TOSHIBA

Leading Innovation

COTORI™: Cryptosystems on Tori

Tomoko Yonemura, Taichi Isogai, Hirofumi Muratani,
and Yoshikazu Hanatani (Toshiba Corporation)

hirofumi.muratani@toshiba.co.jp

Rump session, CRYPTO2012, Santa Barbara
August, 2012

Toshiba Group contributes to
the sustainable future of planet Earth.

COTORI™

- **COTORI™: Cryptosystems on TORI**
  - it is pronounced in the same way as 小鳥, *ko-to-ri* / ことり.

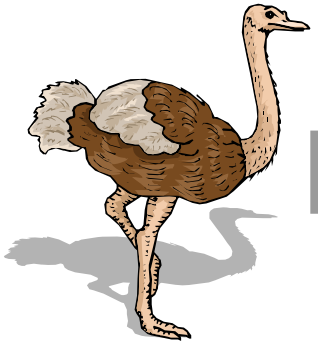
- **Main Features:**
  - discrete logarithm assumption in the finite field
  - reduced key-size and compressed expression

    T. Yonemura, T. Isogai, H. Muratani, and Y. Hanatani, “Factor-4 and 6 (De)compression for Values of Pairing using Trace Maps,” Pairing 2012, 2012.

Key size can be reduced up to 1/6.

What needed more for COTORI™

- **More compression**



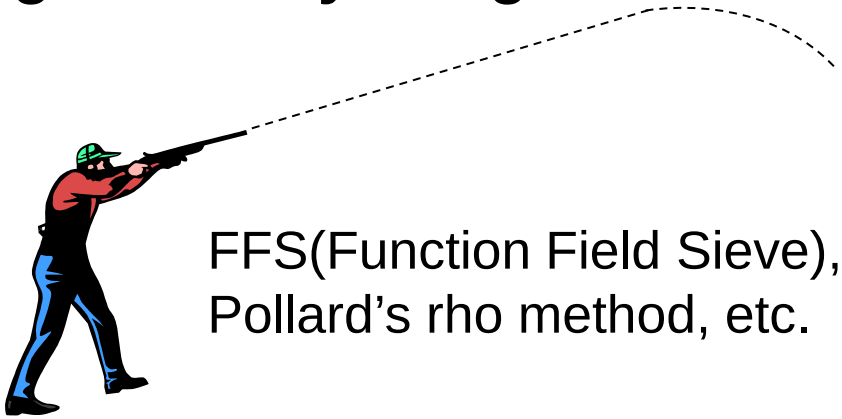
compression

1/6

compression

1/9, 1/12, etc.

- **Enough security margin**



FFS(Function Field Sieve),
Pollard's rho method, etc.

- **Your comments**

TOSHIBA
Leading Innovation