

ASK

Tetsu Iwata and Lei Wang

ASK 2012

Tetsu Iwata and Lei Wang

ASK 2012

The Second **A**sian Workshop on
Symmetric **K**ey Cryptography

Tetsu Iwata and Lei Wang

ASK 2012

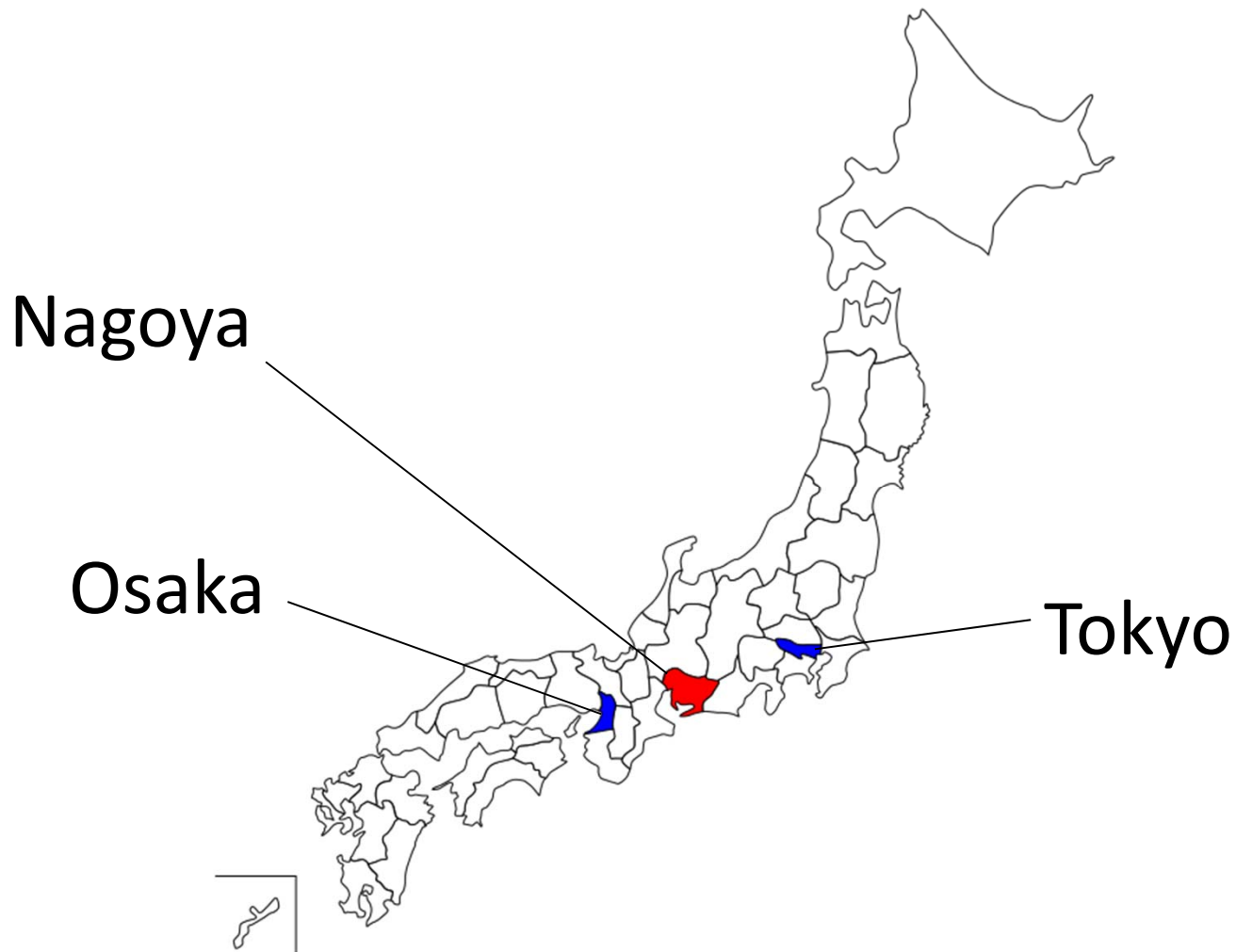
The Second Asian Workshop on Symmetric Key Cryptography

- Date: August 27-29, 2012
Monday-Wednesday after CRYPTO
- Venue: Nagoya University, Nagoya, Japan
- Web:
<http://web.spms.ntu.edu.sg/~ask/2012/>
- Contact: Tetsu Iwata and Lei Wang



ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography



ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

- to promote research on symmetric key cryptography in Asia
 - block ciphers, stream ciphers, hash functions,...
 - analysis, designs, proofs, implementations,...
 - The first ASK 2011 was held in Singapore
 - we also welcome participants from outside of Asia

ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

- Follow the spirit of ECRYPT
 - Morning: Invited talks (about 8-12 talks)
 - Afternoon: Working group sessions
 - work on particular research topics in small working groups

ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

A Methodology for Differential-Linear Cryptanalysis and Its
Applications*
(Extended Abstract)

Jiqiang Lu

Institute for Infocomm Research,
Agency for Science, Technology and Research
1 Fusionopolis Way, #19-01 Connexis, Singapore 138632
lvjiqiang@hotmail.com


- FSE 2012

ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

- Program from ASK 2011

Monday, August 29 @ SPMS-LT5 (SPMS-03-08) 3rd floor	
09:00 - 09:15	Welcome Address, Jian Guo and Thomas Peyrin
09:15 - 10:00	Shoichi Hirose: Security Reductions of Cryptographic Hash Functions [slides]
10:00 - 10:30	Josef Pieprzyk: Differential Distinguishers for Block Ciphers [slides]
10:30 - 11:00	COFFEE BREAK @ MAS Atrium 3rd floor
11:00 - 12:30	Jiqiang Lu: A Few Techniques for Block Cipher Cryptanalysis [slides]
12.30 - 14:00	LUNCH BREAK @ MAS Atrium 3rd floor
14.00 - 16:00	working groups session 1
16.00 - 16:45	COFFEE BREAK @ MAS Atrium 3rd floor
16.45 - 18:00	working groups session 2
18:00 - 19:00	Wrapping up @ SPMS-MAS-05-36



ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

(Pseudo) Preimage Attack on Round-Reduced Grøstl Hash
Function and Others

Shuang Wu¹, Dengguo Feng¹, Wenling Wu¹, Jian Guo², Le Dong¹, and Jian Zou¹

¹ State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences.

² Institute for Infocomm Research, Singapore.

wushuang@is.iscas.ac.cn

- FSE 2012

ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography



Acknowledgement The authors would like to thank Kazumaro Aoki, Keting Jia, Mohammad Ali Orumiehchiha, Somitra Sanadhya, and Chunhua Su for their inspiring suggestions during the ASK 2011 workshop. The authors would also thank Lei Wang for useful discussions, and reviewers of FSE 2012 for helpful comments. This work is supported by the National Natural Science Foundation of China(No.60873259) and the Knowledge Innovation Project of The Chinese Academy of Sciences.

- FSE 2012

ASK 2012

The Second Asian Workshop on Symmetric Key Cryptography

- Date: August 27-29, 2012
- Venue: Nagoya University, Nagoya, Japan
- Web:
<http://web.spms.ntu.edu.sg/~ask/2012/>
- Contact:
 - Tetsu Iwata (iwata@cse.nagoya-u.ac.jp)
 - Lei Wang (lei.wang@uec.ac.jp)