Modern Cryptography	January 31, 2019

Solutions to Homework 14

Lecturer: Christoph Striecks, TA: Karen Klein *Due: 23.59 CET, Jan 28, 2019*

1. Naor's Transformation: Signatures from Identity-Based Encryption (IBE)

- **(2 Points)** In the lecture, we have sketched the Naor transformation. Provide a formal description of the signature scheme $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Vrfy})$ with message space $\mathcal{M}_\Sigma$ resulting from applying the Naor transform to an IBE scheme $\Xi = (\mathsf{IBE.Gen}, \mathsf{IBE.Ext}, \mathsf{IBE.Enc}, \mathsf{IBE.Dec})$ with identity space $\mathcal{ID}_\Xi$ and message space $\mathcal{M}_\Xi$. Show the correctness of Σ.

  Solution: Set $\mathcal{M}_\Sigma := \mathcal{ID}_\Xi$. Further, define

  - $\mathsf{Gen}(1^n)$: for security parameter 1^n, return $(pk, sk) \leftarrow \mathsf{IBE.Gen}(1^n)$.
  - $\mathsf{Sig}_{sk}(m)$: for secret key sk, message $m \in \mathcal{M}_\Sigma$, return $\sigma \leftarrow \mathsf{IBE.Ext}(sk, m)$.
  - $\mathsf{Vrfy}_{pk}(\sigma, m)$: for public key pk, signature σ, and message $m \in \mathcal{M}_\Sigma$, return 1 if $\mathsf{IBE.Dec}(\sigma, c) = R$, for $c \leftarrow \mathsf{IBE.Enc}(pk, m, R)$, for some $R \leftarrow \mathcal{M}_\Xi$ and "identity" m, else return 0.

  Correctness of Σ follows from the correctness of Ξ: for all integer n, for $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, for all $m \in \mathcal{M}$, for all $\sigma \leftarrow \mathsf{Sig}_{sk}(m)$, we have that $\mathsf{Vrfy}_{pk}(\sigma, m) = 1$ holds. (Essentially, if σ is a valid signature for m under pk, then $\mathsf{IBE.Dec}(\sigma, \mathsf{IBE.Enc}(pk, m, R)) = R$, for all $R \in \mathcal{M}_\Xi$, where $\mathcal{M}_\Xi$ is defined in pk.) $\square$

- **(1 Point)** Apply the Naor transformation to the explicit Boneh-Franklin IBE scheme Ξ_{BF} with identity and message spaces $\mathcal{ID}_{BF}$ and $\mathcal{M}_{BF}$, respectively, from the lecture. (Assume that a group generator $g \in \mathcal{G}$ with order p, a random-oracle instantiation $\mathsf{H} : \mathcal{ID} \mapsto \mathcal{G}$, and a suitable pairing $\mathsf{e} : \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}_T$ is given as input to all algorithms.)

  Solution: Set $\mathcal{M}_\Sigma := \mathcal{ID}_\Xi$. Further, define

  - $\mathsf{Gen}(1^n)$: return $(pk, sk) := ((g^x, \mathcal{M}_\Sigma, \mathcal{M}_\Xi), x)$, for $x \leftarrow \mathbb{Z}_p$.
  - $\mathsf{Sig}_{sk}(m)$: return $\sigma := \mathsf{H}(m)^x$.
  - $\mathsf{Vrfy}_{pk}(\sigma, m)$: return 1 if $c_2/\mathsf{e}(c_1, \sigma) = R$, for $(c_1, c_2) := (g^y, \mathsf{e}(pk, \mathsf{H}(m))^y \cdot R)$, $y \leftarrow \mathbb{Z}_p$, and some $R \leftarrow \mathcal{M}_\Xi$, else return 0.

  0.5 bonus points: define verification algorithm as $\mathsf{Vrfy}_{pk}(\sigma, m)$: return 1 if $\mathsf{e}(g, \sigma) = \mathsf{e}(pk, \mathsf{H}(m))$, else return 0. (In this case, the description of the IBE message space $\mathcal{M}_\Xi$ specified in pk is not needed.) $\square$

2. Identity-Based Encryption (IBE) from Attribute-Based Encryption (ABE)

- **(2 Points)** Formally construct an IBE scheme $\Xi = (\mathsf{IBE.Gen}, \mathsf{IBE.Ext}, \mathsf{IBE.Enc}, \mathsf{IBE.Dec})$ with identity and messages spaces $\mathcal{ID}_\Xi$ and $\mathcal{M}_\Xi$, respectively, from a CP-ABE scheme $\Omega = (\mathsf{ABE.Gen}, \mathsf{ABE.Ext}, \mathsf{ABE.Enc}, \mathsf{ABE.Dec})$ with attribute space $\mathcal{A}_\Omega$, policy space $\mathcal{P}_\Omega$, and message space $\mathcal{M}_\Omega$. Show the correctness of Ξ.

  Solution: Set $\mathcal{ID}_\Xi := \mathcal{A}_\Omega$ and $\mathcal{M}_\Xi := \mathcal{M}_\Omega$. Further, define

- $\mathsf{Gen}(1^n)$: for security parameter 1^n, return $(pp, sk) \leftarrow \mathsf{ABE.Gen}(1^n)$.
- $\mathsf{Ext}_{sk}(id)$: for secret key sk, "identity" $id \in \mathcal{ID}_\Xi$, return $usk_{id} \leftarrow \mathsf{ABE.Ext}(sk, id, m)$.
- $\mathsf{Enc}_{pp}(id, m)$: for public parameters pp, identity $id \in \mathcal{ID}_\Xi$, and message $m \in \mathcal{M}_\Xi$, return $\mathsf{ABE.Enc}_{pp}(p, m)$, for policy $p := id$.
- $\mathsf{Dec}_{usk_{id}}(c)$: for user secret key usk_{id} and ciphertext c, return $m \leftarrow \mathsf{ABE.Dec}_{usk_{id}}(c)$.

Correctness of Ξ follows from the correctness of Ω in a straightforward way: for all integer n, for all $(pp, sk) \leftarrow \mathsf{Gen}(1^n)$, for all identities $id \in \mathcal{ID}_\Xi$, for all $usk_{id} \leftarrow \mathsf{Ext}_{sk}(id)$, for all $m \in \mathcal{M}_\Xi$, for all $c \leftarrow \mathsf{Enc}_{pp}(id, m)$, we have that $\mathsf{Dec}_{usk_{id}}(c) = m$ holds. $\square$