Lecture 11.2: Digital Signatures

One-time Signatures for Arbitrarily-long Messages

- Let $H = \{h_i\}_{i \in I}$ be a CRHF with domain $\{0,1\}^*$ and range $\{0,1\}^n$

One-time Signatures for Arbitrarily-long Messages

- Let $H = \{h_i\}_{i \in I}$ be a CRHF with domain $\{0,1\}^*$ and range $\{0,1\}^n$
- Use Lamport signature scheme where $h_i(m)$ is signed instead of m

One-time Signatures for Arbitrarily-long Messages

- Let $H = \{h_i\}_{i \in I}$ be a CRHF with domain $\{0,1\}^*$ and range $\{0,1\}^n$
- Use Lamport signature scheme where $h_i(m)$ is signed instead of m
- Proof?

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathsf{Gen}(1^n)$

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathsf{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:
  - $(sk_i, pk_i) \xleftarrow{\$} \mathrm{Gen}(1^n)$

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:
  - $(sk_i, pk_i) \xleftarrow{\$} \mathrm{Gen}(1^n)$
  - $\widetilde{\sigma}_i = \mathrm{Sign}_{sk_{i-\mathbf{1}}}(m_i \| pk_i)$

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:
  - $(sk_i, pk_i) \xleftarrow{\$} \mathrm{Gen}(1^n)$
  - $\widetilde{\sigma}_i = \mathrm{Sign}_{sk_{i-1}}(m_i \| pk_i)$
  - Output $\sigma_i = (i, \widetilde{\sigma}_i, m_i, pk_i, \sigma_{i-1})$

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:
  - $(sk_i, pk_i) \xleftarrow{\$} \mathrm{Gen}(1^n)$
  - $\widetilde{\sigma}_i = \mathrm{Sign}_{sk_{i-1}}(m_i \| pk_i)$
  - Output $\sigma_i = (i, \widetilde{\sigma}_i, m_i, pk_i, \sigma_{i-1})$
  - Increment i

Multi-message Signatures

- $(sk_0, pk_0) \xleftarrow{\$} \mathrm{Gen}(1^n)$
- Let $\widetilde{\sigma}_0 = \emptyset$, $i = 1$
- To sign m_i:
  - $(sk_i, pk_i) \xleftarrow{\$} \mathrm{Gen}(1^n)$
  - $\widetilde{\sigma}_i = \mathrm{Sign}_{sk_{i-1}}(m_i \| pk_i)$
  - Output $\sigma_i = (i, \widetilde{\sigma}_i, m_i, pk_i, \sigma_{i-1})$
  - Increment i
- Proof?