Advanced FORK-256

Presented by Seokhie Hong

hsh@cist.korea.ac.kr
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
Step transformation of branch j of FORK-256

\[ f(x) = x + (x^{\ll 7} \oplus x^{\ll 22}) \mod 2^{32} \]

\[ g(x) = x + (x^{\ll 13} \oplus x^{\ll 27}) \mod 2^{32} \]
Step transformation of branch j of FORK-256

\[ f(x) = x \oplus x^{\ll 15} \oplus x^{\ll 27} \]
\[ g(x) = x + (x^{\ll 7} \oplus x^{\ll 25}) \mod 2^{32} \]
Thank you for your attention