On Chosen Target Forced Prefix preimage-resistance

Michal Rjaško

Comenius University in Bratislava
Faculty of Mathematics, Physics and Informatics
Department of Computer Science
rjasko@dcs.fmph.uniba.sk

June 23, 2009

Hash function basics

- Hash function, in general, is a function $F : \mathcal{M} \rightarrow \mathcal{Y}$, where $|\mathcal{M}| >> |\mathcal{Y}|$.
  - We consider only functions $F : \{0,1\}^* \rightarrow \{0,1\}^y$.
- Cornerstones of current cryptography due to many applications:
  - Digital signatures
  - Message authentication
  - Password storage
  - Data integrity
  - ...
- Many different applications bring many different security properties that cryptographic hash functions should preserve.

Hash function basics

- Hash function, in general, is a function $F : \mathcal{M} \to \mathcal{Y}$, where $|\mathcal{M}| >> |\mathcal{Y}|$.
  - We consider only functions $F : \{0,1\}^* \to \{0,1\}^y$.
- Cornerstones of current cryptography due to many applications:
  - Digital signatures
  - Message authentication
  - Password storage
  - Data integrity
  - ...
- Many different applications bring many different security properties that cryptographic hash functions should preserve.

Hash function properties

Basic properties of every "good" hash function:

- *Preimage resistance*
  - for given image Y it is hard to find message M: $F(M) = Y$.
- *Second-preimage resistance*
  - for given message M it is hard to find message $M' \neq M$: $F(M) = F(M')$.
- *Collision resistance*
  - it is hard to find two different messages M, M': $F(M) = F(M')$.

Hash function family

$H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$.

- Preimage resistance:
  $$\mathbf{Adv}_H^{\mathrm{Pre}[\lambda]}(A) = \Pr\Big[K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^{\lambda}; Y \leftarrow H_K(M); M' \leftarrow A(K,Y) : H_K(M') = Y\Big]$$
- Second-preimage resistance:
  $$\mathbf{Adv}_H^{\mathrm{Sec}[\lambda]}(A) = \Pr\Big[K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^{\lambda}; M' \leftarrow A(K,M) : (M \neq M') \wedge (H_K(M) = H_K(M'))\Big]$$
- Collision resistance:
  $$\mathbf{Adv}_H^{\mathrm{Coll}}(A) = \Pr\Big[K \xleftarrow{\$} \mathcal{K}; (M,M') \leftarrow A(K) : (M \neq M') \wedge (H_K(M) = H_K(M'))\Big]$$

Everywhere and always versions – maximize the advantage over all keys (always) or messages (everywhere) – aPre, ePre, aSec, eSec

- maximizing Coll advantage makes no sense

Hash function family

$H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$.

- Preimage resistance:
$$\mathbf{Adv}_H^{\mathrm{Pre}[\lambda]}(A) = \Pr\Big[K \stackrel{\$}{\leftarrow} \mathcal{K}; M \stackrel{\$}{\leftarrow} \{0,1\}^\lambda; Y \leftarrow H_K(M); M' \leftarrow A(K,Y) : H_K(M') = Y\Big]$$
- Second-preimage resistance:
$$\mathbf{Adv}_H^{\mathrm{Sec}[\lambda]}(A) = \Pr\Big[K \stackrel{\$}{\leftarrow} \mathcal{K}; M \stackrel{\$}{\leftarrow} \{0,1\}^\lambda; M' \leftarrow A(K,M) : (M \neq M') \wedge (H_K(M) = H_K(M'))\Big]$$
- Collision resistance:
$$\mathbf{Adv}_H^{\mathrm{Coll}}(A) = \Pr\Big[K \stackrel{\$}{\leftarrow} \mathcal{K}; (M,M') \leftarrow A(K) : (M \neq M') \wedge (H_K(M) = H_K(M'))\Big]$$

Everywhere and always versions – maximize the advantage over all keys (always) or messages (everywhere) – aPre, ePre, aSec, eSec

- maximizing Coll advantage makes no sense

Hash function family

$H : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^y$.

- Preimage resistance:
  $$\mathbf{Adv}_H^{\mathrm{Pre}[\lambda]}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^\lambda; Y \leftarrow H_K(M); M' \leftarrow A(K,Y) : H_K(M') = Y\right]$$
- Second-preimage resistance:
  $$\mathbf{Adv}_H^{\mathrm{Sec}[\lambda]}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^\lambda; M' \leftarrow A(K,M) : (M \neq M') \wedge (H_K(M) = H_K(M'))\right]$$
- Collision resistance:
  $$\mathbf{Adv}_H^{\mathrm{Coll}}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; (M, M') \leftarrow A(K) : (M \neq M') \wedge (H_K(M) = H_K(M'))\right]$$

Everywhere and always versions – maximize the advantage over all keys (always) or messages (everywhere) – aPre, ePre, aSec, eSec

- maximizing Coll advantage makes no sense

Nostradamus attack

Created by Kelsey and Kohno, 2006.

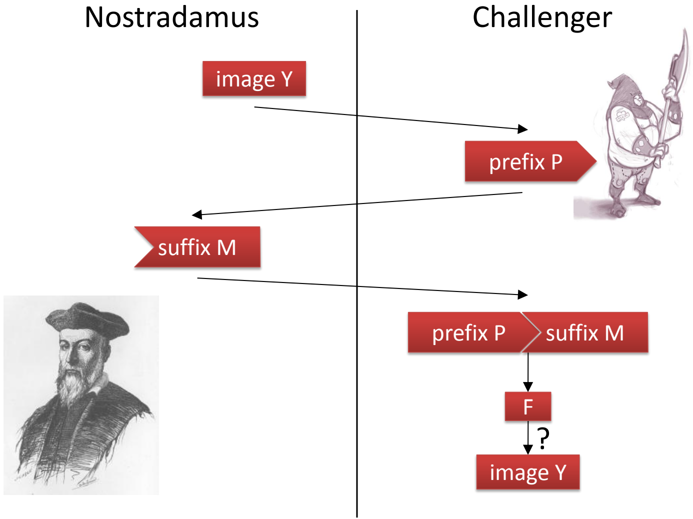
- Applies to Merkle-Damgård hash functions.
- Attack scenario (let F be some hash function) :
  1. Nostradamus provides a hash Y of some predictions, e.g. closing stock prices of S&P500.
  2. The prices become public.
  3. Nostradamus has to publish a message M containing the exact closing prices and possibly some other (uncertain) predictions, where $F(M) = Y$.

Nostradamus attack

Created by Kelsey and Kohno, 2006.

- Applies to Merkle-Damgård hash functions.
- Attack scenario (let F be some hash function) :
  1. Nostradamus provides a hash Y of some predictions, e.g. closing stock prices of S&P500.
  2. The prices become public.
  3. Nostradamus has to publish a message M containing the exact closing prices and possibly some other (uncertain) predictions, where $F(M) = Y$.

Nostradamus attack



Chosen Target Forced Prefix preimage resistance

- Property that guarantees h.f. security against Nostradamus attack
- Chosen Target – the image Y; Forced Prefix – the prefix P
- Formal definition:

$$\begin{aligned}\mathbf{Adv}_H^{\mathrm{CTFP}[\lambda]}(A) \;=\; & \Pr\Big[K \xleftarrow{\$} \mathcal{K}; (Y,S) \leftarrow A(K); P \xleftarrow{\$} \{0,1\}^{\lambda}; \\ & M \leftarrow A(P,S) : H_K(P\|M) = Y\Big]\end{aligned}$$

- always CTFP preimage resistance:

$$\begin{aligned}\mathbf{Adv}_H^{\mathrm{aCTFP}[\lambda]}(A) \;=\; & \max_{K\in\mathcal{K}}\Big(\Pr\Big[(Y,S) \leftarrow A; P \xleftarrow{\$} \{0,1\}^{\lambda}; \\ & M \leftarrow A(P,S) : H_K(P\|M) = Y\Big]\Big)\end{aligned}$$

Chosen Target Forced Prefix preimage resistance

- Property that guarantees h.f. security against Nostradamus attack
- Chosen Target – the image Y; Forced Prefix – the prefix P
- Formal definition:

$$\begin{aligned}\mathbf{Adv}_H^{\mathrm{CTFP}[\lambda]}(A) &= \Pr\Big[K \xleftarrow{\$} \mathcal{K}; (Y,S) \leftarrow A(K); P \xleftarrow{\$} \{0,1\}^{\lambda}; \\ &\qquad M \leftarrow A(P,S) : H_K(P \| M) = Y\Big]\end{aligned}$$

- always CTFP preimage resistance:

$$\begin{aligned}\mathbf{Adv}_H^{\mathrm{aCTFP}[\lambda]}(A) &= \max_{K \in \mathcal{K}} \Big(\Pr\Big[(Y,S) \leftarrow A; P \xleftarrow{\$} \{0,1\}^{\lambda}; \\ &\qquad M \leftarrow A(P,S) : H_K(P \| M) = Y\Big]\Big)\end{aligned}$$

Other properties analyzed in our work:

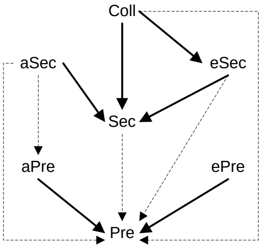
- Message authentication codes (unforgeability) (MAC):
  - $\mathbf{Adv}_H^{\mathrm{MAC}}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; (M, Y) \leftarrow A^{H_K} : H_K(M) = Y \wedge M \text{ not queried}\right]$
- Pseudo random function (Prf):
  - $\mathbf{Adv}_H^{\mathrm{Prf}}(A) = \left| \Pr\left[K \xleftarrow{\$} \mathcal{K}; 1 \leftarrow A^{H_K(\cdot)}\right] - \Pr\left[f \xleftarrow{\$} Func(\mathcal{M}, \mathcal{Y}); 1 \leftarrow A^f\right]\right|$
- Pseudo random oracle (Pro):
  - $$\mathbf{Adv}_{H,f,\mathcal{S}}^{\mathrm{Pro}}(A) = \left| \Pr\left[K \xleftarrow{\$} \mathcal{K}; 1 \leftarrow A^{H_K^f(\cdot), f(\cdot)}(K)\right] - \right.$$ $$\left. - \Pr\left[K \xleftarrow{\$} \mathcal{K}; \mathcal{F} \xleftarrow{\$} Func(\mathcal{M}, \mathcal{Y}); 1 \leftarrow A^{\mathcal{F}(\cdot), \mathcal{S}^{\mathcal{F}}(K, \cdot)}(K)\right]\right|$$

Relationships

- Intuition: xxx $\rightarrow$ yyy $\Leftrightarrow$ $(\forall H)$: if H is xxx-secure, then H is yyy-secure.
- Rogaway, Shrimpton 2004: relationships among preimage resistance, 2nd-preimage resistance and collision resistance.

Two types of implication and separation

- Conventional
- Provisional – the strength depends on a particular hash function
  - e.g. Sec $\rightarrow$ Pre to 2^{y-m} $H : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^y$

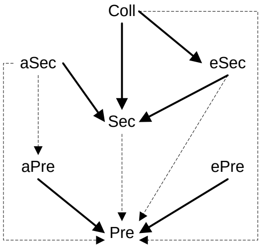


Relationships

- Intuition: xxx $\rightarrow$ yyy $\Leftrightarrow$ $(\forall H)$: if H is xxx-secure, then H is yyy-secure.
- Rogaway, Shrimpton 2004: relationships among preimage resistance, 2nd-preimage resistance and collision resistance.

Two types of implication and separation

- Conventional
- Provisional – the strength depends on a particular hash function
  - e.g. Sec $\rightarrow$ Pre to 2^{y-m}
    $H : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^y$



Relationships II

- We used different, “asymptotic” definitions of implication and separation.
  - xxx $\rightarrow$ yyy, if for every h.f.f. H and polynomial adversary A, that has non-negligible advantage in *yyy* sense there exists a polynomial adversary B with non-negligible advantage in *xxx* sense (against H).
- Such definitions are more “general”
- There are cases, where Rogaway and Shrimpton’s definitions do not work
- Asymptotic definitions are less precise

Result from 2008

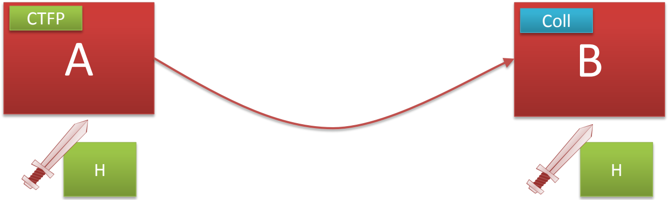
	Pre	aPre	ePre	Sec	aSec	eSec	Coll	MAC	Prf	Pro
Pre	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
aPre	$\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
ePre	$\rightarrow$	$\not\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
Sec	$\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
aSec	$\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
eSec	$\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\not\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
Coll	$\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
Mac	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	x	$\not\rightarrow$	$\not\rightarrow$
Prf	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	x	$\not\rightarrow$
Pro	$\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	x

Extension to CTFP

	CTFP	aCTFP		CTFP	aCTFP
Pre	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	MAC	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$
aPre	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	CTFP	x	$\not\rightarrow$ $\leftarrow$
ePre	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	aCTFP	$\rightarrow$ $\not\leftarrow$	x
Sec	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	Prf	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$
aSec	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	Pro	$\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$
eSec	$\not\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$	Coll	$\rightarrow$ $\not\leftarrow$	$\not\rightarrow$ $\not\leftarrow$

Example 1: Coll $\rightarrow$ CTFP

Let $H : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{Y}$ be a hash function family



$$\mathbf{Adv}_H^{\mathrm{CTFP}[\lambda]}(A) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; (Y, S) \leftarrow A(K); P \xleftarrow{\$} \{0,1\}^\lambda; M \leftarrow A(P, S) : H_K(P||M) = Y\right]$$

Example 1: Coll $\rightarrow$ CTFP

Adversary $B(K)$

1 $(Y, S) \leftarrow A(K)$

2 **let** $P_1 \xleftarrow{\$} \{0,1\}^\lambda$

3 $M_1 \leftarrow A(P_1, S)$

4 **let** $P_2 \xleftarrow{\$} (\{0,1\}^\lambda - \{P_1\})$

5 $M_2 \leftarrow A(P_2, S)$

6 **return** $(P_1 || M_1, P_2 || M_2)$

If A succeeds in the 3^{rd} and 5^{th} line, then B finds a collision.

$$P_1 || M_1 \neq P_2 || M_2$$

$$H_K(P_1 || M_1) = H_K(P_2 || M_2) = Y$$

$\square$

Example 2: CTFP $\not\to$ Coll

Let $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ be a hash function family.

$$H'_K(M) = H_K(M[1 \ldots |M| - 1] || 0)$$

- $\forall K \in \mathcal{K} : \; H'_K(01) = H'_K(00)$
- H' is not Coll secure

We need to show: if H is CTFP secure, then so is H'

Example 2: CTFP $\not\to$ Coll

Let $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ be a hash function family.

$$H'_K(M) = H_K(M[1 \ldots |M| - 1] || 0)$$

- $\forall K \in \mathcal{K} :\ H'_K(01) = H'_K(00)$
- H' is not Coll secure

We need to show: if H is CTFP secure, then so is H'

Example 2: CTFP $\not\to$ Coll

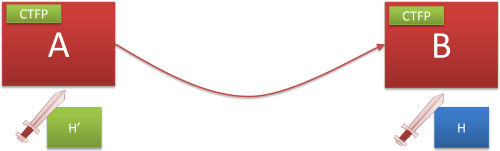
Let $H : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ be a hash function family.

$$H'_K(M) = H_K(M[1 \ldots |M| - 1] || 0)$$

- $\forall K \in \mathcal{K} :\ H'_K(01) = H'_K(00)$
- H' is not Coll secure

We need to show: if H is CTFP secure, then so is H'

Example 2: CTFP $\not\to$ Coll



Adversary B
[1^{st} **stage with input** K**]**
$(Y, S) \leftarrow A(K)$
return $(Y, S||K)$
[2^{nd} **stage with input** $(P, S||K)$**]**
$M \leftarrow A(P, S)$
if $H_K(P||M) = Y$ **then return** M
else let $b := M[|M|]$;
return $M[1 \ldots |M| - 1]||\overline{b}$

- Consider that A succeeds, i.e. $H'_K(P||M) = Y$
- $H_K(P||M) = Y$ or $H_K(P||M') = Y$ ($M' = M$ but with the last bit inverted)
- Therefore B succeeds

$\square$

Conclusion

- We formalize the CTFP preimage resistance in hash function family settings,
- Defined always CTFP preimage resistance,
- Worked out all the relationships among the definitions of CTFP, aCTFP and the other security notions (except those that appeared before).

Motivation:

- It is useful to know the relationships among the properties, that we want the hash function to preserve.

Conclusion

- We formalize the CTFP preimage resistance in hash function family settings,
- Defined always CTFP preimage resistance,
- Worked out all the relationships among the definitions of CTFP, aCTFP and the other security notions (except those that appeared before).

Motivation:

- It is useful to know the relationships among the properties, that we want the hash function to preserve.

The End

Thank you for your attention

and

have a nice day.