

2024 前瞻後量子密碼資安國際合作： 回顧與展望研討會

International Collaboration on Post-Quantum Cryptography and
Cybersecurity: Retrospect and Prospects, 2024.

Date: 2024.12.27

Location: Humanities and Social Sciences Building,
International Conference Hall

Academia Sinica Crypto Group



議程資訊 Tentative Schedule

Time	Speaker	Title
0900-0910	Welcome	
0910-0955	楊柏因 (Bo-Yin Yang)	"Safegcd2: More stories of constant-time inversions"
0955-1025	Coffee break	
1025-1110	蔡明憲 (Ming-Hsien Tsai)	"Verifying postquantum cryptography"
1110-1155	丁津泰 (Jintai Ding)	"On Lattice Cryptanalysis Today"
1155-1325	Lunch	
1325-1410	鐘楷閔 (Kai-Min Chung)	Complexity Theory for Quantum Promise Problems and Cryptography
1410-1455	郎丹雅+雷橋森 (Tanja Lange, Jonathan Levin)	"PQConnect"
1455-1525	Coffee break	
1525-1610	狄傑比 (Daniel J. Bernstein)	"CryptAttackTester"