

Lecture 37: Signature of Long Messages

Recall: Trapdoor OWF/OWP I

- Let $\mathcal{F} = \{f_1, f_2, \dots, f_\alpha\}$ be a family of functions from $\mathcal{D} \rightarrow \mathcal{R}$ (if f_i s are permutations, then $\mathcal{D} = \mathcal{R}$)
- Let $T = \{\text{trap}_1, \text{trap}_2, \dots, \text{trap}_\alpha\}$ 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

Public-key Encryption.

Alice

Bob

$r \xleftarrow{\$} \mathcal{D}$ ← pk Randomly generate $(\text{pk}, \text{trap}) = (i, \text{trap}_i)$

$$y = f_i(r)$$

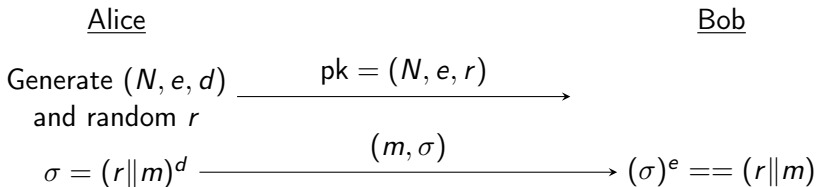
$c = m \cdot r$ → (y, c) → $\tilde{r} = f_i^{-1}(y; \text{trap}_i)$

$$\tilde{m} = c \cdot (\tilde{r})^{-1}$$

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 $e \cdot d = 1 \pmod{\varphi(N)}$

Digital Signature. based on RSA assumption



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 is 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 long messages using a small 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 $\mathcal{H} = \{h_1, h_2, \dots, h_\beta\}$ be a family of collision-resistant hash functions from the domain $\{0, 1\}^* \rightarrow \{0, 1\}^n$

