

Announcing PQCrypto 2011

Chen-Mou Cheng

National Taiwan University



September 30, 2011

Only a few days before Asiacrypt 2011

PQCrypto 2011, Nov 29 — Dec 2

will take place in Taipei, Taiwan.

Registration is now open.

This is the 4th International Conference on
Post-Quantum Cryptography.

Program Chair: Bo-Yin Yang (Academia Sinica)
General chair: Chen-Mou Cheng (National Taiwan University)

Post-Quantum Cryptography

- ▶ (Public-key) cryptosystems that have the potential to resist possible future quantum computers such as:
 - ▶ hash-based Merkle-type signature schemes,
 - ▶ lattice-based cryptosystems,
 - ▶ code-based cryptosystems,
 - ▶ multivariate cryptosystems, and
 - ▶ quantum cryptographic schemes;
- ▶ Classical and quantum attacks including side-channel attacks on the post-quantum cryptosystems;
- ▶ Security models for the post-quantum era.

More reasons to come to Taipei





















PQCrypto 2011

Nov 29 – Dec 2, Taipei

<http://pq.crypto.tw/pqc11/>