ASK

The Asian Workshop on Symmetric Key Cryptography

ASK

- **Founded by Jian Guo and Thomas Peyrin in 2011**
- http://ask.crypto.sg/

ASK

- **To promote research on symmetric key cryptography in Asia**
  - block ciphers
  - stream ciphers
  - hash functions
  - mode operations
  - analysis, design, proof
  - side channel analysis, implementation

ASK

- **Invited talk sessions (morning)**
  - respectable speakers
  - advanced results
  - survey on popular topics
- **Working group sessions (afternoon)**
  - small discussion group
  - particular research topic

ASK

- ASK 2011 (Jian Guo and Thomas Peyrin)
  - Nanyang Technological University, Singapore
  - #attendees: 44
  - http://web.spms.ntu.edu.sg/~ask/2011/
- ASK 2012 (Tetsu Iwata and Lei Wang)
  - Nagoya University, Japan
  - #attendees: 28
  - http://www1.spms.ntu.edu.sg/~ask/2012/
- ASK 2013 (Meiqin Wang and Hongbo Yu)
  - Shandong University, China
  - #attendees: 52
  - http://www.infosec.sdu.edu.cn/ask2013/

ASK

- **Attendees from various countries**
  - Australia, China, India, Japan, Korea, Singapore, Vietnam
- **Attendees outside Asia**
  - Belgium, France, Netherlands
  - We also welcome researchers outside Asia

ASK

- **Results accepted to IACR conferences/ workshops, and other conferences.**
- **Examples**
  - Jiqiang Lu: *A Methodology for Differential-Linear Cryptanalysis and Its Applications*, FSE 2012
  - Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong and Jian Zou: *(Pseudo) Preimage Attack on Reduced-Round Grøstl Hash Function and Others*, FSE 2012
  - Liting Zhang, Wenling Wu, Han Sui and Peng Wang: *3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound*, ASIACRYPT 2012
  - Jian Guo, Yu Sasaki, Lei Wang and Shuang Wu: *Cryptanalysis of HMAC/NMAC-Whirlppol*, ASIACRYPT 2013

ASK

- **Interested of hosting?**

- **Contacts**
  - Jian Guo (ntu.guo@gmail.com)
  - Thomas Peyrin (thomas.peyrin@gmail.com)

ASK 2014

ASK 2014

- **Venue:**
  - Society for Electronic Transactions and Security (SETS), Chennai, **India**
- **Contact:**
  - Nalla Anandakumar (nallananth@gmail.com)
  - Somitra Kumar Sanadhya (somitra@iiitd.ac.in)