Do Collisions Affect the Security of Time-Stamping?

Ahto Buldas

University of Tartu / Tallinn University of Technology / Cybernetica AS

Collisions and Collision-Resistance

$\ell(k)$ – *polynomial parameter*, i.e. polynomially bounded ($\ell(k) = k^{O(1)}$) and poly-time computable function.

Let $h = \{h_k\colon \{0,1\}^{\ell(k)} \to \{0,1\}^k\}_{k\in\mathbb{N}}$ be a poly-time computable family of functions that is chosen according to a distribution $\mathfrak{F}$.

Collision-Resistance: For every poly-time adversary A:

$$\Pr[h \leftarrow \mathfrak{F}, (x_1, x_2) \leftarrow \mathsf{A}(1^k, h)\colon\ x_1 \neq x_2,\ h(x_1) = h(x_2)] = k^{-\omega(1)}\ .$$

Second Preimage Resistance

Sec – *2nd preimage resistance*: For every poly-time A:

$$\Pr[X \underset{\mathcal{U}}{\leftarrow} \{0,1\}^{\ell(k)}, X' \leftarrow \mathsf{A}(X):\ \ X' \neq X, h(X') = h(X)] = k^{-\omega(1)}\ .$$

eSec – *everywhere 2nd preimage resistance*: For every poly-time A:

$$\max_{x \in \{0,1\}^{\ell(k)}} \Pr[X' \leftarrow \mathsf{A}(1^k):\ \ X' \neq x, h(X') = h(x)] = k^{-\omega(1)}\ .$$

Rogaway and Shrimpton (2004): almost exhaustive study about ”classical” security conditions of hash functions.

Recent Success in Finding Collisions ...

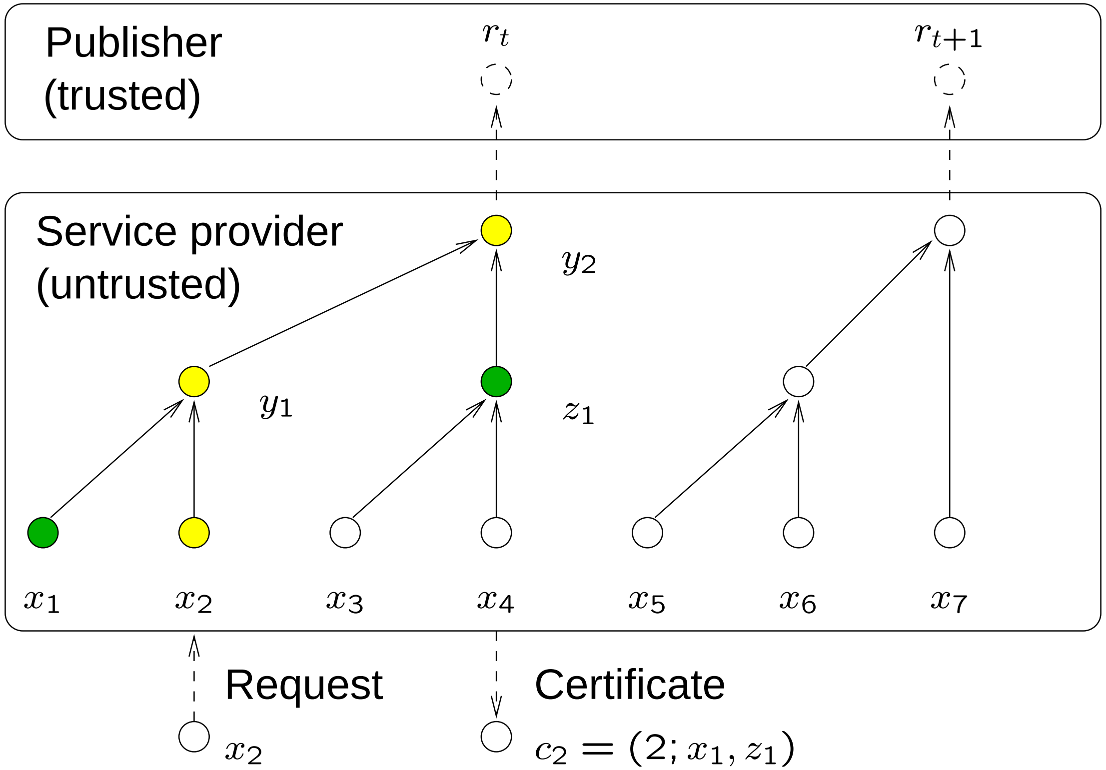
Eurocrypt 2005: Wang et al presented efficient collision-finding attacks for most of the known practical hash functions.

What does this mean for the numerous applications in which hash functions are used as a building block?

Does it mean that ”broken” hash functions cannot be used in time-stamping schemes?

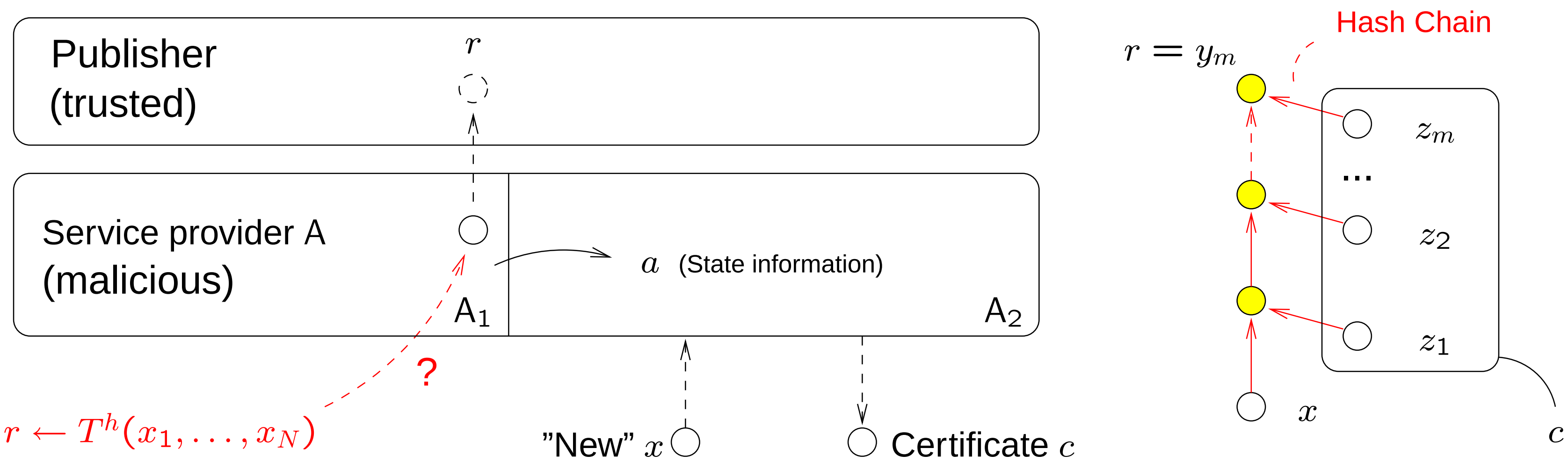
We show that *neither collision resistance nor 2nd pre-image resistance is necessary for secure time-stamping*.

Time-Stamping with Hash Functions



Verifying a certificate: Compute $y_2 = F_h(x_2; c_2) = h(h(x_1, x_2), z_1)$, obtain r_t, and check if $y_2 = r_t$.

Back-Dating Attack and Chain-Resistance



Successful forgery: $F_h(x;c) = r$

Chain – *chain-Resistance (of h)*: For every poly-time $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ and for every unpredictable (poly-sampleable) distribution family $\{\mathcal{D}_k\}_{k\in\mathbb{N}}$:

$$\Pr[(r,a) \leftarrow \mathsf{A}_1(1^k), x \leftarrow \mathcal{D}_k, c \leftarrow \mathsf{A}_2(x,a) \colon F_h(x,c) = r] = k^{-\omega(1)}.$$

Client-Side Hash Functions

$H\colon \{0,1\}^{\ell(k)} \to \{0,1\}^k$ a hash function.

Secure (H,h)-time stamping: For every poly-time $A = (A_1, A_2)$ and for every unpredictable distribution family $\mathcal{D}_k$ on $\{0,1\}^{\ell(k)}$:

$$\Pr[(r,a) \leftarrow A_1(1^k), X \leftarrow \mathcal{D}_k, c \leftarrow A_2(x,a)\colon F_h(H(x),c) = r] = k^{-\omega(1)}.$$

Chain-resistance of h is *necessary* for secure (H,h)-time-stamping, but it is not known whether it is *sufficient* (if H is collision-resistant).

Buldas, Saarepera (2004): If H and h are collision-resistant then a (H,h)-time-stamping is secure in the ”restricted chain model”.

Buldas, Laud, Saarepera, Willemson (2005): If H and h are collision-resistant then a (H,h)-time-stamping scheme with an *additional audit functionality* is secure.

Chain-Resistance vs Collision-Resistance

Buldas, Saarepera (2004): "h is collision-resistant $\Rightarrow$ h is chain-resistant" cannot be proved in a (conventional) black-box way.

It is still not known whether chain-resistant functions can be constructed from collision-resistant ones.

(Unpublished result) Collision-resistance and "shortcut-freedom" together imply chain-resistance.

Does chain-resistance imply collision-resistance, i.e. is collision-resistance of h (and of H) necessary for secure time-stamping ?

Shortcuts of the Previous Security Definitions

Chain-resistance of h and collision-resistance of H do not imply secure (H, h)-time-stamping scheme.

The back-dating component A_2 of the adversary does not ”communicate” with $\mathcal{D}$, which is not necessarily true in practice – During the choice $x \leftarrow \mathcal{D}$, the adversary may store some extra information about x, which may be useful for A_2 in back-dating x.

New Results

New security condition for (H, h)-time-stamping schemes that gives more power to the adversary.

New stronger condition eChain – *everywhere chain resistance* – (for h), which is sufficient for time-stamping.

New weaker (everywhere) 2nd pre-image resistance condition uеSec, which is necessary for both h and H, and sufficient for H (if h is eChain).

We prove that collision-resistance as well as 2nd preimage resistance are unnecessary for the security of time-stamping:

- We prove that ueSec does not imply 2nd preimage resistance
- We show that eChain probably does not imply 2nd preimage resistance

New Security Definition

$\mathsf{FPU}_{\ell(k)}$ – class of all poly-sampleable distribution families $\{\mathcal{A}_k\}_{k\in\mathbb{N}}$ on $\{0,1\}^{\ell(k)} \times \{0,1\}^*$, the first component of which is unpredictable.

Secure (H,h)-time-stamping system – $\forall \mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$:

$$\varepsilon(k) = \max_{r\in\{0,1\}^k} \Pr[(X,c) \leftarrow \mathcal{A}_k \colon F_h(H(X);c) = r] = k^{-\omega(1)} \ .$$

New condition implies the old one: Let $(\mathsf{A}_1,\mathsf{A}_2) \in \mathsf{FP}$ have success

$$\delta(k) = \Pr[(r,a)\leftarrow A_1(1^k), X\leftarrow\mathcal{D}, c\leftarrow\mathsf{A}_2(X,r,a)\colon F_h(H(X);c) = r] \ .$$

Define $\mathcal{A}_k$ so that after simulating $(\mathsf{A}_1,\mathsf{A}_2)$ it outputs (X,c). Then we have $\mathcal{A}_k$ with $\varepsilon(k) \geq \delta(k)$. $\square$

Unpredictability Preservation

$H\colon \{0,1\}^{\ell(k)} \to \{0,1\}^k$ is *unpredictability preserving*, if for every $\mathcal{D}_k \in$ FPU$_{\ell(k)}$, the distribution $H(\mathcal{D})$ is unpredictable.

Polynomial sampleability of $\mathcal{D}_k$ is crucial:

Proposition: For every hash function $H_k\colon \{0,1\}^{\ell(k)} \to \{0,1\}^k$ with $\ell(k) = k+\omega(\log k)$ there exists a distribution family $\mathcal{D}_k$ with Rényi entropy $\mathrm{H}_2[\mathcal{D}_k] = \omega(\log k)$, such that $\mathrm{H}_2[H(\mathcal{D}_k)] = 0$.

Indeed, there exists $y \in \{0,1\}^k$ for which

$$|\, H^{-1}(y)\, |= \frac{2^{k+\omega(\log k)}}{2^k} = k^{\omega(1)} \quad .$$

Define $\mathcal{D}_k$ as the uniform distribution on $H^{-1}(y)$. $\square$

Unpredictability Preservation Is Necessary for H

Theorem 1: In every secure (H, h)-time-stamping system, the client-side hash function H is unpredictability-preserving.
Proof. If Π is a predictor for $H(\mathcal{D})$ with success

$$\pi(k) = \mathsf{Pr}[X' \leftarrow \Pi(1^k), X \leftarrow \mathcal{D}\colon \ X' = H(X)] \ .$$

Define $\mathsf{A}_1(1^k) \equiv \Pi(1^k)$ and $(\mathcal{D}, \bigsqcup) \leftarrow \mathsf{A}_2(\ldots)$. The success of $(\mathsf{A}_1, \mathsf{A}_2)$ is $\pi(k)$. □

Every collision-resistant function is unpredictability-preserving.

2nd preimage resistance does not imply unpredictability-preservation.

Insufficiency of 2nd Pre-Image Resistance

Let $H\colon \{0,1\}^{\ell(k)} \rightarrow \{0,1\}^k$ be 2nd preimage resistant hash function ($\ell(k) = k + \omega(\log k)$).

We construct a function $H'\colon \{0,1\}^{\ell'(k)} \rightarrow \{0,1\}^k$ which is 2nd preimage resistant but not unpredictability- preserving.

Let $\ell'(k) = \ell(k-1)$ for all $k > 1$, and for every $X \in \{0,1\}^{\ell'(k)}$:

$$H'_k(X) = \begin{cases} 0^k & \text{if } X = 0^{k-1} \| X_1 \text{ for an } X_1 \in \{0,1\}^{\ell(k)-k} \\ 1 \| H_{k-1}(X) & \text{otherwise.} \end{cases}$$

Define $\mathcal{D}$ on $\ell'(k)$, so that $\mathcal{D}_k = 0^{k-1} \| \mathcal{U}_{\ell(k-1)-k+1}$.
$\mathcal{D}$ is unpredictable, because it has Rényi entropy $\mathrm{H}_2(\mathcal{D}_k) = \ell(k-1) - k + 1 = \omega(\log k)$.

Everywhere Chain-Resistance and Security

eChain – *everywhere chain-resistance* – $\forall \mathcal{A}_k \in \mathsf{FPU}_k$:

$$\varepsilon(k) = \max_{r\in\{0,1\}^k} \Pr[(x,c) \leftarrow \mathcal{A}_k\colon F_h(x;c) = r] = k^{-\omega(1)} \ .$$

Theorem 2: For secure (in the new sense) (H,h)-time-stamping, it is sufficient that h-is everywhere chain-resistant and H is unpredictability-preserving.

Proof. Let $\mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$, such that

$$\epsilon(k) = \max_{r\in\{0,1\}^k} \Pr[(X,c) \leftarrow \mathcal{A}_k\colon F_h(H(X);c) = r] \neq k^{-\omega(1)} \ .$$

Define $\mathcal{A}'_k$ so that $(H(x),c) \leftarrow \mathcal{A}'_k$ iff $(x,c) \leftarrow \mathcal{A}_k$. We have $\mathcal{A}'_k \in \mathsf{FPU}_k$, because H is unpredictability preserving. Obviously, $\mathcal{A}_k$ breaks h in the sense of eChain with success $\epsilon(k)$. $\square$

Weak Everywhere 2nd Preimage Resistance

ueSec – *weak everywhere 2nd preimage resistance*: For every distribution family $\mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$:

$$\max_{X \in \{0,1\}^{\ell(k)}} \Pr[X' \leftarrow \mathcal{A}_k\colon\ X' \neq X, H(X') = H(X)] = k^{-\omega(1)}\ .$$

We show that:

- uSec *is weaker than 2nd preimage resistance.*
- uSec *is equivalent to unpredictability preservation (*uPre*).*

ueSec Is Weaker Than 2nd Preimage Resistance

Theorem 3: If there are hash functions that are ueSec then there are hash functions which are ueSec but not 2nd preimage resistant.

Let $H\colon \{0,1\}^{\ell(k)} \to \{0,1\}^k$ be ueSec-secure. Define $H'(X) = H(X \text{ or } 1)$. Obviously, H' is not 2nd preimage resistant. To show that H' is ueSec, let $\mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$ and $X \in \{0,1\}^{\ell(k)}$, so that

$$\delta(k) = \Pr[X' \leftarrow \mathcal{A}_k\colon\ X' {\neq} X, H'(X'){=}H'(X)] = p_\sqcap + p_C \ ,$$

where $p_\sqcap = \Pr_{X' \leftarrow \mathcal{A}_k}[X' \text{ or } 1 = X \text{ or } 1] = k^{-\omega(1)}$ ($\mathcal{A}_k$ is uPre) and

$$p_C = \Pr_{X' \leftarrow \mathcal{A}_k}[X' \text{ or } 1 \neq X \text{ or } 1,\ H(X' \text{ or } 1) = H(X \text{ or } 1)] = k^{-\omega(1)} \ ,$$

because otherwise $\mathcal{A}'_k = (\mathcal{A}_k \text{ or } 1)$ breaks H in terms of ueSec (take X or 1 instead of X). Therefore, $\delta(k) = k^{-\omega(1)}$. $\square$

ueSec vs Unpredictability-Preservation

ueSec $\Rightarrow$ uPre: Let $\mathcal{D}_k$ be unpredictable and Π be a predictor for $H(\mathcal{D}_k)$ with success $\pi(k) = \Pr[y \leftarrow \Pi(1^k), X' \leftarrow \mathcal{D}_k \colon y = H(X')] \neq k^{-\omega(1)}$. Therefore,

$$\max_{X \in \{0,1\}^{\ell(k)}} \Pr[X' \leftarrow \mathcal{D}_k \colon H(X') = H(X)] \geq \pi(k) \neq k^{-\omega(1)} \ .$$

$$\Pr_{X' \leftarrow \mathcal{D}_k}[H(X') = H(X)] = \Pr_{X' \leftarrow \mathcal{D}_k}[X' = X] + \Pr_{X' \leftarrow \mathcal{D}_k}[X' \neq X, H(X') = H(X)] \ .$$

As the first probability is negligible ($\mathcal{D}_k$ is unpredictable), the second one is non-negligible and hence $\mathcal{D}_k$ breaks H in the sense of ueSec. $\square$

ueSec vs Unpredictability-Preservation

$\mathsf{uPre} \Rightarrow \mathsf{ueSec}$: Let $\mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$ and $X \in \{0,1\}^{\ell(k)}$ so that

$$\delta(k) = \Pr_{X' \leftarrow \mathcal{A}_k}[X' \neq X, H(X') = H(X)] \neq k^{-\omega(1)} .$$

Therefore, $\Pr_{X' \leftarrow \mathcal{A}_k}[H(X') = H(X)] \geq \delta(k) \neq k^{-\omega(1)}$ and we can define a predictor $\Pi(1^k)$ for $H(\mathcal{A}_k)$ with output distribution $H(\mathcal{A}_k)$. This predictor has success:

$$\pi(k) = \Pr[X' \leftarrow \mathcal{A}_k, X'' \leftarrow \mathcal{A}_k \colon H(X'') = H(X')] \geq \delta^2(k) \neq k^{-\omega(1)} .$$

Hence, H is not unpredictability-preserving. $\square$

h Is Not Necessarily Collision-Resistant

Theorem 4: For every secure (H, h)-time-stamping scheme, there is a secure (H, h')-time-stamping, where h' is not collision-resistant.

Define h', which behaves as h, except that $h'(0^k 1^k) = 0^k = h'(1^k 0^k)$. Let $\mathcal{A}_k \in \mathsf{FPU}_{\ell(k)}$ be an adversary with success

$$\varepsilon(k) = \max_{r \in \{0,1\}^k} \Pr[(X, c) \leftarrow \mathcal{A}_k \colon F_{h'}(H(X); c) = r] \neq k^{-\omega(1)} \ .$$

Let S be the event that $\mathcal{A}_k$ is successful and c comprises 0^k or 1^k as intermediate values. $\mathcal{A}'_k$ simulates $(X, c) \leftarrow \mathcal{A}_k$ and outputs (X, c'), where c' is the left segment of c until the first 0^k or 1^k.

If $\Pr[\mathsf{S}] \neq k^{-\omega(1)}$ then $\mathcal{A}'_k$ breaks (H, h)-time-stamping (for $r \in \{0^k, 1^k\}$). If $\Pr[\mathsf{S}] = k^{-\omega(1)}$ then $\mathcal{A}_k$ breaks (H, h)-time-stamping. A contradiction. □

h Is Not Necessarily 2nd Preimage Resistant

We are unable to show this explicitly – hard to find a specific h' (as above). We use *oracle separation*.

Define h as a randomly chosen function. Let $\mathcal{O}_h$ be an oracle which on input $x \in \{0,1\}^{2k}$ outputs (x', y), where $y = h(x)$ and $x' \underset{\mathcal{U}}{\leftarrow} h^{-1}(y)$.

We show that, relative to random $\mathcal{O}_h$, the function h (computed by calling $(x', y) \leftarrow \mathcal{O}(x)$ and returning y) is everywhere chain-resistant.

We use a counting argument to show that this remains so for a fixed (non-random) oracle $\mathcal{O}$.

There exist no 'generic attacks' that break (H, h)-time-stamping schemes by using arbitrary 2nd pre-image finders for h (when h is viewed as a black-box).