Does Secure Time-Stamping Imply Collision-Free Hash Functions?

Ahto Buldas [1,2,4] Aivo Jürgenson [2,3]

[1]Cybernetica, Tallinn, Estonia

[2]Tallinn University of Technology, Tallinn, Estonia

[3]Elion Enterprises Ltd, Tallinn, Estonia

[4]University of Tartu, Tartu, Estonia

International Conference on Provable Security 2007

Outline

1. Security of hash functions and why this is important
2. Timestamping and backdating attack
3. Blackbox reductions
4. Timestamping doesn't require CRHF

Hash functions

- $X \in \{0,1\}^*$, $x = h(X)$, $x \in \{0,1\}^m$
- $X_1 \neq X_2$, $h(X_1) = h(X_2)$

Hash functions

- $X \in \{0,1\}^*$, $x = h(X)$, $x \in \{0,1\}^m$
- $X_1 \neq X_2$, $h(X_1) = h(X_2)$
- Recent attacks against collision resistance of MD5, SHA-0, SHA-1.
- Is this *collision freedom* really required in applications?

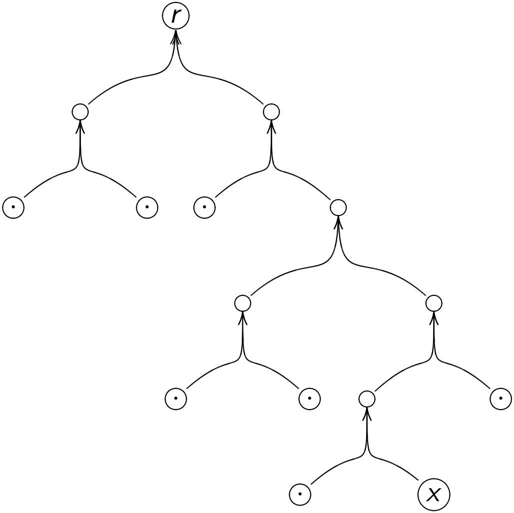
Hash functions

- $X \in \{0,1\}^*$, $x = h(X)$, $x \in \{0,1\}^m$
- $X_1 \neq X_2$, $h(X_1) = h(X_2)$
- Recent attacks against collision resistance of MD5, SHA-0, SHA-1.
- Is this *collision freedom* really required in applications?
- For example, in time-stamping:
  - Buldas and Saarepera in 2004: collision freedom is *insufficient* for security of timestamping.
  - Buldas and Laur in 2006: collision freedom is *unneccessary* for security of timestamping.
  - This paper: secure time-stamping schemes may exist without CRHF.

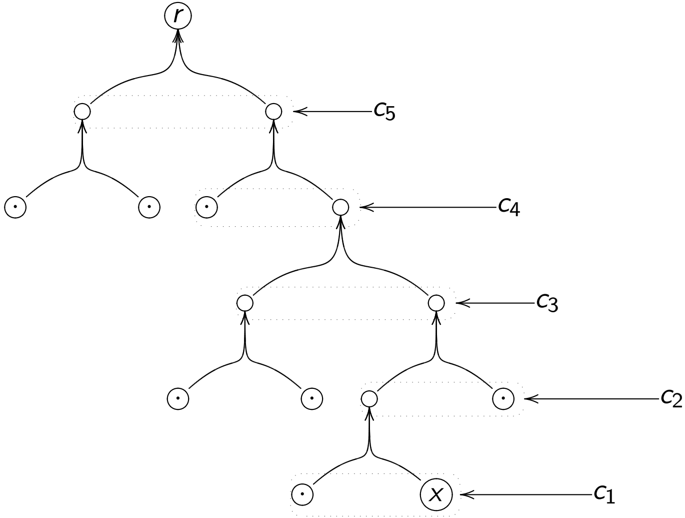
Timestamping

- ... is about vouching the existence of some value x at a certain time.
- Works in batches $\mathcal{X}_1, \mathcal{X}_2, \ldots$, where $\mathcal{X} = \{x_1, x_2, \ldots, x_m\}$.
- TS service provider publishes *commitments* $r = \mathrm{Com}(\mathcal{X})$ after each round.
- When certain value is timestamped, a *certificate* $c = \mathrm{Cert}(\mathcal{X}, x)$ is computed.
- To verify the certificate, there is a function $\mathrm{Ver}(r, x, c) = \mathrm{yes}$ in case everything is correct.

Hash-tree time-stamping certificate chain

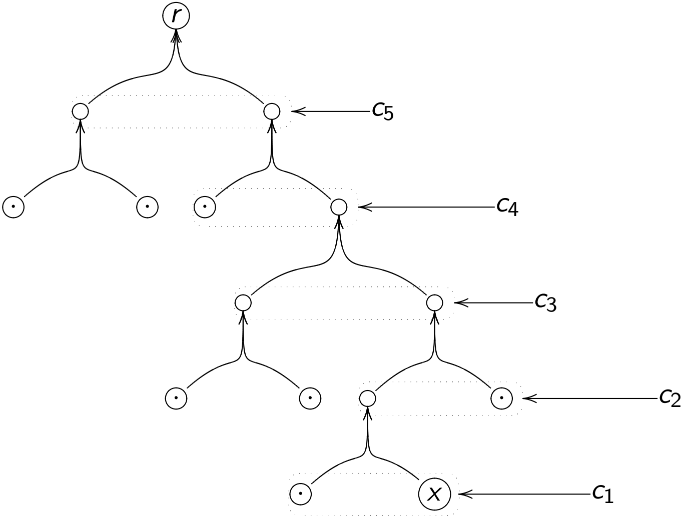


Hash-tree time-stamping certificate chain



Hash-tree time-stamping certificate chain

$c = (c_1, \ldots, c_5), r = h(c_5), c_5 = h(c_4), c_4 = h(c_3), c_3 = h(c_2), c_2 = h(c_1)$



Backdating attack

- Adversary publishes commitment r ($r = \mathsf{Com}(\mathcal{X})$).

Backdating attack

- Adversary publishes commitment r ($r = \mathsf{Com}(\mathcal{X})$).
- Alice invents something $\mathcal{D}_{\mathrm{A}} \in \{0,1\}^*$.

Backdating attack

- Adversary publishes commitment r ($r = \mathsf{Com}(\mathcal{X})$).
- Alice invents something $\mathcal{D}_{\mathrm{A}} \in \{0,1\}^*$.
- Adversary creates a modified description of the Alice's invention $\mathcal{D}'_{\mathrm{A}} \in \{0,1\}^*$ and claims that this was timestamped by himself long before Alice invented it.

Backdating attack

- Adversary publishes commitment r ($r = \mathsf{Com}(\mathcal{X})$).
- Alice invents something $\mathcal{D}_\mathrm{A} \in \{0,1\}^*$.
- Adversary creates a modified description of the Alice's invention $\mathcal{D}'_\mathrm{A} \in \{0,1\}^*$ and claims that this was timestamped by himself long before Alice invented it.
- $x = H(\mathcal{D}'_\mathrm{A})$
- $c = \mathsf{Cert}(\mathcal{X}, x)$
- $\mathsf{Ver}(r, x, c) = \mathsf{yes}$

Formalized attack

- Two-staged adversary $A = (A_1, A_2)$.

Formalized attack

- Two-staged adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$.
- Security condition:

$$\Pr\Big[(r,a) \leftarrow \mathsf{A}_1(1^k), (x,c) \leftarrow \mathsf{A}_2(r,a) : \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

Formalized attack

- Two-staged adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$.
- Security condition:

$$\Pr\Big[(r,a) \leftarrow \mathsf{A}_1(1^k), (x,c) \leftarrow \mathsf{A}_2(r,a) : \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

- $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2) \in \mathsf{FPU}$, i.e.

$$\Pr\Big[(r,a) \leftarrow \mathsf{A}_1(1^k), x' \leftarrow \Pi(r,a), (x,c) \leftarrow \mathsf{A}_2(r,a) : x' = x\Big] = k^{-\omega(1)}$$

Fully blackbox reduction

- First definition by Impagliazzio and Rudich, formally by Gertner et al.

Fully blackbox reduction

- First definition by Impagliazzio and Rudich, formally by Gertner et al.
- Graphical representation:

$$\mathcal{P} \xrightarrow{\mathsf{BB}} \mathcal{Q}$$

Fully blackbox reduction

- First definition by Impagliazzio and Rudich, formally by Gertner et al.
- Graphical representation:

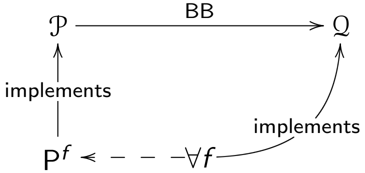
$$\mathcal{P} \xrightarrow{\mathsf{BB}} \mathcal{Q}$$

P^f

$\mathsf{S}^{A,f}$

Fully blackbox reduction

- First definition by Impagliazzio and Rudich, formally by Gertner et al.
- Graphical representation:

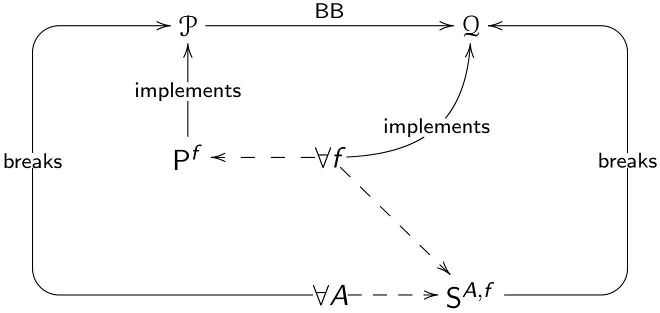


$S^{A,f}$

- Construction condition:
  $\forall f$ (any function) implementing $\mathcal{Q}$, P^f implements $\mathcal{P}$,

Fully blackbox reduction

- First definition by Impagliazzio and Rudich, formally by Gertner et al.
- Graphical representation:



- Construction condition:
  $\forall f$ (any function) implementing $\mathcal{Q}$, P^f implements $\mathcal{P}$,
- Guarantee condition:
  $\forall A \forall f$ (any function) if A breaks P^f (as $\mathcal{P}$), then $\mathsf{S}^{A,f}$ breaks f (as $\mathcal{Q}$).

Fully blackbox reduction. Examples

- PRNG blackbox reduction to one-way functions

PRNG	$\mathcal{P} \xrightarrow{\text{BB}} \mathcal{Q}$		*OWF*

- Bounded time-stamping scheme blackbox reduction to CRHF

TS	$\mathcal{P} \xrightarrow{\text{BB}} \mathcal{Q}$		*CRHF*

Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.

Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:

Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:

$$\mathcal{P} \xrightarrow{\quad\quad\quad\quad \mathsf{BB} \quad\quad\quad\quad} \mathcal{Q}$$

Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:

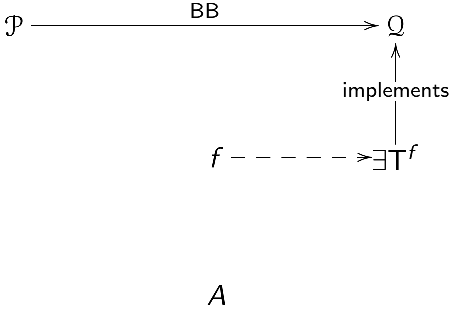
$$\mathcal{P} \xrightarrow{\text{BB}} \mathcal{Q}$$

$$f$$

$$A$$

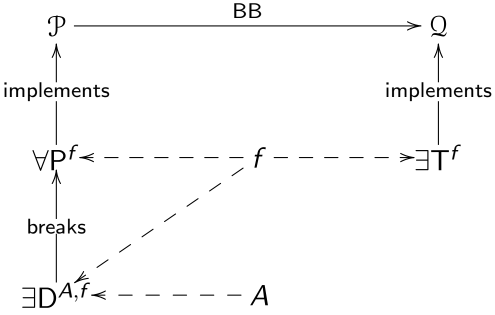
Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:



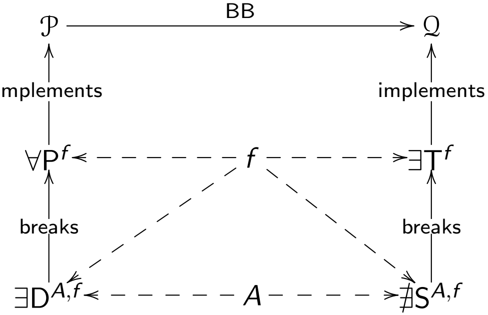
Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:



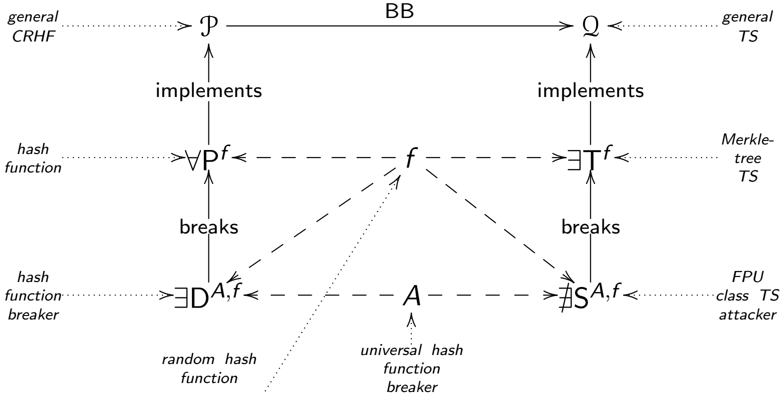
Oracle separation

- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:

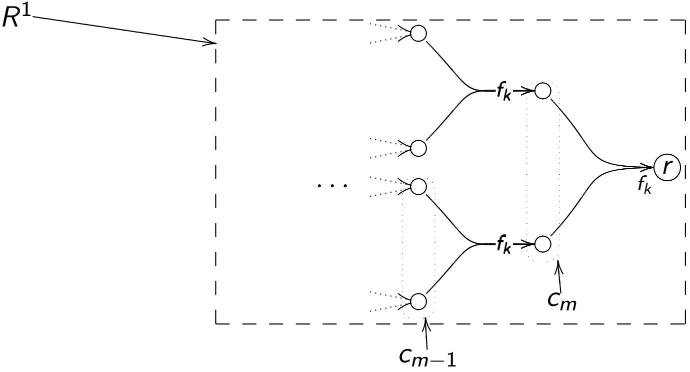


Oracle separation

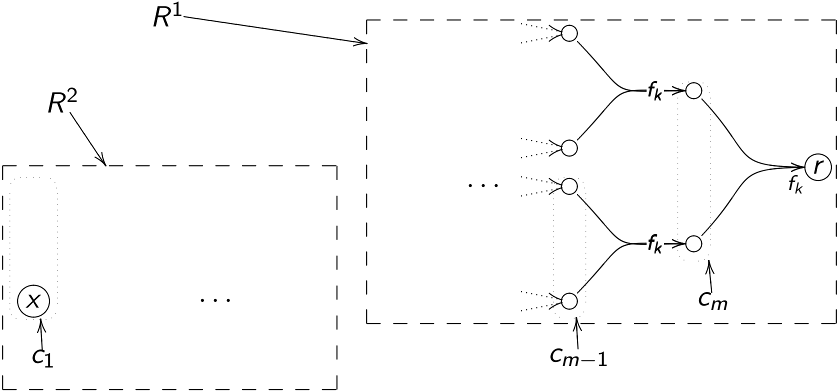
- Theorem by Hsiao and Reyzin about non-existence of blackbox reductions.
- Graphical representation:



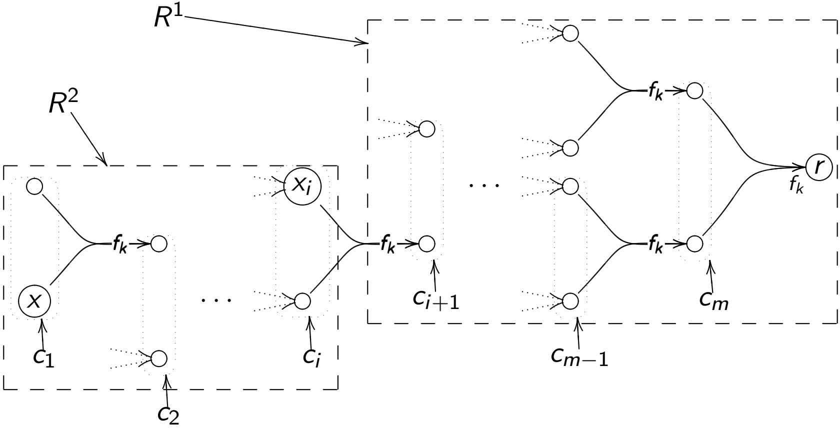
Connecting the hash chain $c = (c_1, c_2, \ldots, c_{m-1}, c_m)$



Connecting the hash chain $c = (c_1, c_2, \ldots, c_{m-1}, c_m)$



Connecting the hash chain $c = (c_1, c_2, \ldots, c_{m-1}, c_m)$



Probability of getting a hit

- A is a universal hash function collision finder: $(x, x') \leftarrow A(''F'')$ and $F(x) = F(x')$
- A works by:
  - picks random $x \leftarrow \{0,1\}^m$
  - chooses $x' \leftarrow F^{-1}(F(x))$
  - returns (x, x')

Probability of getting a hit

- A is a universal hash function collision finder: $(x, x') \leftarrow A(''F'')$ and $F(x) = F(x')$
- A works by:
  - picks random $x \leftarrow \{0, 1\}^m$
  - chooses $x' \leftarrow F^{-1}(F(x))$
  - returns (x, x')
- probability of getting a collision is high, but probability of getting a *hit* is still low
- therefore the powerful A is not particularly useful in our case.

Conclusions

$$\Pr\Big[(r,a) \leftarrow \mathsf{S}_1^{A,f}(1^k), (x,c) \leftarrow \mathsf{S}_2^{A,f}(r,a) : \\ \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

Conclusions

$$\Pr\Big[(r,a) \leftarrow \mathsf{S}_1^{A,f}(1^k), (x,c) \leftarrow \mathsf{S}_2^{A,f}(r,a) : \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

- Blackbox reduction of CRHF to TS is not possible.

Conclusions

$$\Pr\Big[(r,a) \leftarrow \mathsf{S}_1^{A,f}(1^k), (x,c) \leftarrow \mathsf{S}_2^{A,f}(r,a) : \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

- Blackbox reduction of CRHF to TS is not possible.
- In blackbox sense TS $\not\Rightarrow$ CRHF.

Conclusions

$$\Pr\Big[(r,a) \leftarrow \mathsf{S}_1^{A,f}(1^k), (x,c) \leftarrow \mathsf{S}_2^{A,f}(r,a) : \\ \mathsf{Ver}(x,c,r) = \mathsf{yes}\Big] = k^{-\omega(1)}$$

- Blackbox reduction of CRHF to TS is not possible.
- In blackbox sense TS $\not\Rightarrow$ CRHF.
- Secure timestamping may exist even if there are no collision-resistant hash functions.