

# All You Need Is Fault: Zero-Value Attacks on AES and a New $\lambda$ -detection M&M

---

Haruka Hirata, Daiki Miyahara, Victor Arribas, Yang Li, Noriyuki Miura, Svetla Nikova,  
Kazuo Sakiyama

The University of Electro-Communications, Osaka University, KU Leuven, Rambus Inc.

This is some text in the first frame. This is some text in the first frame. This is some text in the first frame.

▶ AAA

- ▶ AAA
- ▶ BBB
  - ▶ CCC

$$\lambda(data) * \lambda(\alpha) = \lambda(data * \alpha)$$