Advanced FORK-256

Presented by Seokhie Hong

hsh@cist.korea.ac.kr

CIST
Center for Information Security Technologies

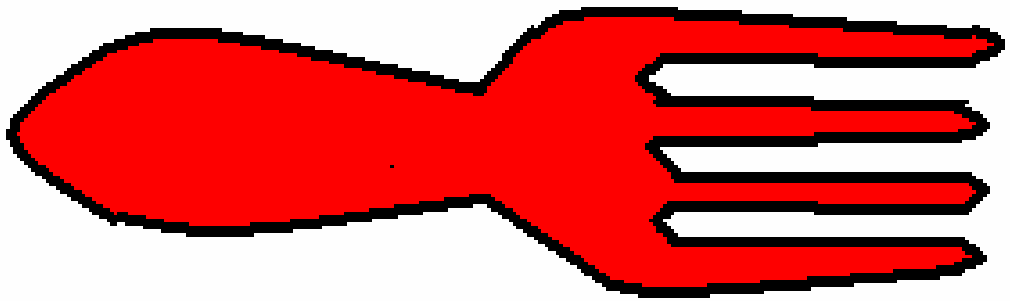
FORK-256

Introduction to FORK-256

- The security of hash functions has recently become one of the hottest topics in the design and analysis of cryptographic primitives.

- FORK-256 : a hash function that was proposed by Hong et al. in 2006
  - The compression function of FORK256 consists of 4 Branches.
  - adopt the message word ordering instead of the message word extension.
  - The performance of the new hash function is at least 30% better than that of SHA-256 in software.

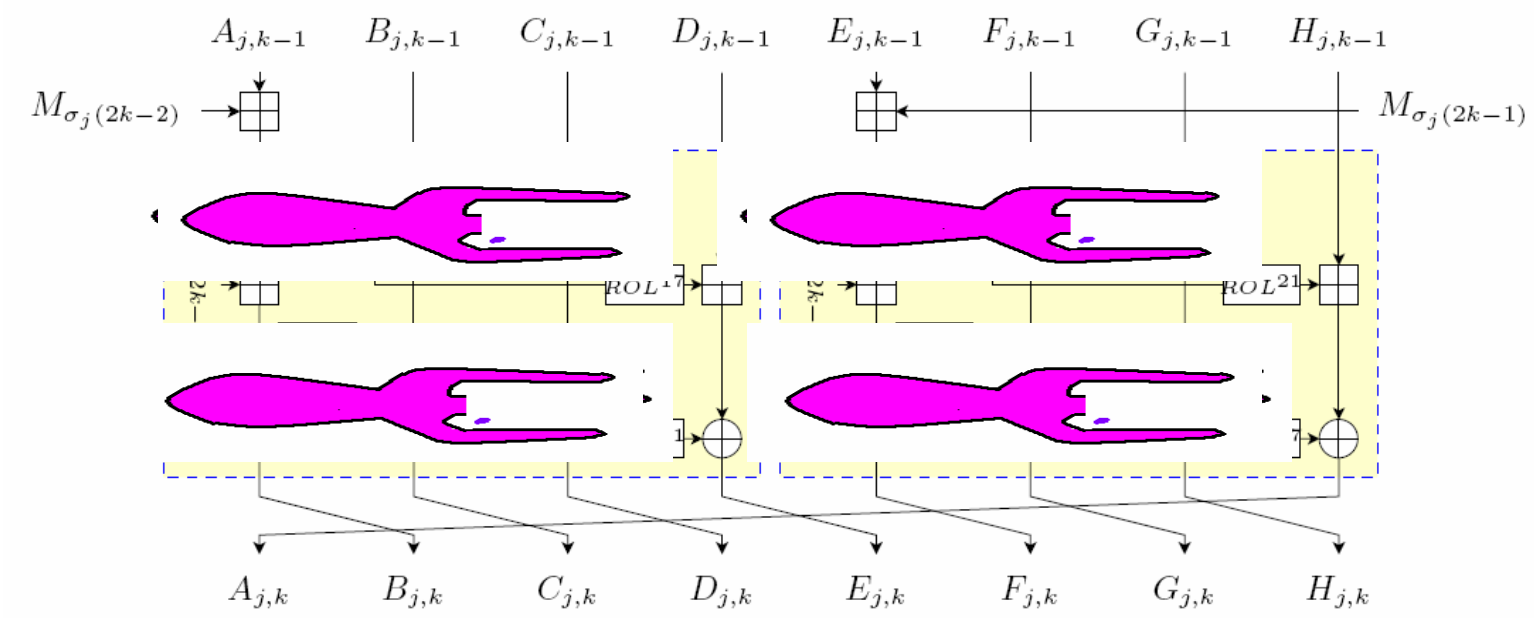
Fork



Old FORK-256

Step transformation of branch j of FORK-256

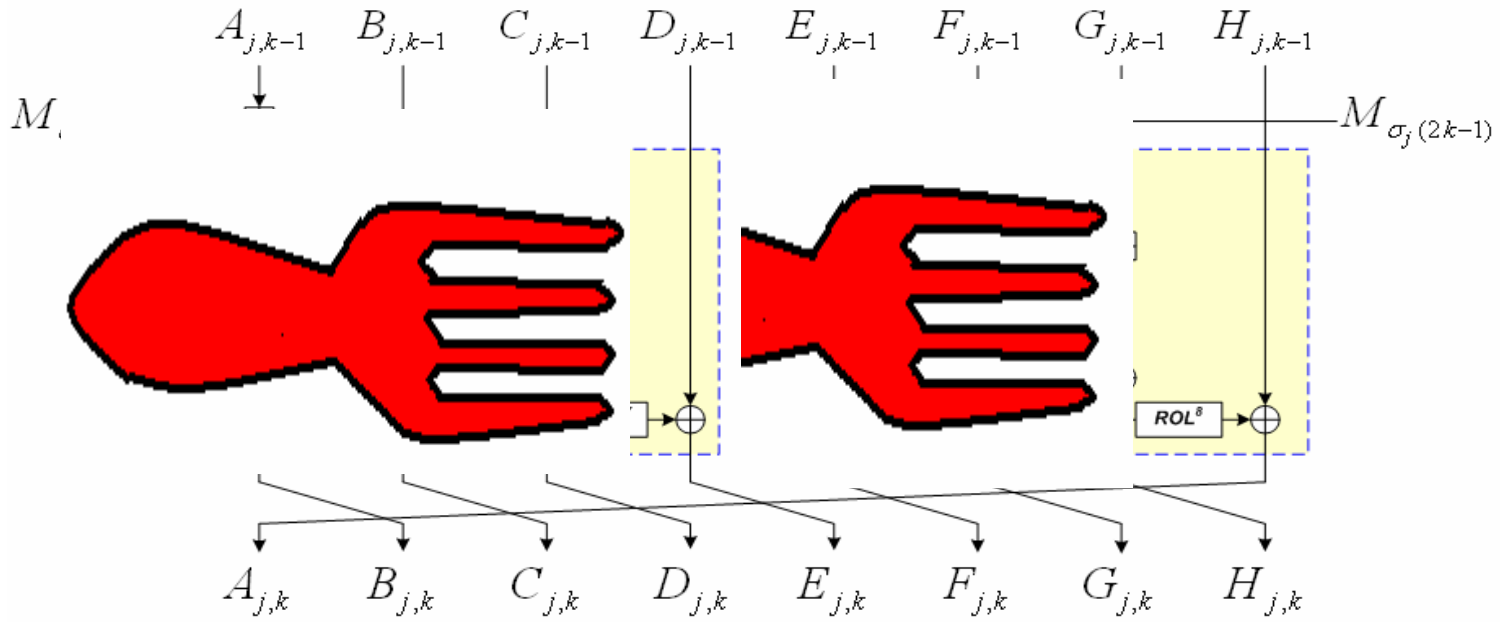
- $f(x) = x + (x^{<<<7} \oplus x^{<<<22}) \bmod 2^{32}$ $\quad g(x) = x + (x^{<<<13} \oplus x^{<<<27}) \bmod 2^{32}$



Advanced FORK-256

Step transformation of branch j of FORK-256

- $f(x) = x \oplus x^{<<<15} \oplus x^{<<<27}$
- $g(x) = x + (x^{<<<7} \oplus x^{<<<25}) \bmod 2^{32}$



Q&A

Thank you for your attention