New Preimage Attacks Against Reduced SHA-1

Simon Knellwolf

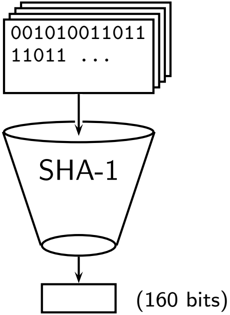
ETH Zurich and FHNW, Switzerland

Dmitry Khovratovich

Microsoft Research Redmond, USA

CRYPTO, Santa Barbara, August 2012

Secure Hash Algorithm SHA-1



Input: $< 2^{64}$ bits

Output: 160 bits

Basic security requirements:

- collision resistance,
- preimage resistance,
- second-preimage resistance.

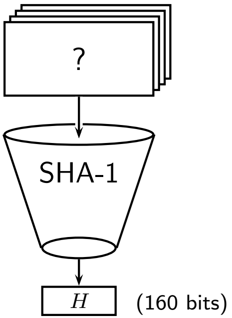
- Specified by U.S. National Security Agency in 1995.
- Collision attacks by Wang, Yin, and Yu (CRYPTO 2005).
- Still widely used and believed preimage resistant.

Preimage Resistance

Challenge: Given H, find M such that SHA-1$(M) = H$.

Brute-force: 2^{160} trials in average.

Preimage attack = a technique that is faster than brute-force.



Attacks Against Reduced SHA-1

Steps	Cost	Reference
44	$2^{157.0}$	De Cannière and Rechberger, CRYPTO 2008
48	$2^{159.3}$	Aoki and Sasaki, CRYPTO 2009
44	$2^{146.2}$	New results, CRYPTO 2012
48	$2^{150.6}$	
...	...	
57	$2^{158.7}$	

Full SHA-1 has 80 steps.

Attacks Against Reduced SHA-1

Steps	Cost	Reference
44	$2^{157.0}$	De Cannière and Rechberger, CRYPTO 2008
48	$2^{159.3}$	Aoki and Sasaki, CRYPTO 2009
44	$2^{146.2}$	New results, CRYPTO 2012
48	$2^{150.6}$	
...	...	
57	$2^{158.7}$	

Full SHA-1 has 80 steps.

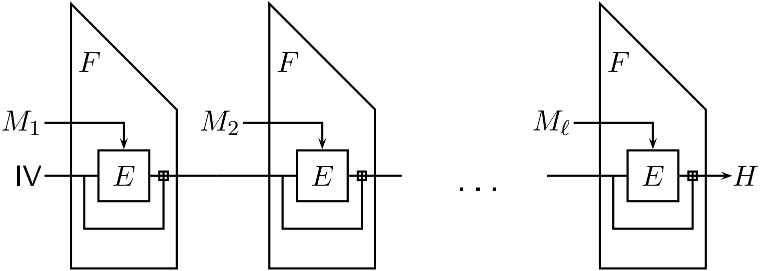
Technical contribution:

Differential perspective on meet-in-the-middle attacks.

Davies-Meyer Compression Function

SHA-1 is a Merkle-Damgård construction with a Davies-Meyer compression function.

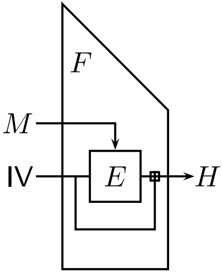
Message is padded and split into 512-bit blocks: $M_1 || \ldots || M_\ell$.



$E : \{0,1\}^{512} \times \{0,1\}^{160} \to \{0,1\}^{160}$ is a block cipher.

Davies-Meyer Compression Function

For one-block messages:



M is a preimage of H

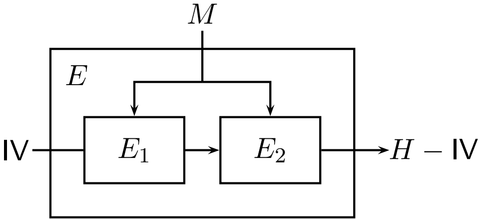
$$\Leftrightarrow$$

$$E(M, \mathsf{IV}) = H - \mathsf{IV}$$

$E : \{0,1\}^{512} \times \{0,1\}^{160} \to \{0,1\}^{160}$ is a block cipher.

Differential Meet-in-the-Middle: Requirements

Separate E into two parts:

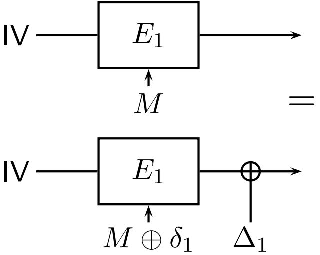


Plan: M is a preimage $\Leftrightarrow E_1(M, \mathsf{IV}) = E_2^{-1}(M, H - \mathsf{IV})$.

Difficulty: M cannot be split into separate inputs to E_1 and E_2.

Differential Meet-in-the-Middle: Requirements

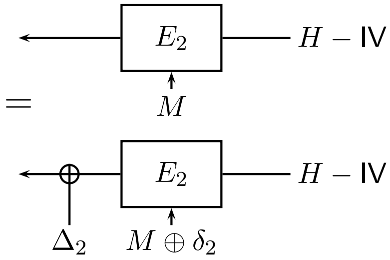
Find differential (δ_1, Δ_1) such that for all M:



Interpretation: Δ_1 "corrects" the effects of δ_1 in E_1.

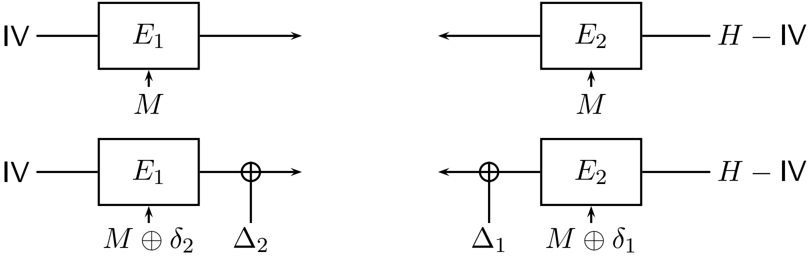
Differential Meet-in-the-Middle: Requirements

Analogously, find differential (δ_2, Δ_2) such that for all M:

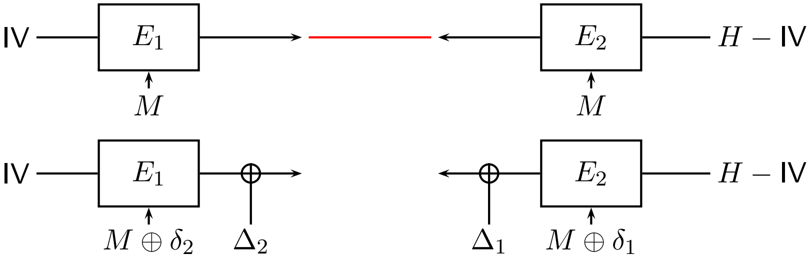


Interpretation: Δ_2 "corrects" the effects of δ_2 in E_2^{-1}.

Differential Meet-in-the-Middle: Attack Principle

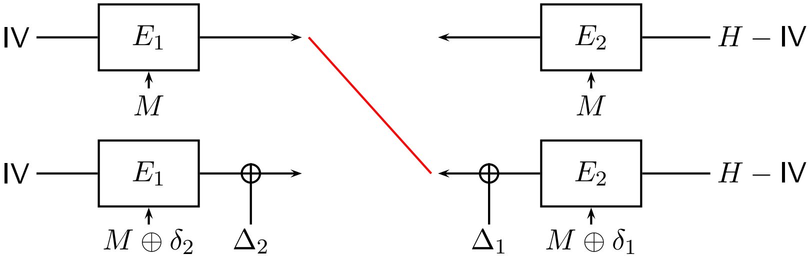


Differential Meet-in-the-Middle: Attack Principle

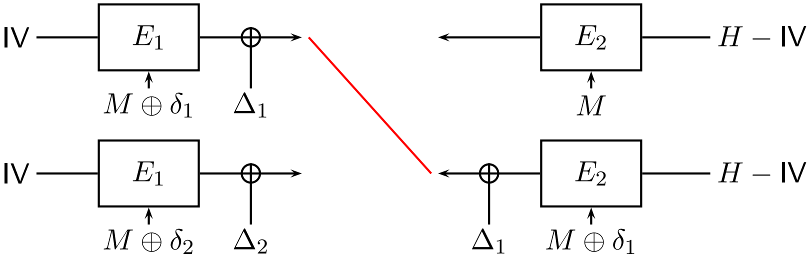


$\Leftrightarrow$ M is a preimage.

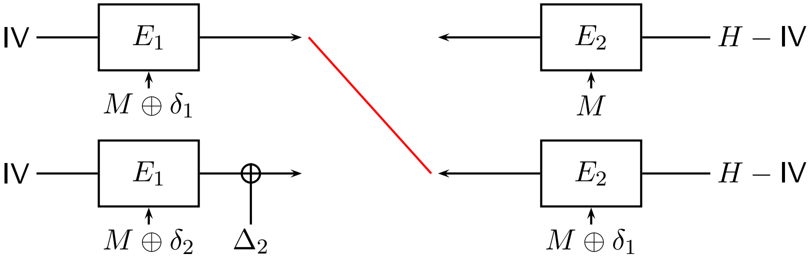
Differential Meet-in-the-Middle: Attack Principle



Differential Meet-in-the-Middle: Attack Principle

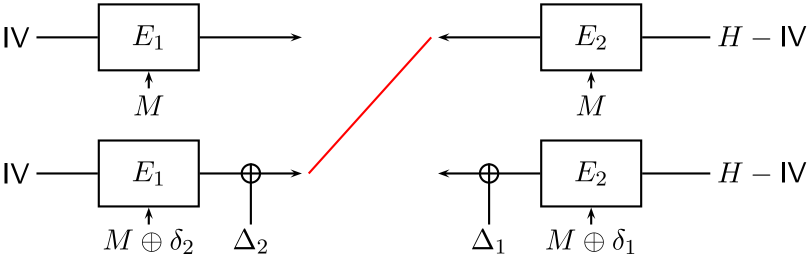


Differential Meet-in-the-Middle: Attack Principle



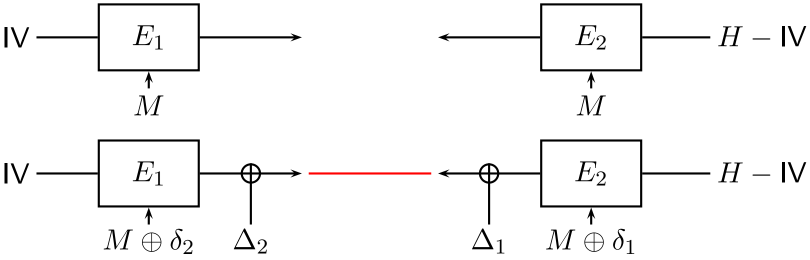
$\Leftrightarrow$ $M \oplus \delta_1$ is a preimage.

Differential Meet-in-the-Middle: Attack Principle



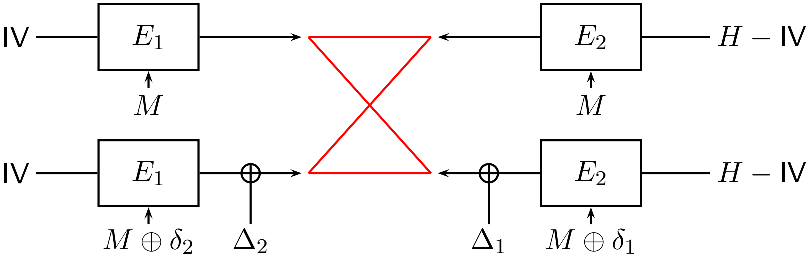
$\Leftrightarrow$ $M \oplus \delta_2$ is a preimage.

Differential Meet-in-the-Middle: Attack Principle



$\Leftrightarrow$ $M \oplus \delta_1 \oplus \delta_2$ is a preimage.

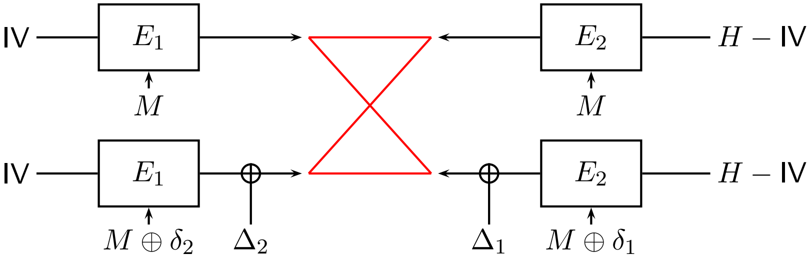
Differential Meet-in-the-Middle: Attack Principle



Four messages tested at the cost of two:

M, $M \oplus \delta_1$, $M \oplus \delta_2$ and $M \oplus \delta_1 \oplus \delta_2$.

Differential Meet-in-the-Middle: Attack Principle



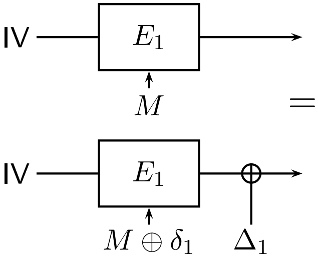
Four messages tested at the cost of two:

M, $M \oplus \delta_1$, $M \oplus \delta_2$ and $M \oplus \delta_1 \oplus \delta_2$.

In general: use 2^d differentials in both directions
$\Rightarrow 2^{2d}$ messages tested at the cost of 2^d.

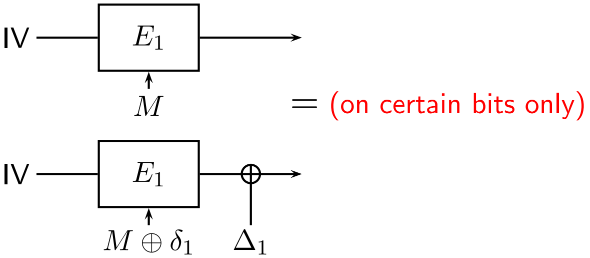
Using Truncated and Probabilistic Differentials

Find differentials (δ_1, Δ_1) such that for all M:



Using Truncated and Probabilistic Differentials

Find differentials (δ_1, Δ_1) such that for many M:



Analogously, find differentials (δ_2, Δ_2) in the backward direction.

$\Rightarrow$ More rounds can be attacked, but errors increase the cost.

Finding Suitable Differentials for SHA-1

SHA-1 has a GF(2)-linear message expansion:

- Some "obvious" candidates for δ_1 and δ_2 can be derived by linear algebra.
- The corresponding Δ_1 and Δ_2 are obtained by linearization (cf. collision attacks).
- Among all the candidates the best configuration is chosen experimentally.

Finding Suitable Differentials for SHA-1

SHA-1 has a GF(2)-linear message expansion:

- Some "obvious" candidates for δ_1 and δ_2 can be derived by linear algebra.
- The corresponding Δ_1 and Δ_2 are obtained by linearization (cf. collision attacks).
- Among all the candidates the best configuration is chosen experimentally.

Dealing with the padding:

- Padding rule restricts the choice of δ_1 and δ_2.
- A dedicated two-block approach circumvents the restriction.

Illustration of Results for SHA-1