Lecture 37: Signature of Long Messages

Recall: Trapdoor OWF/OWP I

- Let $\mathcal{F} = \{f_1, f_2, \ldots, f_\alpha\}$ be a family of functions from $\mathcal{D} \to \mathcal{R}$ (if f_is are permutations, then $\mathcal{D} = \mathcal{R}$)
- Let $T = \{\text{trap}_1, \text{trap}_2, \ldots, \text{trap}_\alpha\}$ be the set of corresponding trapdoors for these functions
- It is difficult to invert the functions f_i
- However, given trap_i, the function f_i is easy to invert
- We saw how these trapdoor OWF/OWP families can be used to construct public-key encryption and digital signatures

Recall: Trapdoor OWF/OWP II

Public-key Encryption.

Alice		Bob
$r \xleftarrow{\$} \mathcal{D}$	$\xleftarrow{\quad \mathsf{pk} \quad}$	Randomly generate $(\mathsf{pk}, \mathsf{trap}) = (i, \mathsf{trap}_i)$
$y = f_i(r)$		
$c = m \cdot r$	$\xrightarrow{\quad (y, c) \quad}$	$\widetilde{r} = f_i^{-1}(y; \mathsf{trap}_i)$
		$\widetilde{m} = c \cdot (\widetilde{r})^{-1}$

Recall: Trapdoor OWF/OWP III

- Using the RSA assumption, the functions are x^e, for $e \in \mathbb{Z}^*_{\varphi(N)}$
- The corresponding trapdoor is d such that $e \cdot d = 1 \mod \varphi(N)$

Digital Signature. based on RSA assumption

$$\begin{array}{lcr}
\underline{\text{Alice}} & & \underline{\text{Bob}} \\
\text{Generate } (N, e, d) \text{ and random } r & \xrightarrow{\mathsf{pk} = (N, e, r)} & \\
\sigma = (r \| m)^d & \xrightarrow{(m, \sigma)} & (\sigma)^e == (r \| m)
\end{array}$$

Intuitively, Alice picks a function f_e by choosing e. Then, the signature on $(r\|m)$ is $\sigma = f_e^{-1}(r\|m) = (r\|m)^d$. Verification if performed by checking $f_e(\sigma) == (r\|m)$.

Signing Long Messages I

- Suppose the integers in $\mathbb{Z}_N^*$ need $2n$-bits to be expressed
- Then, our scheme signs messages m of length n-bits, using a signature σ of length $2n$-bits
- Can we sign <u>long</u> messages using a <u>small</u> signature?

Signing Long Messages II

- The intuition here is to hash down the message using a collision-resistant hash function family, and then sign the hash
- Let $\mathcal{H} = \{h_1, h_2, \ldots, h_\beta\}$ be a family of collision-resistant hash functions from the domain $\{0,1\}^* \to \{0,1\}^n$

$$
\begin{array}{ccc}
\underline{\text{Alice}} & & \underline{\text{Bob}} \\
\begin{array}{c}\text{Generate } (N, e, d) \\ \text{and random } r \text{ and sk}\end{array} & \xrightarrow{\quad \mathsf{pk} = (N, e, r, \mathsf{sk}) \quad} & \\
\sigma = (r \| \; h_{\mathsf{sk}}(m)\;)^d & \xrightarrow{\qquad\qquad (m, \sigma) \qquad\qquad} & (\sigma)^e == (r \| \; h_{\mathsf{sk}}(m)\;)
\end{array}
$$