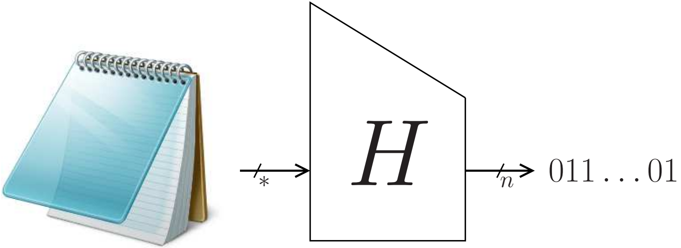
Breaking and Fixing Cryptophia's Short Combiner

Bart Mennink and Bart Preneel

KU Leuven

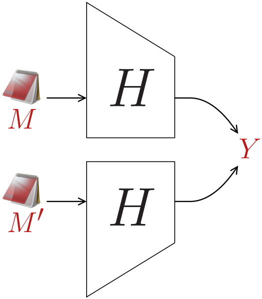
CANS 2014 — October 22, 2014

Cryptographic Hash Functions



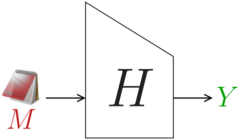
Classical Security Requirements

Collision



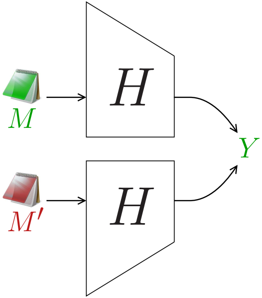
Find $M \neq M'$

Preimage



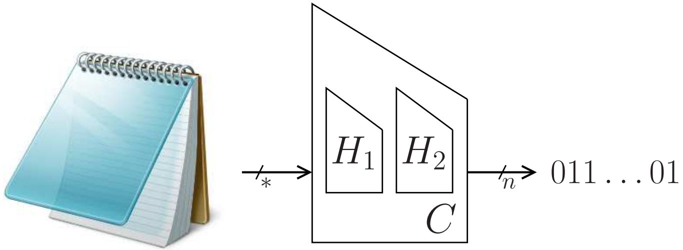
Given Y, find M

Second Preimage

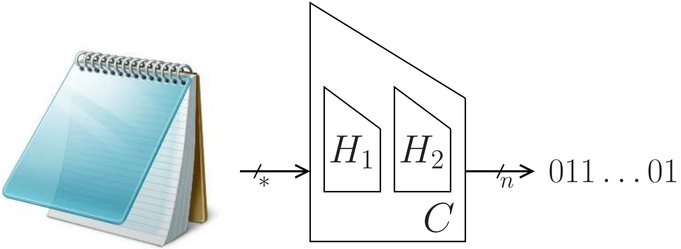


Given M, find $M' \neq M$

Hash Function Combiners

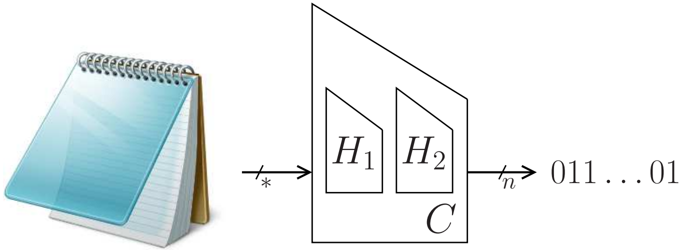


Hash Function Combiners



- Extra security barrier: secure even if one hash function is broken
- Applications in TLS and SSL

Hash Function Combiners



- Extra security barrier: secure even if one hash function is broken
- Applications in TLS and SSL

$$C_{\text{concat}}^{H_1,H_2}(M) = H_1(M) \parallel H_2(M)$$
$$C_{\text{xor}}^{H_1,H_2}(M) = H_1(M) \oplus H_2(M)$$

Robust Combiners

Robustness

- Attack on C^{H_1,H_2} can be reduced to H_1 and H_2

Robust Combiners

Robustness

- Attack on C^{H_1,H_2} can be reduced to H_1 and H_2

	coll	sec	pre	prf
$C^{H_1,H_2}_{\text{concat}} = H_1 \parallel H_2$	yes	yes	yes	no

Robust Combiners

Robustness

- Attack on C^{H_1,H_2} can be reduced to H_1 and H_2

	coll	sec	pre	prf
$C^{H_1,H_2}_{\text{concat}} = H_1 \parallel H_2$	yes	yes	yes	no
$C^{H_1,H_2}_{\text{xor}} = H_1 \oplus H_2$	no	no	no	yes

Robust Combiners

Robustness

- Attack on C^{H_1,H_2} can be reduced to H_1 and H_2

	coll	sec	pre	prf
$C^{H_1,H_2}_{\text{concat}} = H_1 \parallel H_2$	yes	yes	yes	no
$C^{H_1,H_2}_{\text{xor}} = H_1 \oplus H_2$	no	no	no	yes

Long Output

- Collision robustness: $\approx 2n$-bit output [Pietrzak-C08]
- "Robustness" requires explicit reduction

Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$

Ideal Combiner Model [Mittelbach-ACNS13]

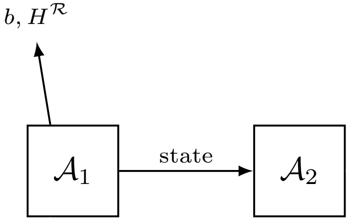
- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

$$C^{H_1,H_2} : \{0,1\}^{\kappa} \times \{0,1\}^{*} \to \{0,1\}^{n}$$

Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

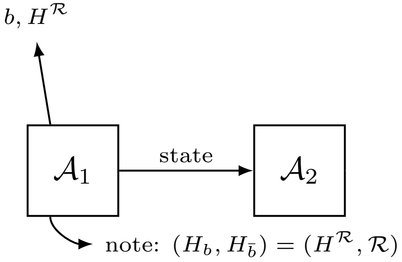
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

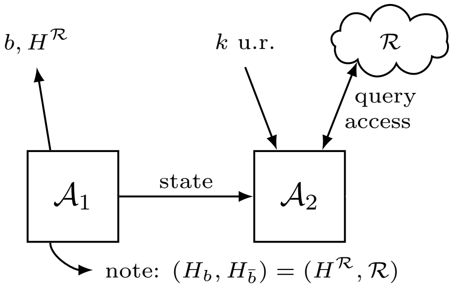
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

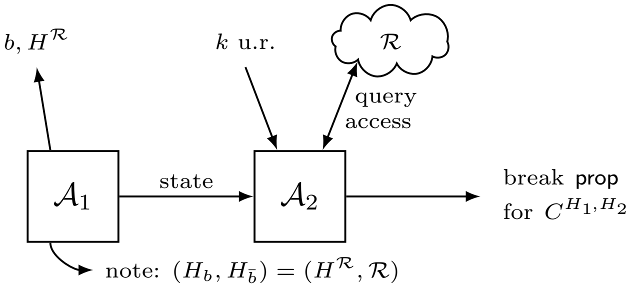
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

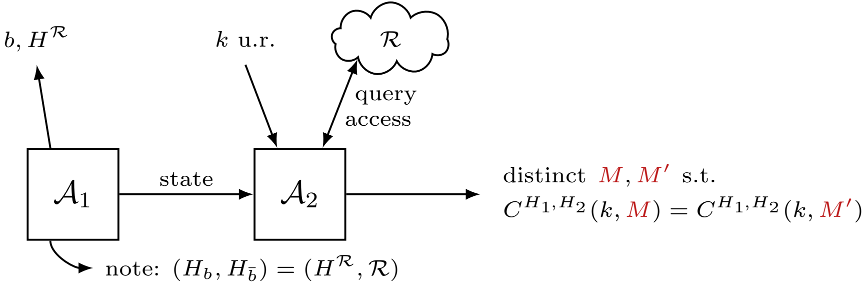
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

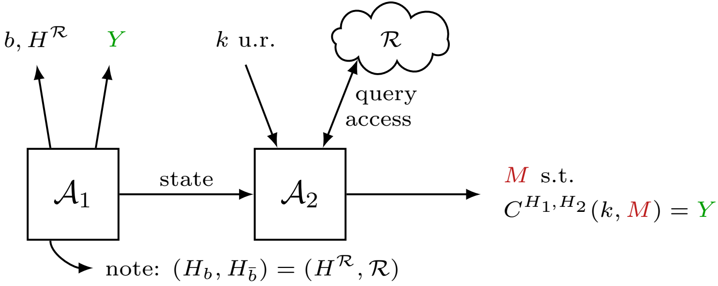
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \rightarrow \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

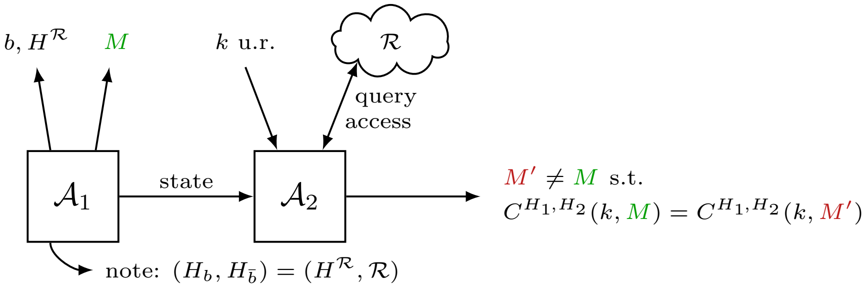
$$C^{H_1,H_2} : \{0,1\}^\kappa \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model [Mittelbach-ACNS13]

- H_1, H_2 based on random oracle
- Discards need of explicit reduction
- Combines well with indifferentiability framework

$$C^{H_1,H_2} : \{0,1\}^{\kappa} \times \{0,1\}^* \to \{0,1\}^n$$



Ideal Combiner Model

C_{concat} is secure

- $H_1 = \mathcal{R}$ or $H_2 = \mathcal{R}$

C_{xor} is insecure

- If $\mathcal{A}_1$ chooses $H^{\mathcal{R}} = \mathcal{R}$, we have $C_{\text{xor}}^{H_1,H_2}(M) = 0$

	coll	sec	pre
$C_{\text{concat}}^{H_1,H_2} = H_1 \parallel H_2$	yes	yes	yes
$C_{\text{xor}}^{H_1,H_2} = H_1 \oplus H_2$	no	no	no

Ideal Combiner Model

C_{concat} is secure

- $H_1 = \mathcal{R}$ or $H_2 = \mathcal{R}$

C_{xor} is insecure

- If $\mathcal{A}_1$ chooses $H^{\mathcal{R}} = \mathcal{R}$, we have $C_{\text{xor}}^{H_1,H_2}(M) = 0$

	coll	sec	pre
$C_{\text{concat}}^{H_1,H_2} = H_1 \parallel H_2$	yes	yes	yes
$C_{\text{xor}}^{H_1,H_2} = H_1 \oplus H_2$	no	no	no

Can we build secure “short combiner”?

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\text{mit}}^{H_1,H_2}(k, M) =$$

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$C_{\mathrm{mit}}^{H_1,H_2}(k, M) =$

$k = (k_1, \ldots, k_6)$ is a fixed key

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$C_{\mathrm{mit}}^{H_1,H_2}(k, M) =$

$k = (k_1, \ldots, k_6)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\mathrm{mit}}^{H_1,H_2}(k,M) = H_1\Big(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\Big) \oplus H_2\Big(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\Big)$$

$k = (k_1, \ldots, k_6)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\text{mit}}^{H_1,H_2}(k, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$k = (k_1, \ldots, k_6)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$$\tilde{m}_j^1 = H_1(1 \parallel m_j \oplus k_1) \oplus m_j \oplus k_2 \oplus H_2(1 \parallel m_j \oplus k_3) \quad (\forall j)$$

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\text{mit}}^{H_1,H_2}(k, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$k = (k_1, \ldots, k_6)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$$\tilde{m}_j^1 = H_1(1 \parallel m_j \oplus k_1) \oplus m_j \oplus k_2 \oplus H_2(1 \parallel m_j \oplus k_3) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_2(0 \parallel m_j \oplus k_4) \oplus m_j \oplus k_5 \oplus H_1(0 \parallel m_j \oplus k_6) \quad (\forall j)$$

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\text{mit}}^{H_1,H_2}(k, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$k = (k_1, \ldots, k_6)$ is a fixed key

$$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$$

$$\tilde{m}_j^1 = H_1(1 \parallel m_j \oplus k_1) \oplus m_j \oplus k_2 \oplus H_2(1 \parallel m_j \oplus k_3) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_2(0 \parallel m_j \oplus k_4) \oplus m_j \oplus k_5 \oplus H_1(0 \parallel m_j \oplus k_6) \quad (\forall j)$$

- Entanglement of hash functions!

Cryptophia's Short Combiner [Mittelbach-ACNS13]

$$C_{\text{mit}}^{H_1,H_2}(k, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$k = (k_1, \ldots, k_6)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$$\tilde{m}_j^1 = H_1(1 \| m_j \oplus k_1) \oplus m_j \oplus k_2 \oplus H_2(1 \| m_j \oplus k_3) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_2(0 \| m_j \oplus k_4) \oplus m_j \oplus k_5 \oplus H_1(0 \| m_j \oplus k_6) \quad (\forall j)$$

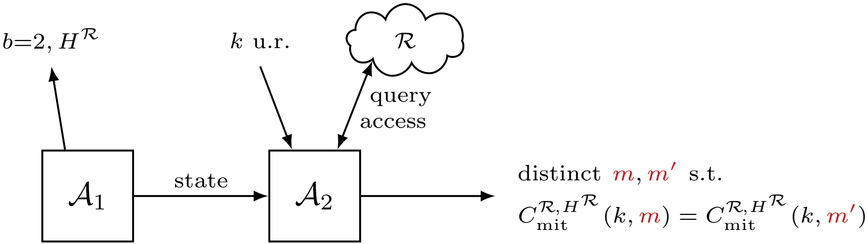
- Entanglement of hash functions!
- Proven: $2^{n/2}$ collision security
  2^n (second) preimage security

Collision Attack

- Now: no padding and $M = m$ (one block) and $b = 2$

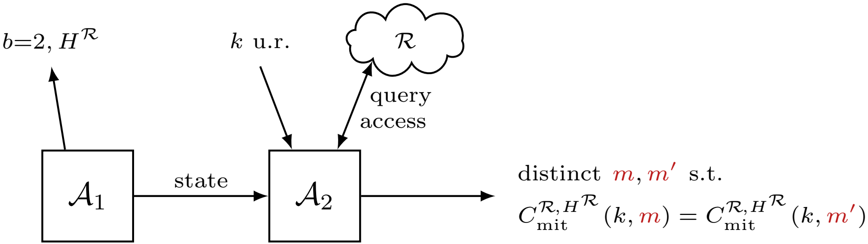
Collision Attack

- Now: no padding and $M = m$ (one block) and $b = 2$



Collision Attack

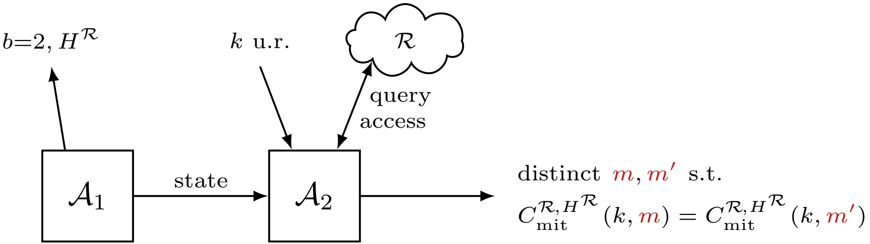
- Now: no padding and $M = m$ (one block) and $b = 2$



$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k, m) = \mathcal{R}\left(\tilde{m}^1\right) \oplus H^{\mathcal{R}}\left(\tilde{m}^2\right)$$

Collision Attack

- Now: no padding and $M = m$ (one block) and $b = 2$



$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k, m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus H^{\mathcal{R}}\big(\tilde{m}^2\big)$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus m \oplus k_2 \oplus H^{\mathcal{R}}(1 \parallel m \oplus k_3)$$

$$\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)$$

Collision Attack

$$
\begin{aligned}
C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) &= \mathcal{R}\big(\tilde{m}^1\big) \oplus H^{\mathcal{R}}\big(\tilde{m}^2\big) \\
\tilde{m}^1 &= \mathcal{R}(1 \parallel m \oplus k_1) \oplus m \oplus k_2 \oplus H^{\mathcal{R}}(1 \parallel m \oplus k_3) \\
\tilde{m}^2 &= H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)
\end{aligned}
$$

- $\mathcal{A}_1$ outputs

  $$H^{\mathcal{R}}(x)$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus H^{\mathcal{R}}\big(\tilde{m}^2\big)$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus m \oplus k_2 \oplus H^{\mathcal{R}}(1 \parallel m \oplus k_3)$$

$$\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1 \| y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus \cancel{H^{\mathcal{R}}\big(\tilde{m}^2\big)}$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus m \oplus k_2 \oplus H^{\mathcal{R}}(1 \parallel m \oplus k_3)$$

$$\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1 \| y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus \sout{H^{\mathcal{R}}(\tilde{m}^2)}$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus m \oplus k_2 \oplus H^{\mathcal{R}}(1 \parallel m \oplus k_3)$$

$$\sout{\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)}$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1\|y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus \cancel{H^{\mathcal{R}}\big(\tilde{m}^2\big)}$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus k_2 \oplus k_3 \oplus \mathcal{R}(1 \parallel m \oplus k_3)$$

$$\cancel{\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)}$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1 \| y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus \cancel{H^{\mathcal{R}}\big(\tilde{m}^2\big)}$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus k_2 \oplus k_3 \oplus \mathcal{R}(1 \parallel m \oplus k_3)$$

$$\cancel{\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)}$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1 \| y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair $m \in \{0,1\}^n$ and $m' = m \oplus k_1 \oplus k_3$

Collision Attack

$$C_{\text{mit}}^{\mathcal{R},H^{\mathcal{R}}}(k,m) = \mathcal{R}\big(\tilde{m}^1\big) \oplus \cancel{H^{\mathcal{R}}(\tilde{m}^2)}$$

$$\tilde{m}^1 = \mathcal{R}(1 \parallel m \oplus k_1) \oplus k_2 \oplus k_3 \oplus \mathcal{R}(1 \parallel m \oplus k_3)$$

$$\cancel{\tilde{m}^2 = H^{\mathcal{R}}(0 \parallel m \oplus k_4) \oplus m \oplus k_5 \oplus \mathcal{R}(0 \parallel m \oplus k_6)}$$

- $\mathcal{A}_1$ outputs

$$H^{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) \oplus y, \text{ if } x = 1\|y \text{ for some } y \in \{0,1\}^n, \\ 0, \text{ otherwise.} \end{cases}$$

- $\mathcal{A}_2^{\mathcal{R}}(k)$ outputs colliding pair $m \in \{0,1\}^n$ and $m' = m \oplus k_1 \oplus k_3$

- Generalizes to second preimage resistance (where $\mathcal{A}_1$ chooses m)

New Short Combiner

$$C^{H_1,H_2}(kl, M) = H_1\Big(\tilde{m}_1^1\|\cdots\|\tilde{m}_\ell^1\Big) \oplus H_2\Big(\tilde{m}_1^2\|\cdots\|\tilde{m}_\ell^2\Big)$$

$kl = (k_1, k_2, l_1, l_2)$ is a fixed key

$m_1\|\cdots\|m_\ell = M\|\mathsf{pad}(M)$

New Short Combiner

$$C^{H_1,H_2}(kl, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$kl = (k_1, k_2, l_1, l_2)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$\tilde{m}_j^1 = H_1(0 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$

$\tilde{m}_j^2 = H_1(1 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$

New Short Combiner

$$C^{H_1,H_2}(kl, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$kl = (k_1, k_2, l_1, l_2)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$$\tilde{m}_j^1 = H_1(0 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_1(1 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$$

Changes

1. Use extra keys l_1, l_2 to impose injectivity (w.h.p.)

New Short Combiner

$$C^{H_1,H_2}(kl, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$kl = (k_1, k_2, l_1, l_2)$ is a fixed key

$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$

$$\tilde{m}_j^1 = H_1(0 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_1(1 \parallel l_1 \parallel m_j \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m_j \oplus k_2) \quad (\forall j)$$

Changes

1. Use extra keys l_1, l_2 to impose injectivity (w.h.p.)
2. Keys k_3, k_4, k_5, k_6 have become redundant

New Short Combiner

$$C^{H_1,H_2}(kl, M) = H_1\left(\tilde{m}_1^1 \| \cdots \| \tilde{m}_\ell^1\right) \oplus H_2\left(\tilde{m}_1^2 \| \cdots \| \tilde{m}_\ell^2\right)$$

$kl = (k_1, k_2, l_1, l_2)$ is a fixed key

$$m_1 \| \cdots \| m_\ell = M \| \mathsf{pad}(M)$$

$$\tilde{m}_j^1 = H_1(0 \| l_1 \| m_j \oplus k_1) \oplus H_2(0 \| l_2 \| m_j \oplus k_2) \quad (\forall j)$$

$$\tilde{m}_j^2 = H_1(1 \| l_1 \| m_j \oplus k_1) \oplus H_2(1 \| l_2 \| m_j \oplus k_2) \quad (\forall j)$$

Changes

1. Use extra keys l_1, l_2 to impose injectivity (w.h.p.)
2. Keys k_3, k_4, k_5, k_6 have become redundant
3. Simplifications in notation

Security

Theorem

- Adversary $\mathcal{A}$ makes at most $q_{\mathcal{A}}$ queries to C^{H_1,H_2}
- $H^{\mathcal{R}}$ makes at most q_H calls to $\mathcal{R}$

$$\mathbf{Adv}^{\mathsf{coll}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}^2/2^n$$
$$\mathbf{Adv}^{\mathsf{sec}}(\mathcal{A}) \leq 4q_H^3 q_{\mathcal{A}}/2^n$$
$$\mathbf{Adv}^{\mathsf{pre}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}/2^n$$

Security

Theorem

- Adversary $\mathcal{A}$ makes at most $q_{\mathcal{A}}$ queries to C^{H_1,H_2}
- $H^{\mathcal{R}}$ makes at most q_H calls to $\mathcal{R}$

$$\mathbf{Adv}^{\mathsf{coll}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}^2/2^n$$
$$\mathbf{Adv}^{\mathsf{sec}}(\mathcal{A}) \leq 4q_H^3 q_{\mathcal{A}}/2^n$$
$$\mathbf{Adv}^{\mathsf{pre}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}/2^n$$

Remarks

- One can assume $q_H = \mathcal{O}(1)$

Security

Theorem

- Adversary $\mathcal{A}$ makes at most $q_{\mathcal{A}}$ queries to C^{H_1,H_2}
- $H^{\mathcal{R}}$ makes at most q_H calls to $\mathcal{R}$

$$\mathbf{Adv}^{\mathsf{coll}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}^2/2^n$$
$$\mathbf{Adv}^{\mathsf{sec}}(\mathcal{A}) \leq 4q_H^3 q_{\mathcal{A}}/2^n$$
$$\mathbf{Adv}^{\mathsf{pre}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}/2^n$$

Remarks

- One can assume $q_H = \mathcal{O}(1)$
- n corresponds to $|l_1| = |l_2|$, not to $|m_j|$

Security

Theorem

- Adversary $\mathcal{A}$ makes at most $q_{\mathcal{A}}$ queries to C^{H_1,H_2}
- $H^{\mathcal{R}}$ makes at most q_H calls to $\mathcal{R}$

$$\mathbf{Adv}^{\mathsf{coll}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}^2/2^n$$
$$\mathbf{Adv}^{\mathsf{sec}}(\mathcal{A}) \leq 4q_H^3 q_{\mathcal{A}}/2^n$$
$$\mathbf{Adv}^{\mathsf{pre}}(\mathcal{A}) \leq 2q_H^3 q_{\mathcal{A}}/2^n$$

Remarks

- One can assume $q_H = \mathcal{O}(1)$
- n corresponds to $|l_1| = |l_2|$, not to $|m_j|$
- Tighter bounds in paper

Proof Idea

$$\tilde{m}^1(kl, m) = H_1(0 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m \oplus k_2)$$
$$\tilde{m}^2(kl, m) = H_1(1 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m \oplus k_2)$$

Proof Idea

$$\tilde{m}^1(kl, m) = H_1(0 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m \oplus k_2)$$
$$\tilde{m}^2(kl, m) = H_1(1 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m \oplus k_2)$$

Lemma

- For any kl and any m, m':

  $$\tilde{m}^1(kl, m) \quad \tilde{m}^2(kl, m) \quad \tilde{m}^1(kl, m') \quad \tilde{m}^2(kl, m')$$

  are "more or less" mutually unrelated

Proof Idea

$$\tilde{m}^1(kl, m) = H_1(0 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m \oplus k_2)$$
$$\tilde{m}^2(kl, m) = H_1(1 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m \oplus k_2)$$

Lemma

- For any kl and any m, m':

  $$\tilde{m}^1(kl, m) \quad \tilde{m}^2(kl, m) \quad \tilde{m}^1(kl, m') \quad \tilde{m}^2(kl, m')$$

  are "more or less" mutually unrelated
- Formally, (conditional) min-entropies $\geq n - 2\log(q_H)$

Proof Idea

$$\tilde{m}^1(kl, m) = H_1(0 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(0 \parallel l_2 \parallel m \oplus k_2)$$
$$\tilde{m}^2(kl, m) = H_1(1 \parallel l_1 \parallel m \oplus k_1) \oplus H_2(1 \parallel l_2 \parallel m \oplus k_2)$$

Lemma

- For any kl and any m, m':

  $$\tilde{m}^1(kl, m) \quad \tilde{m}^2(kl, m) \quad \tilde{m}^1(kl, m') \quad \tilde{m}^2(kl, m')$$

  are "more or less" mutually unrelated
- Formally, (conditional) min-entropies $\geq n - 2\log(q_H)$

Consequences

- Preprocessing functions injective (w.h.p.)
- $H^{\mathcal{R}}$-evaluation "cancels out" an $\mathcal{R}$-call w.p. $\leq q_H^3/2^n$

Conclusions

Our Results

- Constant time attacks on Cryptophia's short combiner
- Fix to re-establish security claims

Conclusions

Our Results

- Constant time attacks on Cryptophia's short combiner
- Fix to re-establish security claims

Future Research

- Different security properties?
- Less H_1/H_2-calls?
- Beyond random oracle model?

Conclusions

Our Results

- Constant time attacks on Cryptophia's short combiner
- Fix to re-establish security claims

Future Research

- Different security properties?
- Less H_1/H_2-calls?
- Beyond random oracle model?

Thank you for your attention!