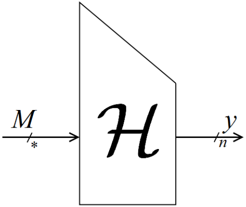
Provable Chosen-Target-Forced-Midfix Preimage Resistance

Elena Andreeva and Bart Mennink (K.U.Leuven)

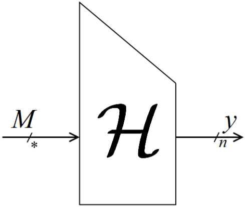
Selected Areas in Cryptography
Toronto, Canada

August 11, 2011

Hash Functions

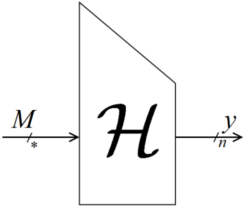


Hash Functions



Merkle-Damgård Hash Function Design (MD):

Hash Functions

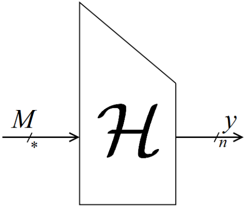


Merkle-Damgård Hash Function Design (MD):

- M injectively padded: $M \mapsto M_1 \cdots M_k = M \| 1 \| 0^{-|M|-1 \bmod m} \| \langle |M| \rangle_m$

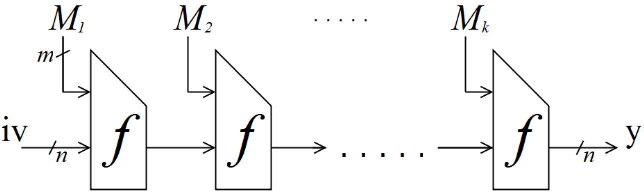
M_1 M_2 ..... M_k

Hash Functions

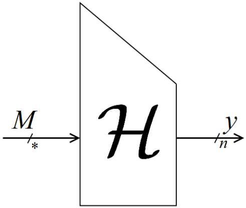


Merkle-Damgård Hash Function Design (MD):

- M injectively padded: $M \mapsto M_1 \cdots M_k = M \| 1 \| 0^{-|M|-1 \bmod m} \| \langle |M| \rangle_m$
- M_i compressed iteratively using $f : \{0,1\}^{n+m} \to \{0,1\}^n$



Hash Function Security Requirements

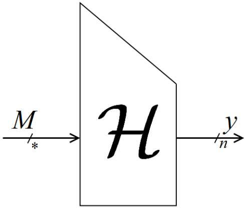


Preimage resistance

Second preimage resistance

Collision resistance

Hash Function Security Requirements



Preimage resistance

Second preimage resistance

Collision resistance

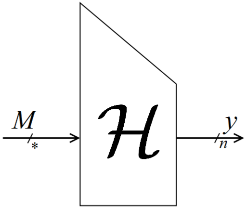
Multicollision resistance

Security against length extension attack

Chosen-target-forced-prefix preimage resistance

....

Hash Function Security Requirements

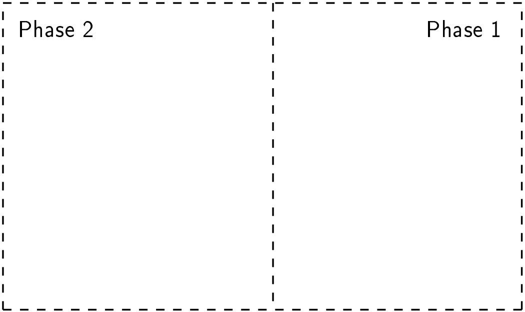


Preimage resistance
Second preimage resistance
Collision resistance
Multicollision resistance
Security against length extension attack
Chosen-target-forced-prefix preimage resistance
....

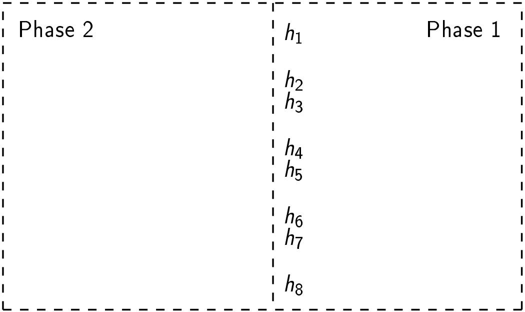
Chosen-target-forced-prefix (CTFP) preimage resistance (security against herding attack)

- Choose y, given P, find R such that $\mathcal{H}(P \| R) = y$
- Applications: predicting elections, sports games, etc.
- Ideally, CTFP attack requires 2^n work

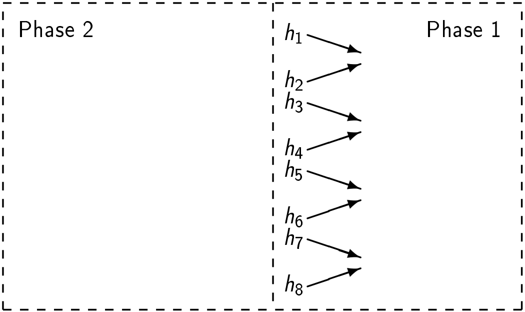
Herding Attack for MD [Kelsey & Kohno, 06]



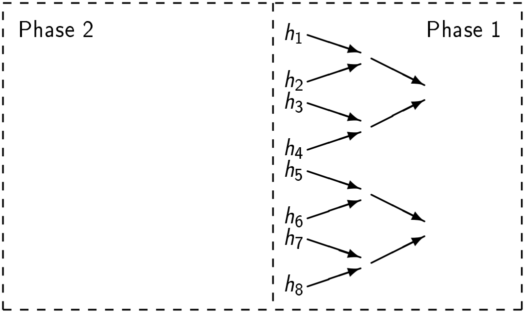
Herding Attack for MD [Kelsey & Kohno, 06]



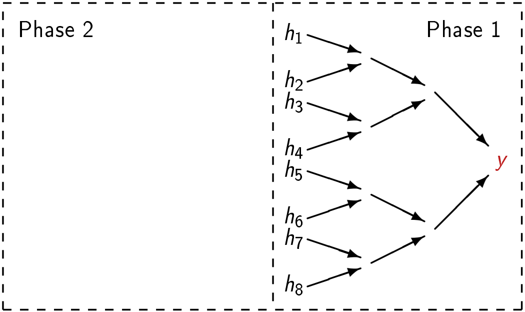
Herding Attack for MD [Kelsey & Kohno, 06]



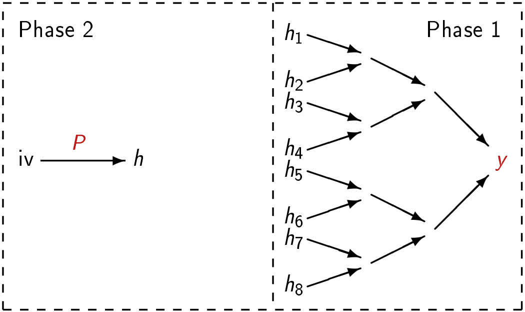
Herding Attack for MD [Kelsey & Kohno, 06]



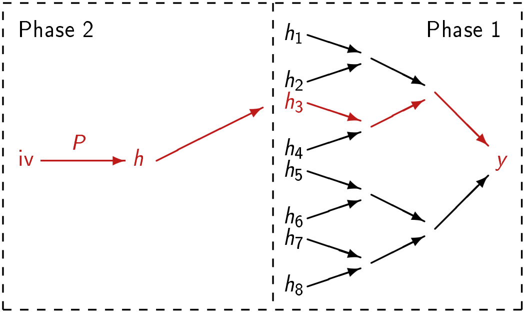
Herding Attack for MD [Kelsey & Kohno, 06]



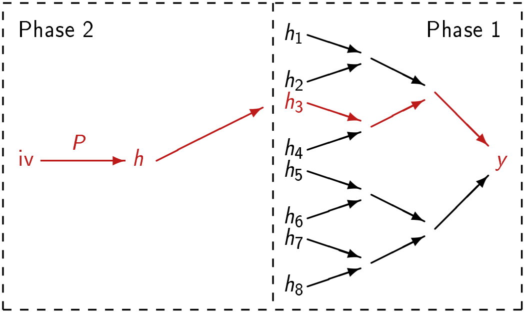
Herding Attack for MD [Kelsey & Kohno, 06]



Herding Attack for MD [Kelsey & Kohno, 06]

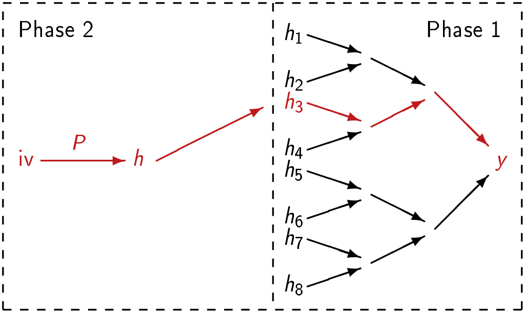


Herding Attack for MD [Kelsey & Kohno, 06]



attack	$L = \|M\|$	complexity (f-calls)
herding	$O(n)$ blocks	$\sqrt{n}2^{2n/3}$

Herding Attack for MD [Kelsey & Kohno, 06]



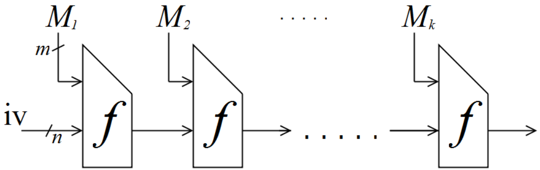
attack	$L = \|M\|$	complexity (f-calls)
herding	$O(n)$ blocks	$\sqrt{n}2^{2n/3}$
elongated herding ($0 \leq r \leq n/2$)	$O(n + 2^r)$ blocks	$\sqrt{n}2^{2n/3}/2^{r/3}$

Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]

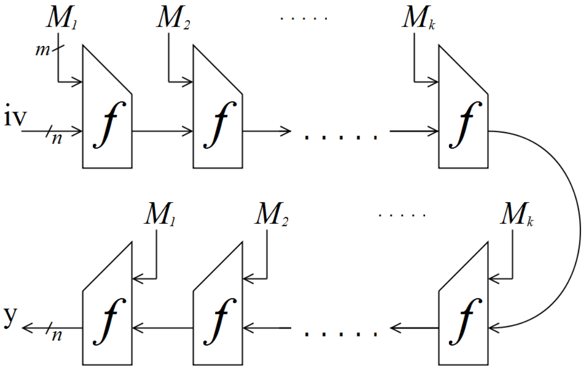
Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]



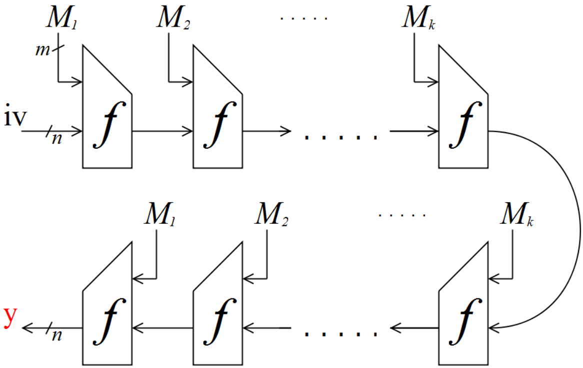
Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]



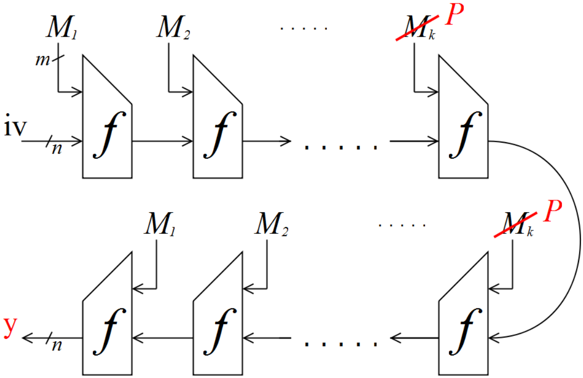
Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]



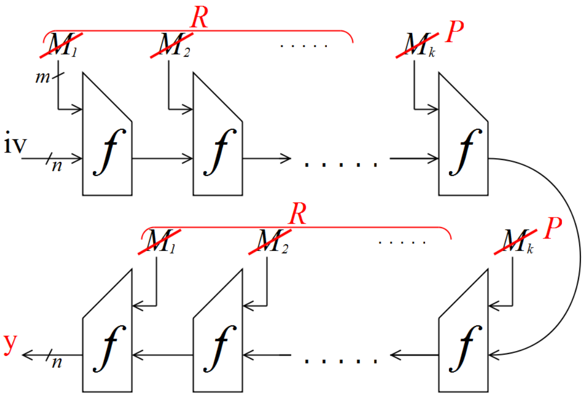
Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]



Herding Attack Beyond MD

- Herding attack generalized to MD-based hash functions
  - Merkle-Damgård with checksums [Gauravaram et al., 08, 10]
  - Hash twice, concatenated, zipper and tree hash [Andreeva et al., 09]



Our Contributions

Our Contributions

Chosen-target-forced-midfix (CTFM) preimage resistance

- Formalize and generalize security against herding
- Notion particularly covers all known attacks

Our Contributions

Chosen-target-forced-midfix (CTFM) preimage resistance

- Formalize and generalize security against herding
- Notion particularly covers all known attacks

CTFM security bound for MD

- We formally prove security of MD
- Analysis directly applies to other hash functions

Our Contributions

Chosen-target-forced-midfix (CTFM) preimage resistance

- Formalize and generalize security against herding
- Notion particularly covers all known attacks

CTFM security bound for MD

- We formally prove security of MD
- Analysis directly applies to other hash functions

Existence of optimally CTFM secure hash functions?

- No optimally secure *narrow-pipe* design known

Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \rightarrow \{0,1\}^n$

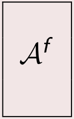
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \rightarrow \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



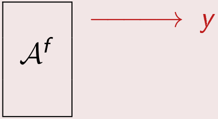
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



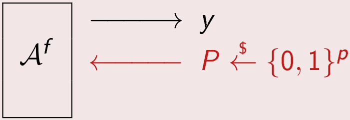
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



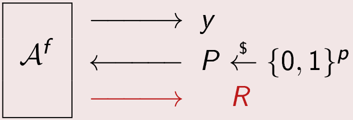
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



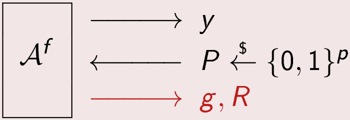
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f

$$\mathcal{A}^f \longrightarrow y$$

$$\mathcal{A}^f \longleftarrow P \xleftarrow{\$} \{0,1\}^p$$

$$\mathcal{A}^f \longrightarrow g, R$$

- $\mathcal{A}$ wins if $\mathcal{H}^f(g(P,R)) = y$ and $|\mathrm{rng}(g)| \leq 2^{Lm}$

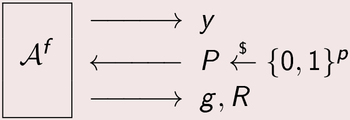
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



- $\mathcal{A}$ wins if $\mathcal{H}^f(g(P,R)) = y$ and $|\mathrm{rng}(g)| \leq 2^{Lm}$
- $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{ctfm}}(q)$: success probability of any adversary making q queries

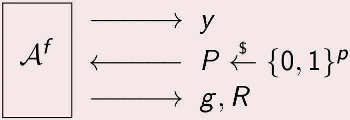
Chosen-Target-Forced-Midfix (CTFM) Security

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Definition

- $\mathcal{H}$ using ideal compression function $f : \{0,1\}^{n+m} \to \{0,1\}^n$
- Adversary $\mathcal{A}$ query access to f



- $\mathcal{A}$ wins if $\mathcal{H}^f(g(P,R)) = y$ and $|\mathrm{rng}(g)| \leq 2^{Lm}$
- $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{ctfm}}(q)$: success probability of any adversary making q queries

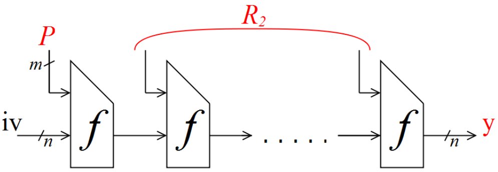
In remainder, $g(P, R_1 \| R_2) = R_1 \| P \| R_2$, where R_1, R_2 of arbitrary length

Chosen-Target-Forced-Midfix (CTFM) Security

Herding attack for MD

$g(P, R_2) = P \| R_2$

- R_1 is empty string
- P is prefix

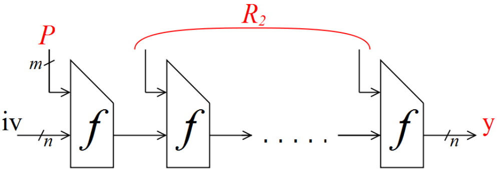


Chosen-Target-Forced-Midfix (CTFM) Security

Herding attack for MD

$g(P, R_2) = P \| R_2$

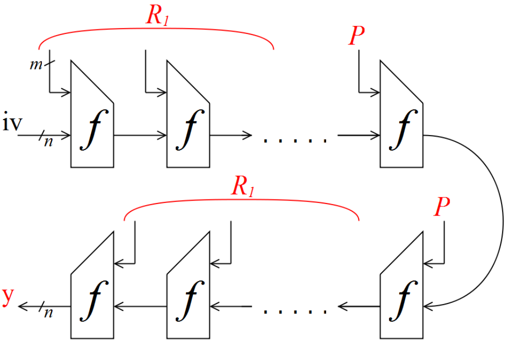
- R_1 is empty string
- P is prefix



Herding attack for zipper

$g(P, R_1) = R_1 \| P$

- R_2 is empty string
- P is suffix



CTFM Security of MD

p :	length of forced midfix (bits)
L :	max. length of forged preimage (blocks)

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\mathrm{ctfm}}(q) \leq \frac{(L-1)tq}{2^n} + \frac{m2^{\lceil p/m \rceil}q}{2^p} + \left(\frac{q^2 e}{t2^n}\right)^t + \frac{q^3}{2^{2n}}$$

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\mathrm{ctfm}}(q) \leq \frac{(L-1)tq}{2^n} + \underbrace{\frac{m2^{\lceil p/m \rceil}q}{2^p}}_{\mathrm{E}_0} + \underbrace{\left(\frac{q^2 e}{t2^n}\right)^t}_{\mathrm{E}_1} + \underbrace{\frac{q^3}{2^{2n}}}_{\mathrm{E}_2}$$

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\text{ctfm}}(q) \leq \underbrace{\frac{(L-1)tq}{2^n}}_{\text{succ} \mid \neg \text{E}_i} + \underbrace{\frac{m2^{\lceil p/m \rceil}q}{2^p}}_{\text{E}_0} + \underbrace{\left(\frac{q^2 e}{t2^n}\right)^t}_{\text{E}_1} + \underbrace{\frac{q^3}{2^{2n}}}_{\text{E}_2}$$

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\mathrm{ctfm}}(q) \leq \underbrace{\frac{(L-1)tq}{2^n}}_{\text{succ} \mid \neg \mathsf{E}_i} + \underbrace{\frac{m 2^{\lceil p/m \rceil} q}{2^p}}_{\mathsf{E}_0} + \underbrace{\left(\frac{q^2 e}{t 2^n}\right)^t}_{\mathsf{E}_1} + \underbrace{\frac{q^3}{2^{2n}}}_{\mathsf{E}_2}$$

- t: tradeoff between first and third term

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\text{ctfm}}(q) \le \underbrace{\frac{(L-1)tq}{2^n}}_{\text{succ} \mid \neg E_i} + \underbrace{\frac{m2^{\lceil p/m \rceil}q}{2^p}}_{E_0} + \underbrace{\left(\frac{q^2 e}{t2^n}\right)^t}_{E_1} + \underbrace{\frac{q^3}{2^{2n}}}_{E_2}$$

- t: tradeoff between first and third term
- p dominates second term: E_0 covers event "$\mathcal{A}$ guesses P"

CTFM Security of MD

p : length of forced midfix (bits)

L : max. length of forged preimage (blocks)

Theorem

For any integral $t > 0$:

$$\mathbf{Adv}_{MD}^{\text{ctfm}}(q) \leq \underbrace{\frac{(L-1)tq}{2^n}}_{\text{succ} \mid \neg \mathsf{E}_i} + \underbrace{\frac{m2^{\lceil p/m \rceil} q}{2^p}}_{\mathsf{E}_0} + \underbrace{\left(\frac{q^2 e}{t2^n}\right)^t}_{\mathsf{E}_1} + \underbrace{\frac{q^3}{2^{2n}}}_{\mathsf{E}_2}$$

- t: tradeoff between first and third term
- p dominates second term: E_0 covers event "$\mathcal{A}$ guesses P"
- L dominates first term: larger L gives higher success probability

Implications

Corollary

Let p be "large enough" (see paper). For any $\varepsilon > 0$*:*

$$\lim_{n\to\infty} \mathbf{Adv}^{\text{ctfm}}_{MD}\left(2^{2n/3}/L^{1/3}\cdot 2^{-n\varepsilon}\right) = 0$$

Implications

Corollary

Let p be "large enough" (see paper). For any $\varepsilon > 0$:

$$\lim_{n\to\infty} \mathbf{Adv}_{MD}^{\mathrm{ctfm}}\left(2^{2n/3}/L^{1/3} \cdot 2^{-n\varepsilon}\right) = 0$$

- Implies (asymptotic) optimality of
  - Original attack of Kelsey & Kohno
  - Almost all attacks of Gauravaram et al. and Andreeva et al.
- Analysis can easily be generalized to other hash functions, such as
  - MD with prefix-free or suffix-free padding
  - Enveloped MD
  - MD with permutation
  - HAIFA

Proof Idea

- Attack consists of two phases:
  - First phase: $\mathcal{A}$ queries f and decides on y
  - $\mathcal{A}$ receives random challenge P
  - Second phase: $\mathcal{A}$ queries f and outputs g, R s.t. $\mathcal{H}^f(g(P, R)) = y$
- Graph: $f(h_{i-1}, M_i) = h_i$ corresponds to arc $h_{i-1} \xrightarrow{M_i} h_i$
- "x at distance k from y": there exists a path $x \longrightarrow y$ of length k

Proof Idea

- Attack consists of two phases:
  - First phase: $\mathcal{A}$ queries f and decides on y
  - $\mathcal{A}$ receives random challenge P
  - Second phase: $\mathcal{A}$ queries f and outputs g, R s.t. $\mathcal{H}^f(g(P,R)) = y$
- Graph: $f(h_{i-1}, M_i) = h_i$ corresponds to arc $h_{i-1} \xrightarrow{M_i} h_i$
- "x at distance k from y": there exists a path $x \longrightarrow y$ of length k

$\mathcal{A}$ wins if:

E_0	He guesses P in the first phase
E_1	For some node y and $k \in \{0, \ldots, L\}$: graph contains more than t elements at distance k from y
E_2	Graph contains 3-way collision
$\mathrm{succ} \mid \neg \mathrm{E}_i$	Adversary finds CTFM preimage given $\neg \mathrm{E}_i$

Optimally CTFM Secure Hash Functions

Optimally CTFM Secure Hash Functions

Wide-pipe

- Wide-piping renders optimal CTFM security (trivial)

Optimally CTFM Secure Hash Functions

Wide-pipe

- Wide-piping renders optimal CTFM security (trivial)

Narrow-pipe

- No optimally CTFM secure narrow-pipe hash function known
- We consider two possible directions:
  - Salting
  - Message modification: MD with more sophisticated padding

Salted-Chosen-Target-Forced-Midfix (SCTFM) Security

$$\mathcal{H} : \{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^n$$
$$\mathcal{H}(S, M) = y$$

Salted-Chosen-Target-Forced-Midfix (SCTFM) Security

$$\mathcal{H} : \{0,1\}^s \times \{0,1\}^* \to \{0,1\}^n$$
$$\mathcal{H}(S, M) = y$$

Variant 1:

$\mathcal{A}^f$ $\longrightarrow$ y, S

$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$

$\longrightarrow$ g, R

Variant 2:

$\mathcal{A}^f$ $\longrightarrow$ y

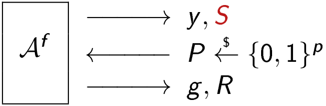
$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$

$\longrightarrow$ g, R, S

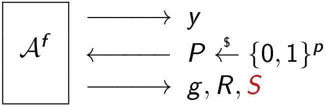
Salted-Chosen-Target-Forced-Midfix (SCTFM) Security

$$\mathcal{H} : \{0,1\}^s \times \{0,1\}^* \to \{0,1\}^n$$
$$\mathcal{H}(S, M) = y$$

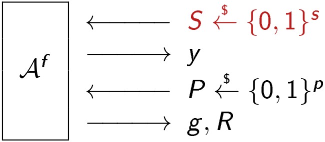
Variant 1:



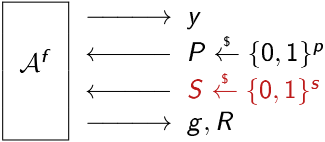
Variant 2:



Variant 3:



Variant 4:



Salted-Chosen-Target-Forced-Midfix (SCTFM) Security

$$\mathcal{H} : \{0,1\}^s \times \{0,1\}^* \to \{0,1\}^n$$
$$\mathcal{H}(S, M) = y$$

Variant 1:

$\mathcal{A}^f$
$\longrightarrow$ y, S
$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
$\longrightarrow$ g, R

Variant 2:

$\mathcal{A}^f$
$\longrightarrow$ y
$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
$\longrightarrow$ g, R, S

Variant 3:

$\mathcal{A}^f$
$\longleftarrow$ $S \xleftarrow{\$} \{0,1\}^s$
$\longrightarrow$ y
$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
$\longrightarrow$ g, R

Variant 4:

$\mathcal{A}^f$
$\longrightarrow$ y
$\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
$\longleftarrow$ $S \xleftarrow{\$} \{0,1\}^s$
$\longrightarrow$ g, R

Variant 1, 2, 3 : $\mathcal{A}$ knows salt, so $\mathbf{Adv}_{\mathcal{H}}^{\text{sctfm}}(\mathcal{A}) = \mathbf{Adv}_{\mathcal{H}}^{\text{ctfm}}(\mathcal{A})$

Salted-Chosen-Target-Forced-Midfix (SCTFM) Security

$$\mathcal{H} : \{0,1\}^s \times \{0,1\}^* \rightarrow \{0,1\}^n$$
$$\mathcal{H}(S, M) = y$$

Variant 1:

$\mathcal{A}^f$
- $\longrightarrow$ y, S
- $\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
- $\longrightarrow$ g, R

Variant 2:

$\mathcal{A}^f$
- $\longrightarrow$ y
- $\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
- $\longrightarrow$ g, R, S

Variant 3:

$\mathcal{A}^f$
- $\longleftarrow$ $S \xleftarrow{\$} \{0,1\}^s$
- $\longrightarrow$ y
- $\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
- $\longrightarrow$ g, R

Variant 4:

$\mathcal{A}^f$
- $\longrightarrow$ y
- $\longleftarrow$ $P \xleftarrow{\$} \{0,1\}^p$
- $\longleftarrow$ $S \xleftarrow{\$} \{0,1\}^s$
- $\longrightarrow$ g, R

Variant 1, 2, 3 : $\mathcal{A}$ knows salt, so $\mathbf{Adv}_{\mathcal{H}}^{\text{sctfm}}(\mathcal{A}) = \mathbf{Adv}_{\mathcal{H}}^{\text{ctfm}}(\mathcal{A})$

Variant 4 : $\mathcal{A}$ commits to y without knowing hash function instance

Message Modification

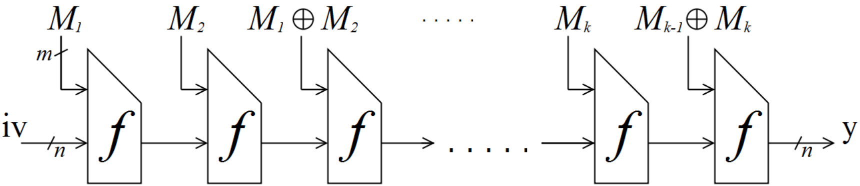
- Herding attack: edges in diamond added independently of each other

Message Modification

- Herding attack: edges in diamond added independently of each other
- Idea: create dependence among message blocks

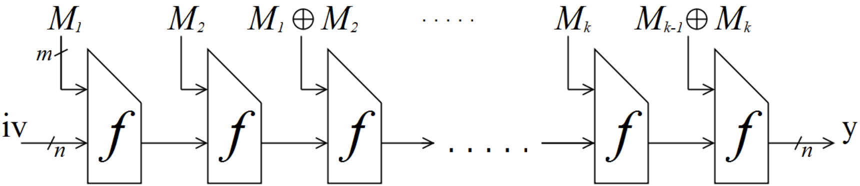
Message Modification

- Herding attack: edges in diamond added independently of each other
- Idea: create dependence among message blocks



Message Modification

- Herding attack: edges in diamond added independently of each other
- Idea: create dependence among message blocks



- We describe attack for this and similar hash functions
  - Same complexity as original herding attack (up to constant)
  - Optimal due to our security bound

Conclusions

Chosen-target-forced-midfix preimage resistance

Conclusions

Chosen-target-forced-midfix preimage resistance

- Security notion

Conclusions

Chosen-target-forced-midfix preimage resistance

- Security notion

- Introduced proof methodology
- Optimality of herding attack

Conclusions

Chosen-target-forced-midfix preimage resistance

- Security notion

- Introduced proof methodology
- Optimality of herding attack

- Optimal (2^n) security???
- Open problem

Supporting Slides

SUPPORTING SLIDES!!!

Detailed Proof Idea (1)

$E_0 \mid \neg E_2$: $\mathcal{A}$ guesses P

- By $\neg E_2$: graph contains at most $m2^{\lceil p/m \rceil} q$ strings of length p
- Any such path equals P with probability at most $1/2^p$

$$\mathbf{Pr}\left(E_0 \mid \neg E_2\right) \leq \frac{m2^{\lceil p/m \rceil} q}{2^p}$$

Detailed Proof Idea (1)

$E_0 \mid \neg E_2$: $\mathcal{A}$ guesses P

- By $\neg E_2$: graph contains at most $m2^{\lceil p/m \rceil} q$ strings of length p
- Any such path equals P with probability at most $1/2^p$

$$\mathbf{Pr}\left(E_0 \mid \neg E_2\right) \leq \frac{m2^{\lceil p/m \rceil} q}{2^p}$$

$E_1 \mid \neg E_2$: $> t$ elements at distance k from y

- By $\neg E_2$: only 2-way collisions
- One can show: graph must contain t 2-way collisions

$$\mathbf{Pr}\left(E_1 \mid \neg E_2\right) \leq \binom{q}{t} \left(\frac{q}{2^n}\right)^t \leq \left(\frac{q^2 e}{t2^n}\right)^t$$

Detailed Proof Idea (2)

E_2: 3-way collision

$$\mathbf{Pr}\left(E_2\right) \leq \frac{q^3}{2^{2n}}$$

Detailed Proof Idea (2)

E_2: 3-way collision

$$\mathbf{Pr}(E_2) \leq \frac{q^3}{2^{2n}}$$

succ | $\neg E_i$: CTFM preimage

- Forged message of length at most L blocks
- $\mathcal{A}$ needs at least one query to hit any of the $L-1$ closest layers to y
- By $\neg E_1$: at most t nodes per layer

$$\mathbf{Pr}(\mathrm{suc}_{\mathcal{A}}(q_2) \mid \neg E_0 \wedge \neg E_1) \leq \frac{(L-1)tq}{2^n}$$