# The Hash Function Hamsi

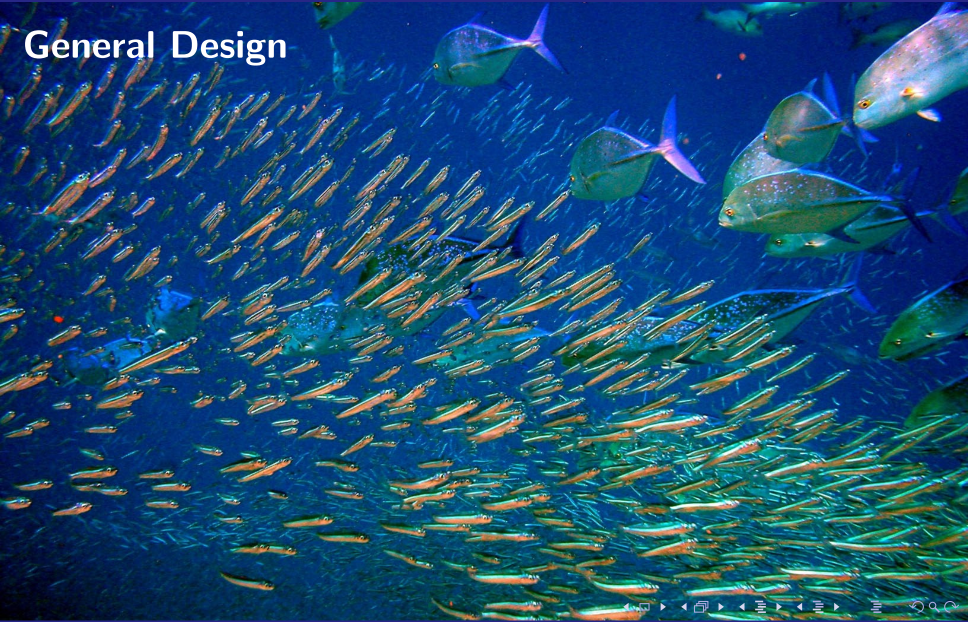
Özgül Küçük

Katholieke Universiteit Leuven

Second SHA-3 Conference
August 24, 2010

# Outline

# General Design



# Design Choices (1/3)

# Design Choices (1/3)

- Inspired by stream based hash algorithms

# Design Choices (1/3)

- Inspired by stream based hash algorithms
  - Short message blocks are processed with a light compression function in each iteration.

# Design Choices (1/3)

- Inspired by stream based hash algorithms
  - Short message blocks are processed with a light compression function in each iteration.
  - Mixing of message blocks into the state takes several iterations.

# Design Choices (1/3)

- Inspired by stream based hash algorithms
  - Short message blocks are processed with a light compression function in each iteration.
  - Mixing of message blocks into the state takes several iterations.
  - Security of compression function should be considered in the context of the iteration mode.

# Design Choices (1/3)

- Inspired by stream based hash algorithms
  - Short message blocks are processed with a light compression function in each iteration.
  - Mixing of message blocks into the state takes several iterations.
  - Security of compression function should be considered in the context of the iteration mode.
- Narrow-pipe design
  - Chaining value has the same size as the digest length.

# Design Choices (1/3)

- Inspired by stream based hash algorithms
  - Short message blocks are processed with a light compression function in each iteration.
  - Mixing of message blocks into the state takes several iterations.
  - Security of compression function should be considered in the context of the iteration mode.
- Narrow-pipe design
  - Chaining value has the same size as the digest length.
  - Hamsi-256/512 is mainly intended for users who want 128/256-bit security

# Design Choices (2/3)

# Design Choices (2/3)

- Strong linear message expansion

# Design Choices (2/3)

- Strong linear message expansion
  - Best Known Linear Codes (high minimum distance).
    - $[128, 16, 70] \longrightarrow$ Hamsi-256
    - $[256, 32, 131] \longrightarrow$ Hamsi-512

# Design Choices (2/3)

- Strong linear message expansion
  - Best Known Linear Codes (high minimum distance).
    - $[128, 16, 70] \rightarrow$ Hamsi-256
    - $[256, 32, 131] \rightarrow$ Hamsi-512
  - Flexible

# Design Choices (2/3)

- Strong linear message expansion
  - Best Known Linear Codes (high minimum distance).
    - $[128, 16, 70] \rightarrow$ Hamsi-256
    - $[256, 32, 131] \rightarrow$ Hamsi-512
  - Flexible
    - Can be implemented with a table of 1Kb
    - Or with a table of 32Kb (fast software)
    - Or by exploiting the structure of the code (compact hardware)

# Design Choices (2/3)

- Strong linear message expansion
  - Best Known Linear Codes (high minimum distance).
    - $[128, 16, 70] \longrightarrow$ Hamsi-256
    - $[256, 32, 131] \longrightarrow$ Hamsi-512
  - Flexible
    - Can be implemented with a table of 1Kb
    - Or with a table of 32Kb (fast software)
    - Or by exploiting the structure of the code (compact hardware)
  - Independent of the chaining variable

# Design Choices (3/3)

- Suitable for bitsliced implementation

# Design Choices (3/3)

- Suitable for bitsliced implementation
  - Components from Serpent:
    4-bit Sbox, Linear Transformation L

# Design Choices (3/3)

- Suitable for bitsliced implementation
  - Components from Serpent:
    4-bit Sbox, Linear Transformation L
- Concatenate-Permute-Truncate

# Design Choices (3/3)

- Suitable for bitsliced implementation
  - Components from Serpent:
    4-bit Sbox, Linear Transformation L
- Concatenate-Permute-Truncate
  - Expanded message overwrites part of the state $\rightarrow$ Narrow-pipe

# Design Choices (3/3)

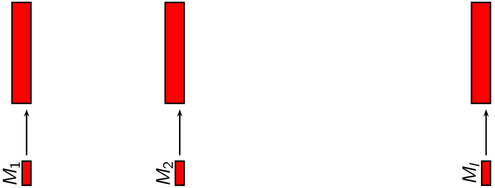
- Suitable for bitsliced implementation
  - Components from Serpent:
    4-bit Sbox, Linear Transformation L
- Concatenate-Permute-Truncate
  - Expanded message overwrites part of the state → Narrow-pipe
- Alternative option: Concatenate-Permute-XOR

# Design Choices (3/3)

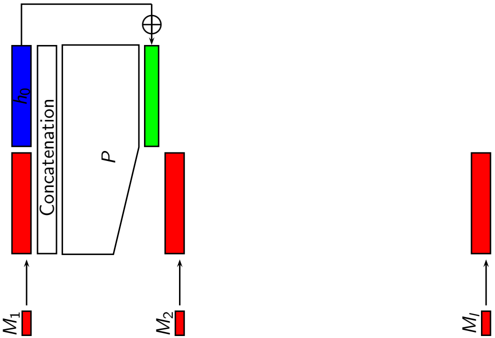
- Suitable for bitsliced implementation
  - Components from Serpent:
    4-bit Sbox, Linear Transformation L
- Concatenate-Permute-Truncate
  - Expanded message overwrites part of the state → Narrow-pipe
- Alternative option: Concatenate-Permute-XOR
  - Expanded message is XORed into the state → Wide-pipe

# General Design

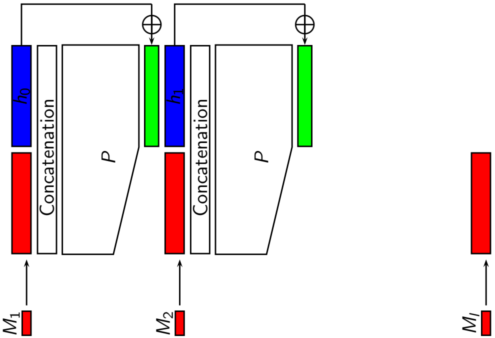
# General Design



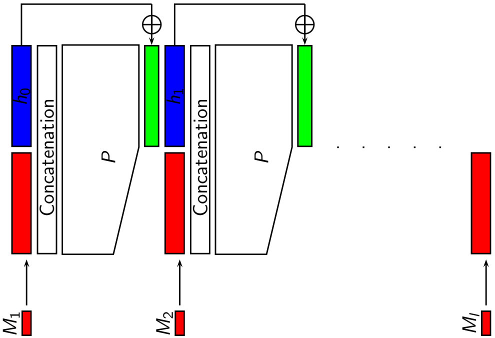
# General Design



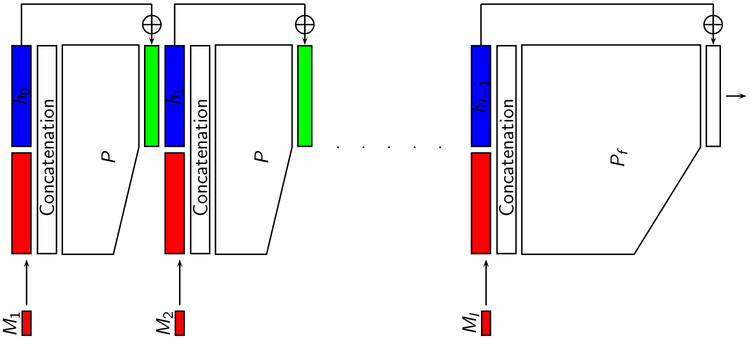
# General Design



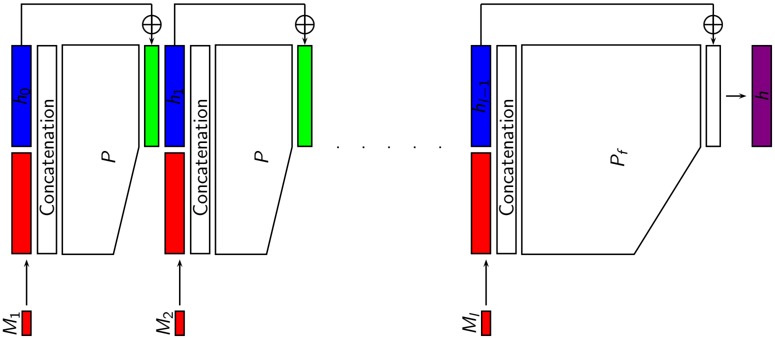
# General Design



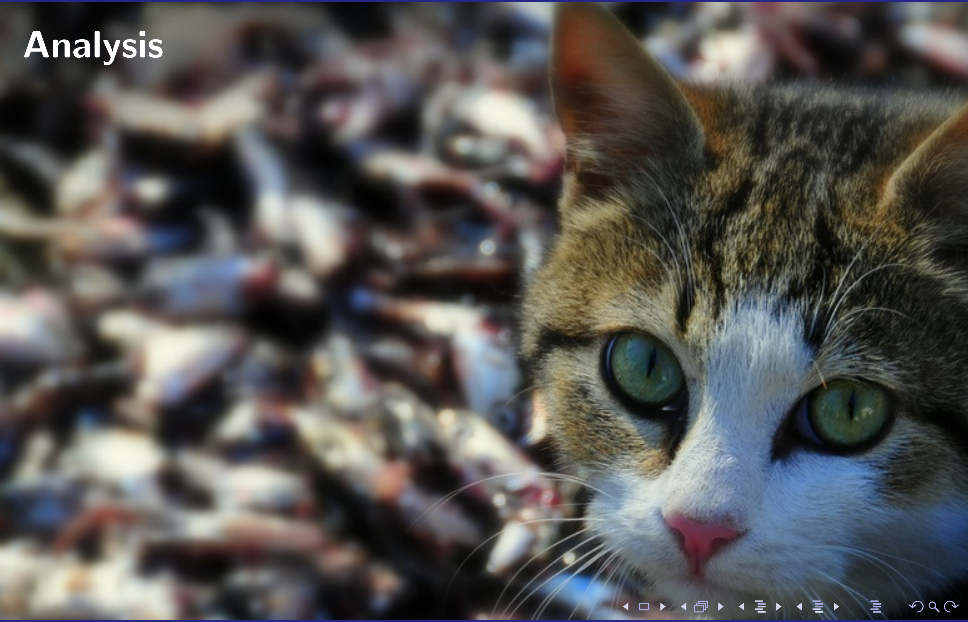
# General Design



# General Design



# Analysis



# Analysis of the Compression Function

- "On the pseudorandomness of Hamsi," J.P. Aumasson
- "Near Collisions for the Compression Function of Hamsi-256," I. Nikolic
- "Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi-256," J.P. Aumasson, W. Meier
- "New Pseudo-Near-Collision Attack on reduced round of Hamsi-256," M. Wang et al.
- "Message Recovery and Pseudo-Preimage Attacks on the Compression Function of Hamsi-256," Ç. Çalik, M.S. Turan
- "Differential Distinguishers for the Compression Function and Output Transformation of Hamsi-256," J.P. Aumasson et al.

# About Pseudo Near-Collisions

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct
  - Not surprising
    Hamsi has a light compression function by design.

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct
  - Not surprising
    Hamsi has a light compression function by design.
- Of limited use for collision paths through hash function
  - Assumes that attacker has already obtained low weight $\Delta h_{i-1}$.

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct
  - Not surprising
    Hamsi has a light compression function by design.
- Of limited use for collision paths through hash function
  - Assumes that attacker has already obtained low weight $\Delta h_{i-1}$.
  - In all attacks, $\mathrm{hw}(\Delta h_i)$ is greater than $\mathrm{hw}(\Delta h_{i-1})$.

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct
  - Not surprising
    Hamsi has a light compression function by design.
- Of limited use for collision paths through hash function
  - Assumes that attacker has already obtained low weight $\Delta h_{i-1}$.
  - In all attacks, $\mathrm{hw}(\Delta h_i)$ is greater than $\mathrm{hw}(\Delta h_{i-1})$.
  - Message expansion is bypassed by avoiding differences in the message.

# About Pseudo Near-Collisions

- Pseudo near-collisions are easy to construct
  - Not surprising
    Hamsi has a light compression function by design.
- Of limited use for collision paths through hash function
  - Assumes that attacker has already obtained low weight $\Delta h_{i-1}$.
  - In all attacks, $\text{hw}(\Delta h_i)$ is greater than $\text{hw}(\Delta h_{i-1})$.
  - Message expansion is bypassed by avoiding differences in the message.
- Pseudo-collisions are much harder to construct.

# Attack on the Hash Function

# Attack on the Hash Function

- “An Algebraic Attack on Hamsi-256” by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.
  - Interesting and valid result, details are not published yet.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.
  - Interesting and valid result, details are not published yet.
- NIST: "Second-preimage resistance of approximately $n - k$ bits for any message shorter than $2^k$ bits."

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.
  - Interesting and valid result, details are not published yet.
- NIST: "Second-preimage resistance of approximately $n - k$ bits for any message shorter than $2^k$ bits."
  - For 8-block messages (256 bits) NIST requires 248-bit security.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.
  - Interesting and valid result, details are not published yet.
- NIST: "Second-preimage resistance of approximately $n - k$ bits for any message shorter than $2^k$ bits."
  - For 8-block messages (256 bits) NIST requires 248-bit security.
- Hamsi is a narrow-pipe design.

# Attack on the Hash Function

- "An Algebraic Attack on Hamsi-256" by Itai Dinur and Adi Shamir, presented at rump session of Crypto 2010.
  - 2nd preimage attack on the hash function, $2^8$ times faster than generic attack, for messages of at least 8 blocks.
  - Finding a 2nd preimage takes about $2^{248}$.
  - Interesting and valid result, details are not published yet.
- NIST: "Second-preimage resistance of approximately $n - k$ bits for any message shorter than $2^k$ bits."
  - For 8-block messages (256 bits) NIST requires 248-bit security.
- Hamsi is a narrow-pipe design.
  - If first message is more than a few kilo bytes then there are faster generic attacks.

# Performance

# Software Performance

# Software Performance

- Long messages:
  - 32cpb, Intel Core 2 Duo [eBASH].
  - 26cpb, Intel Core i7 [eBASH].

# Software Performance

- Long messages:
  - 32cpb, Intel Core 2 Duo [eBASH].
  - 26cpb, Intel Core i7 [eBASH].
- Short messages:
  - 116cpb, Intel Core 2 Duo [eBASH].
  - 129cpb, Intel Core i7 [eBASH].

# Software Performance

- Long messages:
  - 32cpb, Intel Core 2 Duo [eBASH].
  - 26cpb, Intel Core i7 [eBASH].
- Short messages:
  - 116cpb, Intel Core 2 Duo [eBASH].
  - 129cpb, Intel Core i7 [eBASH].

- Moderate speed for long messages.
- Among the best performers for short messages.

# Hardware Performance

# Hardware Performance

- Hamsi has a small state size.
  - 768-bit (including the feedforward).

# Hardware Performance

- Hamsi has a small state size.
  - 768-bit (including the feedforward).
- As reported in many papers Hamsi has a good performance in FPGA and ASIC implementations.

# Hardware Performance

- "Developing a Hardware Evaluation Method for SHA-3 Candidates," Integrated Systems Laboratory of the ETH Zurich.
- "Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates using FPGAs," Kris Gaj et al.
- "Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations," Xu Guo et al.
- "Evaluation of Hardware Performance for the SHA-3 Candidates Using SASEBO-GII," K. Kobayashi et al.
- "Uniform Evaluation of Hardware Implementations of the Round-two SHA-3 Candidates," S. Tillich et al.

# Conclusion

- Hamsi has some unique design features.
- Received a fair amount of attention from cryptanalysts.
- It has attractive software/hardware performance.

# More information:

[http://homes.esat.kuleuven.be/ okucuk/hamsi/]