CSC 2426: Fundamentals of Cryptography **Fall 2023**

Lecture 7: Digital Signatures

Instructor: Akshayaram Srinivasan *Scribe: Reina Li*

Date: October 30, 2023

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

7.1 Recap and roadmap

Last time, we constructed a one-time signature (OTS) scheme (KeyGen, Sign, Verify) that is correct and secure. In that scheme, the signing key and verification keys need to be size $2nm(n)$ (where $m(n)$ is the output size of the OWF used) for messages of size n. This begs the question: can we make an OTS for longer messages with a shorter key? Furthermore, can we make a signature scheme that is secure for signing multiple messages?

In this lecture, first, we introduce a new class of functions: Collision-Resistant Hash Functions. We will defer the discussion on their existence and construction to a future lecture. Then, we will use such a function to construct an OTS for long messages. Finally, we will use this new OTS to create a signature scheme that can securely sign polynomially many messages.

7.2 Collision-Resistant Hash Function (CRHF)

Consider a function (Setup, Eval):

$$\begin{aligned} \text{Setup}(1^n) &\to hk, \text{ the hash key} \\ \text{Eval}(hk, x) &\to h, \text{ the digest} \end{aligned}$$

Where $|x| > |h|$. Then, the range of Eval ($\subseteq \{0,1\}^{|h|}$) must be smaller than its domain ($\{0,1\}^{|x|}$), and, as such, there are many collisions occurring (at least $\lfloor 2^{|x|}/2^{|h|} \rfloor$ collisions).

We say (Setup, Eval) is a CRHF if the probability of an adversary finding a pair of inputs that collide is negligible. That is, for any PPT adversary $\mathcal{A}$

$$\Pr_{hk \leftarrow (Setup)(1^n)}[\mathcal{A}(1^n, hk) = (x, x') \text{ s.t. } x \neq x' \text{and Eval}(hk, x) = \text{Eval}(hk, x')] \leq \text{negl}(n)$$

For now, assume such functions exist. In particular, assume there exists a CRHF where the message is size $q(n)$ (i.e. polynomial in the input size n) and the digest is size n.

7.3 OTS for large messages

We will use collision-resisitant hashing to construct a one-time signature scheme with short verification keys.

7.3.1 Construction

Consider (KeyGen, Sign, Verify), an OTS that signs messages of size n and has $|vk|= 2nm(n)$, and (Setup, Eval), a CRHF mapping $\{0,1\}^{q(n)} \to \{0,1\}^n$. From these, we will construct a OTS scheme, (KeyGen′, Sign′, Verify′), with $|vk'|= 2nm(n) + n$, that signs messages of size $q(n)$ (which may be polynomially larger than n).

We define it as follows:

$$\begin{aligned}
\mathrm{KeyGen}'(1^n): \quad & (vk, sk) \leftarrow \mathrm{KeyGen}(1^n) \\
& hk \leftarrow \mathrm{Setup}(1^n) \\
& vk' = (vk, hk),\ sk' = (sk, hk) \\
\mathrm{Sign}'\left(sk', m \in \{0,1\}^{q(n)}\right): \quad & m' = \mathrm{Eval}(hk, m) \\
& \sigma = \mathrm{Sign}(sk, m') \\
\mathrm{Verify}'(vk', (m, \sigma)): \quad & m' = \mathrm{Eval}(hk, m) \\
& \mathrm{Verify}(vk, (m', \sigma))
\end{aligned}$$

Where the last line of each part are the respective outputs.

7.3.2 Correctness and security

Correctness: follows from the correctness of (KeyGen, Sign, Verify).

Security: We will use a hybrid argument.

H0: Real game

H1: Modified game where, when $\mathcal{A}$ produces (m^*, σ^*) (with $m^* \neq m$), if $\mathrm{Eval}(hk, m^*) = \mathrm{Eval}(hk, m)$, then abort.

Claim 7.1 $|\Pr[\mathcal{A}$ *wins in H0*$] - \Pr[\mathcal{A}$ *wins in H1*$]| \leq$ *negl.*

Proof: Note Pr[H1 aborts] = Pr[$\mathcal{A}$ finds collision] is a negligible function (from CRHF security). Also, the games are identical when $\mathcal{A}$ does not find a collision.

$$
\begin{aligned}
&\Pr[\mathcal{A} \text{ wins in H0}] - \Pr[\mathcal{A} \text{ wins in H1}] \\
&= \Pr[\text{wins H0}] - \Pr[\text{wins H1}|!\,\text{collision}]\Pr[!\,\text{collision}] \\
&= \Pr[\text{wins H0}] - \Pr[\text{wins H0}|!\,\text{collision}]\Pr[!\,\text{collision}] \\
&= \Pr[\text{wins H0}|\text{collision}]\Pr[\text{collision}] \\
&\leq \Pr[\text{collision}]
\end{aligned}
$$

■

Now, it remains to show that $\Pr[\mathcal{A}$ wins in H1$]$ is negligible, which would imply $\Pr[\mathcal{A}$ wins in H0$]$ is also negligible.

Claim 7.2 $\Pr[\mathcal{A}$ *wins in H1*$] \leq$ *negl.*

Proof: Assume towards a contradiction that $\Pr[\mathcal{A}$ wins in H1$]$ is non-negligible. Consider an adversary $\mathcal{B}$, who breaks the security of the OTS by playing *H1* against $\mathcal{A}$ as follows:

$$
\begin{array}{ccrcr}
\mathcal{A} & & \mathcal{B} & & \text{Challenger} \\
 & \xleftarrow{(vk, hk)} & hk \leftarrow \text{Setup}(1^n) & \xleftarrow{vk} & (vk, sk) \leftarrow \text{KeyGen}(1^n) \\
 & \xrightarrow{m} & m' \leftarrow \text{Eval}(hk, m) & \xrightarrow{m'} & \\
 & \xleftarrow{\sigma} & & \xleftarrow{\sigma} & \sigma \leftarrow \text{Sign}(sk, m') \\
 & \xrightarrow{(m^*, \sigma^*)} & m^{**} \leftarrow \text{Eval}(hk, m^*) & \xrightarrow{(m^{**}, \sigma^*)} &
\end{array}
$$

When $\mathcal{A}$ wins, it produces a (m^*, σ^*) that $\text{Verify}'(vk', \cdot)$ accepts. Then, $(\text{Eval}(hk, m^*), \sigma^*)$ must be accepted by $\text{Verify}(vk, \cdot)$, by definition. Furthermore, $\text{Eval}(hk, m^*) \neq \text{Eval}(hk, m)$, by assumption. Thus, $\mathcal{A}$ wins against $\mathcal{B} \implies \mathcal{B}$ wins against OTS. So, $\mathcal{B}$ wins against the OTS with non-negligible probability, a contradiction. ■

7.4 q-Time Signature

We will now construct a q-time digital signature scheme where the adversary can query for q-signatures before attempting to forge a signature on a different message.

7.4.1 Construction

Let (Setup, Eval) be a PRF and (KeyGen, Sign, Verify) be an OTS (as constructed in the previous section). From these, we construct a q-Time secure signature scheme (KeyGen′, Sign′, Verify′) for messages of length n as follows:

$$\text{KeyGen}'(1^n): \quad (vk_\epsilon, sk_\epsilon) \leftarrow \text{KeyGen}(1^n)$$
$$k \leftarrow \text{Setup}(1^n)$$
$$vk = vk_\epsilon,\ sk = (k, sk_\epsilon)$$

$$\text{Sign}'(sk, m \in \{0,1\}^n): \quad \text{does the following:}$$

Build a complete binary tree with 2^n leaves. For each node, labelled l, let $r \leftarrow \text{Eval}(k, l)$. Use a PRG to stretch r to $2n^2$ bits to generate sk_l and then generate vk_l as in the OTS construction. This way, (vk_l, sk_l) are deterministic but computationally indistinguishable from random.

Starting from the root ($l = \epsilon$, $h = 0$), do $\text{Sign}(sk_l, vk_{l,0}||vk_{l,1}) = \sigma_h$, where $vk_{l,0}$ and $vk_{l,1}$ are the vk's of the left and right children of node l. If the h^{th} bit of m is 0, continue on the left child, otherwise continue on the right child. When the leaf node is reached, do $\text{Sign}(sk_m, m) = \sigma_m$, where sk_m is the sk of the node corresponding to m.

Output σ, which contains $vk_{l,0}||vk_{l,1}$ for each node l visited, and the signatures $\sigma_1, ..., \sigma_n, \sigma_m$.

$$\text{Verify}'(vk, \sigma): \quad \text{does the following:}$$

For each level h (besides the leaf), call $\text{Verify}(vk_{l_h}, (vk_{l_h,0}||vk_{l_h,1}, \sigma_h))$ (where l_h is the node visited at level h). Also call $\text{Verify}(vk_m, (m, \sigma_m))$, where vk_m is the vk of the node corresponding to m. (Note that each vk is either vk_ϵ or given in σ, so each Verify call is possible). Output the AND of these Verify calls.

7.4.2 Correctness and security

Correctness: follows from OTS correctness.

Security: We will use a hybrid argument.

H0: Real game

H1: Modified game where $sk_l \leftarrow \text{KeyGen}(1^n)$ (i.e. $sk_l \leftarrow$ random), as opposed to generated by PRF and stretched by PRG.

Then, $|\Pr[\mathcal{A} \text{ wins in H1}] - \Pr[\mathcal{A} \text{ wins in H0}]| \leq negl.$ by pseudo-randomness of PRF and PRG.

H2: Modified game where:

First, we randomly choose i from $1...q(n)$ and j from $1...n$, where $q(n)$ is the number of queries the adversary can make. Let i^* be the j^{th} node visited in the i^{th} query. Then we play the game in *H1*, where, $\mathcal{A}$ queries on $q(n)$ messages and, finally, submits (m^*, σ^*) (with $m^* \neq m_1, ..., m_{q(n)}$), which consists of $\sigma_{m^*}, (vk_{m^*}||vk_{m_s^*}, \sigma_n), ..., (vk_0||vk_1, \sigma_1)$. If it turns out that i^* is the first node from the bottom in the intersection of nodes visited when signing m^* and the nodes seen when signing $m_1, ..., m_{q(n)}$, we proceed. Otherwise, abort. (Note: visited here refers to having had its sk used, while seen refers to having had its vk signed).

Claim 7.3 $\Pr[\mathcal{A}$ *wins in H2*$] = \Pr[\mathcal{A}$ *wins in H1*$] \Pr[i^*$ *correct*$]$.

Proof: Note that producing valid (m^*, σ^*) is independent from correctly guessing i^*. Then,

$$\begin{aligned} &\Pr[\mathcal{A} \text{ wins in H2}] \\ &= \Pr[\mathcal{A} \text{ correctly produces } (m^*, \sigma^*) \text{ and } i^* \text{ correct}] \\ &= \Pr[\mathcal{A} \text{ correctly produces } (m^*, \sigma^*)] \Pr[i^* \text{ correct}] \\ &= \Pr[\mathcal{A} \text{ wins in H1}] \Pr[i^* \text{ correct}] \end{aligned}$$

■

Claim 7.4 $\Pr[i^*$ *correct*$] \geq \frac{1}{q(n)n}$

Proof: It follows from the selection of i^* and the fact that only one node can be the first node in the intersection of the m^* path and the previous paths. The inequality arises because the intersection may be found on multiple paths. ■

Now, it remains to show that $\Pr[\mathcal{A}$ wins in H2$]$ is negligible, which would imply $\Pr[\mathcal{A}$ wins in H1$]$ (and thus $\Pr[\mathcal{A}$ wins in H0$]$) is also negligible.

Claim 7.5 $\Pr[\mathcal{A}$ *wins in H2*$] \leq$ *negl.*

Proof: Assume towards a contradiction that $\Pr[\mathcal{A}$ wins in H2$]$ = non-negl. Consider an adversary $\mathcal{B}$ who breaks the OTS security by playing against $\mathcal{A}$ as follows:

$\mathcal{A}$		$\mathcal{B}$		Challenger
		$i^* \leftarrow$ random	$\xleftarrow{vk}$	$(vk, sk) \leftarrow \text{KeyGen}(1^n)$
		$\forall l, (vk_l, sk_l) \leftarrow \text{KeyGen}(1^n)$		
	$\xleftarrow{vk_\epsilon}$	$vk_{i^*} \leftarrow vk$ (sk_{i^*} is unknown)		
	$\xrightarrow{m_1...m_{q(n)}}$			
			$\xrightarrow{vk_{i^*\Vert 0}, vk_{i^*\Vert 1}}$	
			$\xleftarrow{\sigma}$	
	$\xleftarrow{\sigma_1, ...\sigma_{q(n)}}$	$\forall i = 1...q(n),\ \text{Sign}'(sk_\epsilon, m_i) = \sigma_i$		
	$\xrightarrow{(m^*, \sigma^*)}$	$((vk_{i^*,0}\Vert vk_{i^*,1}, \sigma_{i^*}) \in \sigma^*)$	$\xrightarrow{(vk^*_{i^*,0}\Vert vk^*_{i^*,1}, \sigma_{i^*})}$	

Since vk_{i^*} is generated through $\text{KeyGen}(1^n)$, it is generated identically to all the other vk's in the tree. Thus, the game between $\mathcal{A}$ and $\mathcal{B}$ is just *H2*.

When $\mathcal{A}$ wins, (m^*, σ^*) is accepted by $\text{Verify}'(vk_\epsilon, \cdot)$. Then, $(vk_{i^*,0}||vk_{i^*,1}, \sigma_{i^*})$ must be accepted by $\text{Verify}(vk = vk_{i^*}, \cdot)$, by the construction of Verify$'$.

Since it is assumed that i^* was correctly chosen and is the first intersection, it must be that $(vk_{i^*\|0}, vk_{i^*\|1}) \neq (vk^*_{i^*\|0}, vk^*_{i^*\|1})$. Also, it means $(vk^*_{i^*,0}||vk^*_{i^*,1}, \sigma_{i^*})$ is a valid response from $\mathcal{B}$ to win against the Challenger.

Thus, $\mathcal{A}$ wins against $\mathcal{B} \implies \mathcal{B}$ wins against OTS. So, $\mathcal{B}$ wins against the OTS with non-negligible probability, a contradiction. ■

7.4.3 Discussion

Note that we can use the OTS security because in this construction, while the scheme can sign polynomially many messages, each (vk, sk) pair signs the same message on any input.

Also, note that we use the OTS that employs the CRHF because if we used the original OTS, we would need $|vk_\epsilon| \geq 2^n n$ (since $|vk_n| \geq 2n$, $|vk_{n-1}| \geq 4n$, $vk_{n-2} \geq 8n$, etc.), whereas here, we only need $|vk| = 2nm(n)$ for each vk.