

Homework 14

*Lecturer: Christoph Striecks, TA: Karen Klein**Due: 23.59 CET, Jan 29, 2019*

To get credit for this homework it must be submitted no later than Tuesday, January 29th via email to `michael.walter@ist.ac.at`, please use “MC18 Homework 14” as subject. Please put your solutions into a single pdf file¹ 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 $\Sigma = (\text{Gen}, \text{Sig}, \text{Vrfy})$ with message space \mathcal{M}_Σ resulting from applying the Naor transform to an IBE scheme $\Xi = (\text{IBE.Gen}, \text{IBE.Ext}, \text{IBE.Enc}, \text{IBE.Dec})$ with identity space \mathcal{ID}_Ξ and message space \mathcal{M}_Ξ . 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 $H : \mathcal{ID} \mapsto \mathcal{G}$, and a suitable pairing $e : \mathcal{G} \times \mathcal{G} \mapsto \mathcal{G}_T$ is given as input to all algorithms.)

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

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

¹If you don’t know how to do it, you can use e.g. <https://www.pdfmerge.com/>