Lecture 11.1: Collision-Resistant Hash Functions

Collision-resistant Hash Functions

- A function h for which it is hard to find two $x \neq x'$ such that $h(x) = h(x')$

Collision-resistant Hash Functions

- A function h for which it is hard to find two $x \neq x'$ such that $h(x) = h(x')$
- Impossible for non-uniform adversary notion: Why?

Collision-resistant Hash Functions

- A function h for which it is hard to find two $x \neq x'$ such that $h(x) = h(x')$
- Impossible for non-uniform adversary notion: Why?
- Must consider a family of hash functions

Collision-Resistant Hash Function Family

Definition (Collision-Resistant Hash Function Family)

A set of functions $H = \{h_i \colon D_i \to R_i\}_{i \in I}$ is a collision-resistant hash function family (CRHF) if:

- (Easy to Sample) There exists PPT Gen such that: $\mathrm{Gen}(1^n) \in I$

Collision-Resistant Hash Function Family

Definition (Collision-Resistant Hash Function Family)

A set of functions $H = \{h_i \colon D_i \to R_i\}_{i \in I}$ is a collision-resistant hash function family (CRHF) if:

- (Easy to Sample) There exists PPT Gen such that: $\mathsf{Gen}(1^n) \in I$
- (Compression) $|R_i| < |D_i|$

Collision-Resistant Hash Function Family

Definition (Collision-Resistant Hash Function Family)

A set of functions $H = \{h_i \colon D_i \rightarrow R_i\}_{i \in I}$ is a collision-resistant hash function family (CRHF) if:

- (Easy to Sample) There exists PPT Gen such that: $\mathrm{Gen}(1^n) \in I$
- (Compression) $|R_i| < |D_i|$
- (Easy to Evaluate) Given $x \in D_i$ and $i \in I$, there exists PPT Eval such that $\mathrm{Eval}(x, i)$ computes $h_i(x)$

Collision-Resistant Hash Function Family

Definition (Collision-Resistant Hash Function Family)

A set of functions $H = \{h_i \colon D_i \to R_i\}_{i \in I}$ is a collision-resistant hash function family (CRHF) if:

- (Easy to Sample) There exists PPT Gen such that: $\mathsf{Gen}(1^n) \in I$
- (Compression) $|R_i| < |D_i|$
- (Easy to Evaluate) Given $x \in D_i$ and $i \in I$, there exists PPT Eval such that $\mathsf{Eval}(x, i)$ computes $h_i(x)$
- (Collision Resistance) For all n.u. PPT $\mathcal{A}$, there exists negligible $\nu(\cdot)$ such that (eventually) for $n \in \mathbb{N}$,

$$\Pr\left[\begin{array}{c} i \xleftarrow{\$} \mathsf{Gen}(1^n), \\ (x,x') \xleftarrow{\$} \mathcal{A}(1^n,i) \end{array} : \begin{array}{c} x \neq x' \ \wedge \\ h_i(x) = h_i(x') \end{array}\right] \leqslant \nu(n)$$

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]
- Related notion: Universal One-way Hash Functions (UOWHF)

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]
- Related notion: Universal One-way Hash Functions (UOWHF)
  - $\Pr\left[\begin{array}{c}(x,\text{state})\xleftarrow{\$}\mathcal{A}(1^n),\\ i\xleftarrow{\$}\mathsf{Gen}(1^n),\\ x'\xleftarrow{\$}\mathcal{A}(i,\text{state})\end{array} : \begin{array}{c}x\neq x' \wedge\\ h_i(x)=h_i(x')\end{array}\right]\leqslant \nu(n)$

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]
- Related notion: Universal One-way Hash Functions (UOWHF)
  - $\Pr\left[\begin{array}{c} (x,\mathsf{state}) \xleftarrow{\$} \mathcal{A}(1^n), \\ i \xleftarrow{\$} \mathsf{Gen}(1^n), \\ x' \xleftarrow{\$} \mathcal{A}(i,\mathsf{state}) \end{array} : \begin{array}{c} x \neq x' \ \wedge \\ h_i(x) = h_i(x') \end{array}\right] \leqslant \nu(n)$
  - Can be constructed from OWF [Rompel-90]

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]
- Related notion: Universal One-way Hash Functions (UOWHF)
  - $\Pr\left[\begin{array}{c} (x,\mathsf{state}) \xleftarrow{\$} \mathcal{A}(1^n), \\ i \xleftarrow{\$} \mathsf{Gen}(1^n), \\ x' \xleftarrow{\$} \mathcal{A}(i,\mathsf{state}) \end{array} : \begin{array}{c} x \neq x' \ \wedge \\ h_i(x) = h_i(x') \end{array}\right] \leqslant \nu(n)$
  - Can be constructed from OWF [Rompel-90]
  - Suffices for Digital Signatures [Naor-Yung-89]

Perspective

- One-bit compression implies arbitrary bit compression (Proof?)
- Read: Merkle Tree
- Range cannot be too small
  - Enumeration Attacks
  - Birthday Attacks
- Unlikely that they can be constructed from OWF or OWP [Simon-98]
- Related notion: Universal One-way Hash Functions (UOWHF)
  - $\Pr\left[\begin{array}{c} (x,\mathsf{state}) \xleftarrow{\$} \mathcal{A}(1^n), \\ i \xleftarrow{\$} \mathsf{Gen}(1^n), \\ x' \xleftarrow{\$} \mathcal{A}(i,\mathsf{state}) \end{array} : \begin{array}{c} x \neq x' \;\wedge \\ h_i(x) = h_i(x') \end{array}\right] \leqslant \nu(n)$
  - Can be constructed from OWF [Rompel-90]
  - Suffices for Digital Signatures [Naor-Yung-89]
  - More Efficient Construction [Haitner-Holenstein-Reingold-Vadhan-Wee-10]