The Skein Hash Function

First Hash Function Candidate Conference
Leuven, Belgium

26 February 2009

Niels Ferguson
Stefan Lucks
Bruce Schneier
Doug Whiting
Mihir Bellare
Tadayoshi Kohno
Jon Callas
Jesse Walker

Overview

- Fast
  - 6.1 cycles/byte on reference platform
  - More than 500 MB/s (4 Gb/s) per core.
- Secure
  - Uses block cipher (we know how to analyze those)
  - Conservative choice in # rounds
  - Formal security arguments for the mode
- Flexible
  - Lots of extra features

Design Philosophy

- Simplicity
- Optimize security per clock cycle
- Implementability on a variety of platforms
- Many simple rounds
- Maximum diffusion
- Simple CPU operations
- Flexibility

Critical Design Decisions

- A block cipher
  - There are many tools to analyze block ciphers
  - Streaming modes are not as well understood
- A tweakable block cipher
  - Message block offset in tweak replaces MD-strengthening
  - Considerable flexibility at no additional cost
- Matyas-Meyer-Oseas mode
  - Attacker controls plaintext input, not key input
- No table lookups (avoids side channel attacks)
- Three different internal state size, arbitrary output size

Skein Building Blocks

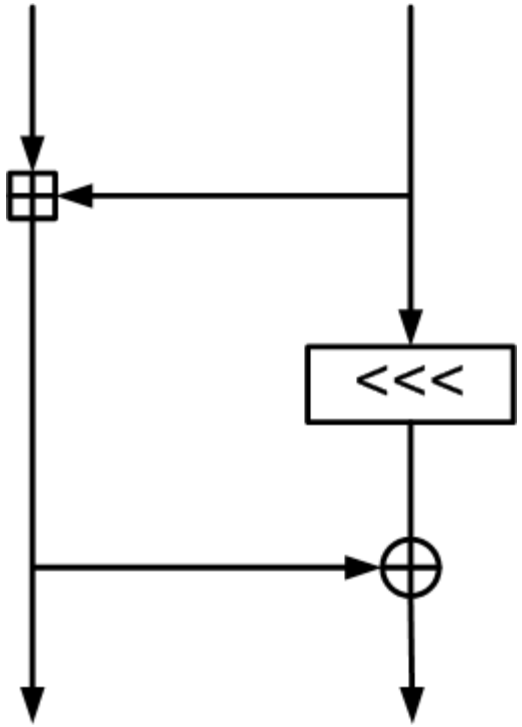
- Threefish large-block tweakable block cipher
- Unique Block Iteration(UBI)
- Optional Argument System

The Threefish Block Cipher

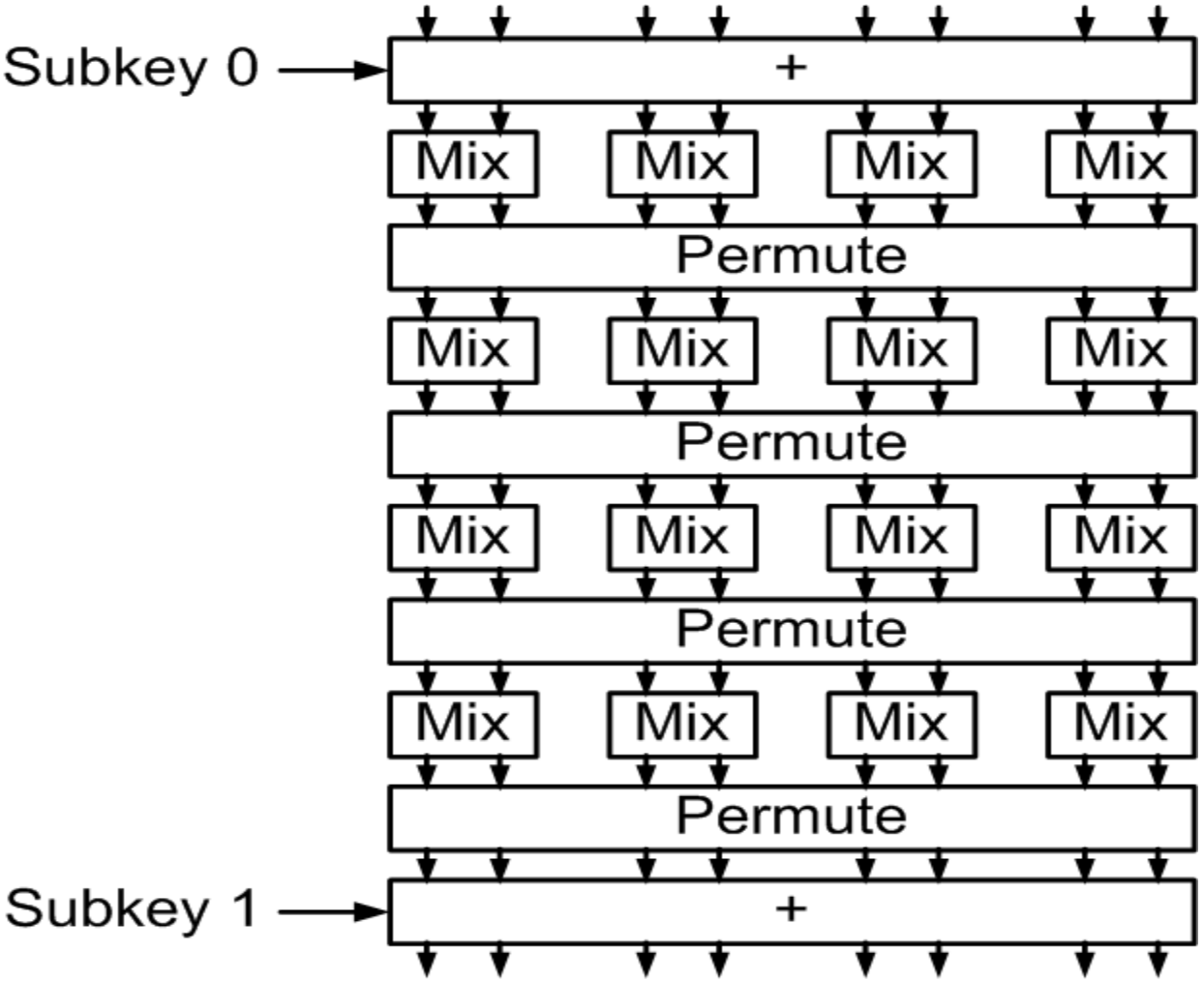
- Three versions
  - 256-bit block size
  - 512-bit block size
  - 1024-bit block size
- SP-network
- Based on very simple Mix function
- Simple key schedule

MIX Function

- Operates on two 64-bit words
- Uses only three primitive operations
- Takes 1 clock cycle (amortized) on reference platform



Four Rounds of Threefish-512



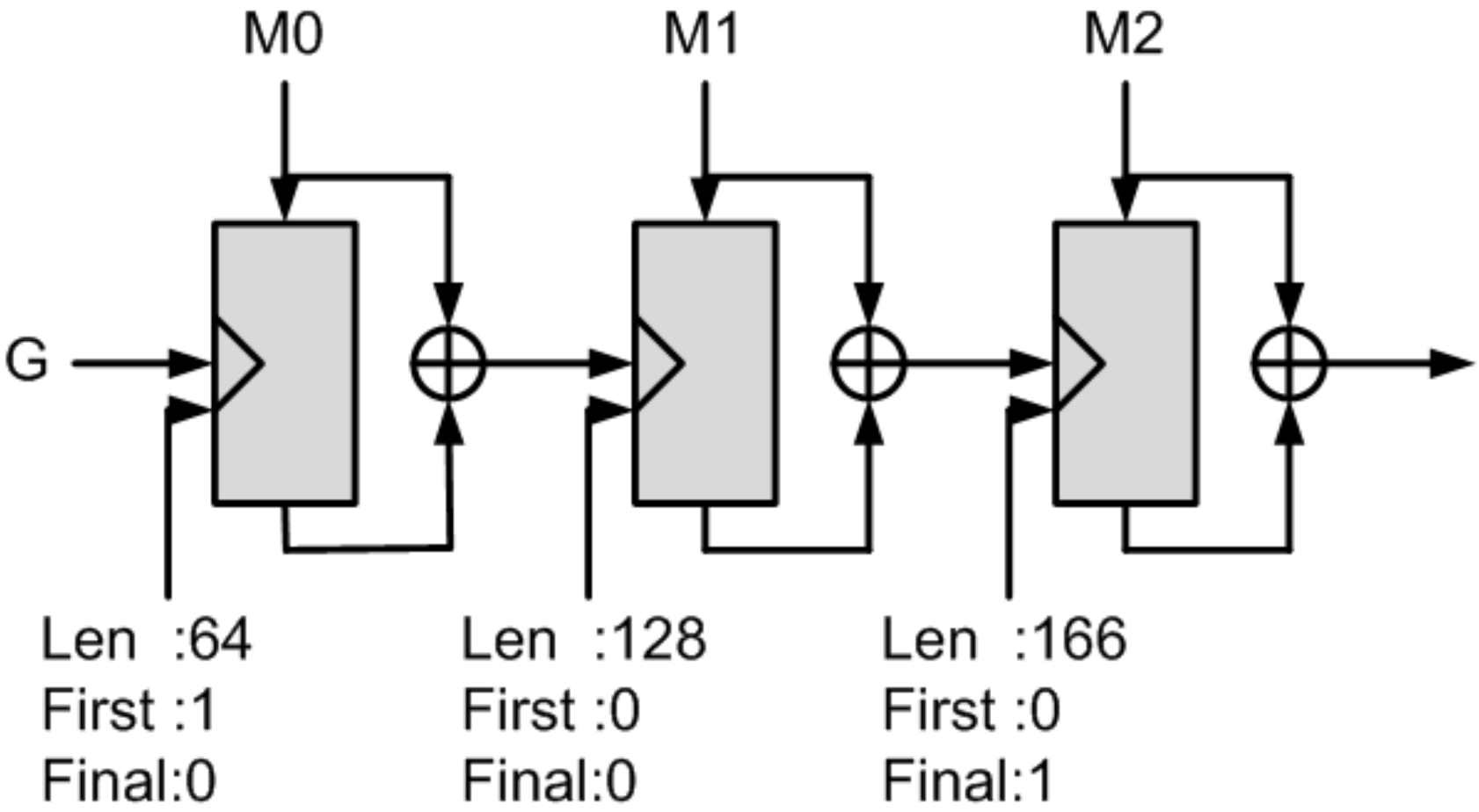
Threefish Key Schedule

- Inspired by Skipjack key schedule
- Key is the same size as the plaintext
- 128-bit Tweak value
- Each subkey is computed using three additions
- Counter to avoid slide attacks

Many Rounds

- Threefish has many rounds
  - Threefish-256 has 72
  - Threefish-512 has 72
  - Threefish-1024 has 80
- Each round is very simple, easy to analyze
  - But there are so many of them
- Full diffusion takes 9-11 rounds
- 7-8 full diffusions in the cipher
  - Compare with 5-7 for AES

UBI Compression Mode



Other Features

- Variable hash output size
- Tree hashing (with flexible leaf & node size)
- Large-block block cipher

- Through Optional Argument System:
  - Personalization
  - Zero-overhead MAC
  - Key Derivation Function
  - Password-based key derivation (PBKDF)
  - PRNG
  - Stream cipher (with nonce)

Security Proofs

- If the compression function is collision-resistant, then so is Skein.
- If Treefish is a tweakable PRP, then Skein is:
  - A PRF
  - A secure KDF
  - A secure MAC
  - A stream cipher
  - A PRNG
  - Secure when used in HMAC
- If Threefish is an ideal tweakable cipher, then Skein is indifferentiable from a random oracle.

Speed (in cycles/byte)

	Skein-256	Skein-512	Skein-1024
x64	7.6	6.1	6.5
x86 no SSE	32.8	32.5	37.5
x86 + SSE	21.6	20.1	25.5
Atmel AVR (8-bit CPU)	600 (C) 300 (asm)	600 (C)	625 (C)
FPGA (Xilinx Virtex-5)		>1 Gb/s	

~1000 cycles to hash a one-block message (Skein-512).

Memory Usage

- ~100 bytes RAM for Skein-256
  - SHA-256 needs > 128 bytes
- ~200 bytes RAM for Skein-512
  - SHA-512 needs > 256 bytes
- Many speed/code-size tradeoffs

Questions?

For more information: http://www.skein-hash.info