DIAC 2016 and ASK 2016 in Nagoya

Tetsu Iwata, Shiho Moriai, Yu Sasaki

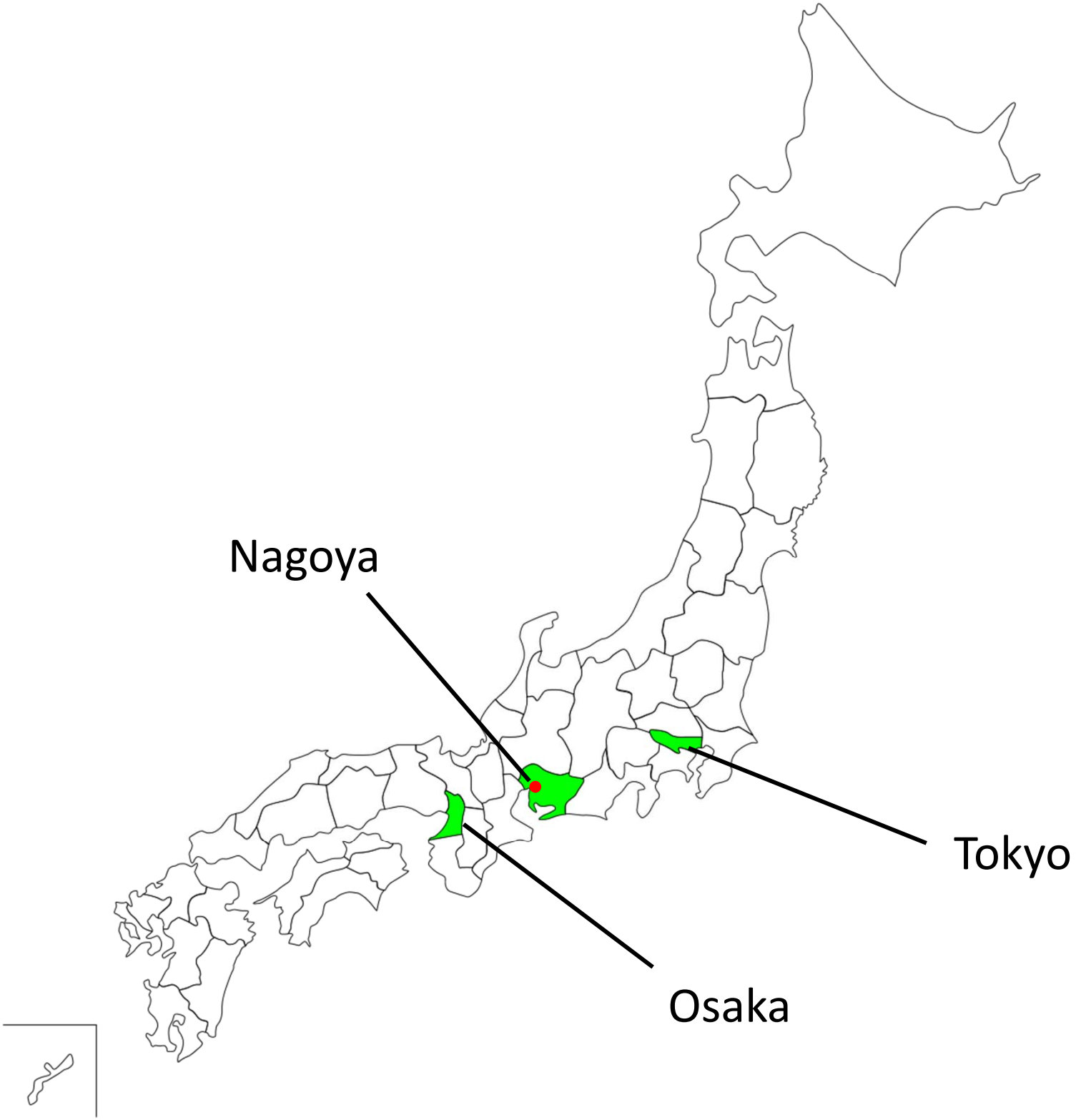
FSE 2016 Rump Session

March 22, 2016

Bochum, Germany

DIAC 2016 and ASK 2016 in Nagoya

- DIAC: Directions in Authenticated Ciphers
  - September 26-27, 2016
  - Organizers: Tetsu Iwata and Shiho Moriai
- ASK: Asian Workshop on Symmetric Key Cryptography
  - September 28-30, 2016
  - Organizers: Tetsu Iwata and Yu Sasaki
- Both in Nagoya, Japan
- Web sites will be opened soon


Nagoya
Tokyo
Osaka

Nagoya

- a few direct flights from Europe/USA
- many direct flights from Asian countries
- High speed train “Shinkansen” and domestic flights from Tokyo

DIAC 2016

- DIAC: Directions in Authenticated Ciphers
  - September 26-27, 2016, Nagoya, Japan
  - CAESAR, Competition for Authenticated Encryption: Security, Applicability, and Robustness
  - To evaluate the state of the art in authenticated encryption and gather community input regarding desired future directions

ASK 2016

- ASK: Asian Workshop on Symmetric Key Cryptography
  - September 28-30, 2016, Nagoya, Japan
    - Invited talks in morning sessions
    - group discussions for research collaboration in afternoon sessions

ASK 2016

- Two papers at FSE 2016 from ASK 2015!

Key Recovery Attack against 2.5-round π-Cipher

Christina Boura[1], Avik Chakraborti[2], Gaëtan Leurent[3], Goutam Paul[2], Dhiman Saha[4], Hadi Soleimany[5,6] and Valentin Suder[7]

Cryptanalysis of Reduced NORX

Nasour Bagheri[1], Tao Huang[2], Keting Jia[3,4], Florian Mendel[5] and Yu Sasaki[2,6]

Images from FSE 2016 pre-proceedings

DIAC 2016 and ASK 2016 in Nagoya

- DIAC: Directions in Authenticated Ciphers
  - September 26-27, 2016
- ASK: Asian Workshop on Symmetric Key Cryptography
  - September 28-30, 2016
- Both in Nagoya, Japan