Institute of Information Engineering, Chinese Academy of Sciences*	**Jintai Ding**
09:30-10:00	**Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms** Youming Qiao, *University of Technology Sydney*	
10:00-10:30	**Cryptanalysis of GeMSS** Chengdong Tao, *Yanqi Lake Beijing Institute of Mathematical Sciences and Applications*	
10:30-11:00	**Tea Break**	
11:00-11:30	**Compact Lattice Gadget and Its Applications to Hash-and-Sign Signatures** Yang Yu, *Tsinghua University*	**Bei Liang**
11:30-12:00	**An efficient lattice based threshold signature with proactive security** Long Chen, *Institute of Software Chinese Academy of Sciences*	
12:00-13:30	**Lunch Buffet** Shenganhui Buffet Restaurant, 1st Floor, Liaoning International Hotel	
14:00-15:00	**Panel discussion: PQC standardization and Key Technologies of U.S., Japan and Korea**	**Hong Xiang**
	END	