Modern Cryptography Jan 22, 2019

Homework 14

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

To get credit for this homework it must be submitted no later than Tuesday, January 28th via email to `michael.walter@ist.ac.at`, please use "MC18 Homework 14" as subject.
Please put your solutions into a single pdf file[1] and name this file Yourlastname_HW14.pdf.

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.
    - **(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.)

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.

[1] If you don't know how to do it, you can use e.g. `https://www.pdfmerge.com/`