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
• **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


Key size can be reduced up to 1/6.
What needed more for COTORI™

• More compression

• Enough security margin
  
  FFS(Function Field Sieve), Pollard’s rho method, etc.

• Your comments
Thank you for your attention!