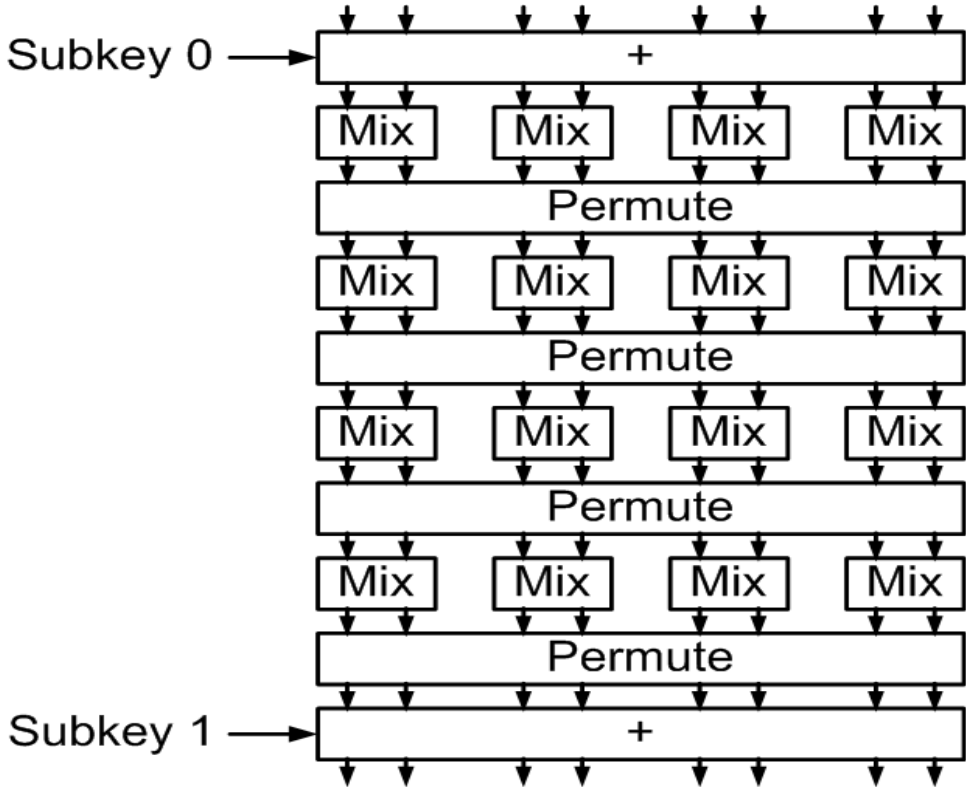
Skein

Fast, secure, and flexible



Fast in Software

- High throughput:
  - 6.0 cycles/byte on 64-bit reference platform
  - 17.4 cycles/byte on 32-bit reference platform
  - 303 cycles/byte on AVR 8-bit CPU
- Also very fast for small messages
  - Low per-message overhead

Fast in Hardware

- Skein-512 at 32 Gbit/s in 32 nm in only 58k gates
  - 32 nm = standard ASIC technology by 2012
  - 57 Gbit/s if processing two messages in parallel
  - Skein-1024 should be ≈ 1.8x *faster*

- Other implementations are slower
  - Probably due to inefficient adders
  - We are investigating further

Secure

- Conservative design
  - Best attack on Skein is 24 of 72 rounds
    [Su, Wu, Wu, Dong 2010]
  - Best attack on Threefish is 57 of 72 rounds
    [Rechberger, Khovratovich, Nikolic 2010]
- Builds on well-understood primitives
- Easy to understand and analyze
- Formal security arguments for the mode
  - Mathematical proof that a weakness in Skein implies a weakness in Threefish
  - We know how to analyze block ciphers

Next Round Tweak

- Change key schedule constant to a value without rotational symmetries
  - Minimal tweak
  - No effect on performance
  - Improves resistance against rotational attacks
  - No known affect on other cryptanalysis

- Best attack after tweak:
  - 33 of 72 rounds

Flexible

- Any output size
  - Simplifies many applications
- Extra features:
  - MAC mode eliminates HMAC overhead
  - KDF
  - PRNG
  - Stream cipher
  - Tree hash and tree MAC
    - Unlimited throughput through parallelism
    - Random-access hash and MAC

Skein Versions

- Skein-512: Our primary proposal
  - Any output size, including 256 and 512 bits
- Other variants available for standardization
  - Skein-1024 (1024-bit state)
    - Maximizes security margin
    - Within 10% of Skein-512 software speed
    - Any output size, including 512 bits (“wide pipe”)
  - Skein-256 (256-bit state)
    - Minimizes memory footprint

Implementation

- Easy to implement
- Existing implementations in:
  - Python, C, SPARK, Atmel AVR, x86, x64, C#, Java, C++, Ada, Cryptol, FPGA, ASIC
  - Parallel tree hashing

Free Block Cipher

- Threefish is the block cipher at the heart of Skein
- Wide block: 256-, 512-, and 1024-bit blocks
  - Solves the birthday bound problems we have with 128-bit block ciphers
- Tweakable: extra flexibility
- Provides a fallback for AES

Skein

Fast, secure, and flexible