第一届雁栖湖国际抗量子密码标准化与应用研讨会暨第五届亚洲抗量子密码论坛

The 1st Yanqi Lake International PQC Standardization and Application Workshop & the 5th Asia PQC Forum

研讨会采用线上/线下结合的方式，欢迎各位同仁在线参与。

Zoom info:

All times are in China Standard Time.

Time: 2021/04/24-25

https://zoom.com.cn/j/3610386975?pwd=YW4yeWFKbkVjcWtVSXFxYnZVUnQ0Zz09

Meeting ID: **361 038 6975**

Password: **BIMSA**

2021.4.23	
15:00	**Registration**

2021.4.24	
8:55	**Opening Speech**
9:00	**Toward a more resilient quantum-safe future** *Michele Mosca* (online) *University of Waterloo*
10:00	**Computational Problems in Post-Quantum Cryptography** *Tsuyoshi TAKAGI* (online) *Tokyo University*
10:30	**Side-channel attacks on isogeny-based cryptosystems** *David Jao* (online) *University of Waterloo*
11:00	**参与国际国内抗量子密码标准设计的经验与体会** *路献辉* *中科院信工所*
11:30	**格密码方案的攻击与防护：历史、现状与未来** *潘彦斌* *中科院数学与系统所*
14:00	**实用格基签名及参数调优** *赵运磊* *复旦大学*

14:30	**TLS 1.x：面向互联网安全的抗量子认证密钥交换方案设计与分析** *程池* *中国地质大学（武汉）*
15:00	**不可逆群的构造与应用** *陈一镭* *清华大学*
15:30	**抗量子密码方案的量子安全性分析：从 FO 变换开始** *江浩东* *中科院软件所*
16:00	**Perspectives on PQC from Industry** *Jihoon Cho* (online) *Samsung SDS*
16:30	**河防口长城**
19:00	**晚宴**

2021.4.25

9:00	**Round 3 of the NIST PQC Competition** *Dustin Moody* (online) *NIST*
10:00	**Preparing Industry for the Quantum Age** *Atsushi Yamada* (online) *ISARA*
10:30	**央行数字货币设计的安全、隐私与合规：现状与挑战** *向宏* *重庆大学*
11:00	**Can lattice signature be as efficient as lattice encryption?** *黄桂芳* *中科院信工所*
11:30	**Post-quantum security of key encapsulation mechanisms** *张振峰* *中科院软件所*
12:00	**后量子密码学发展方向和重大挑战** *丁津泰* *清华大学/北京雁栖湖应用数学研究院（BIMSA）*