PQCrypto 2011

The Fourth International Workshop on Post-Quantum Cryptography
Taipei, Taiwan, November 29 - December 2, 2011

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

First Call for Participation

The PQCrypto conference serves as a forum for researchers to present results and exchange ideas in post-quantum cryptography. Authors are invited to submit original research papers on all technical aspects of cryptographic research related to a future world with large quantum computers. The topics include (but are not restricted to):

- (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.

PQCrypto 2011 will be held at the International House by Howard Plaza, conveniently accessible by subway and many busses and situated in the middle of Downtown Taipei right next to National Taiwan University. Special rates (less than 50 EUR/night for a single including internet and breakfast) have been blocked off at this nice hotel http://intl-house.howard-hotels.com.tw/.
It is being organized by the School of EECS at National Taiwan University and sponsored by the Intel Connected Context Computing Center and Academia Sinica.

Contact Information of Organizers

Bo-Yin Yang by@crypto.tw Academia Sinica, Taipei, Taiwan

Chen-Mou Cheng doug@crypto.tw
National Taiwan University, Taipei 106, Taiwan

Webmaster: Peter Schwabe peter@cryptojedi.org