Eidgenössische
Technische Hochschule
Zürich

Ecole polytechnique fédérale de Zurich
Politecnico federale di Zurigo
Federal Institute of Technology at Zurich

Departement of Computer Science
Prof. Dennis Hofheinz
Julia Kastner

Information Security Lab 2022
Module 02 - Reductions - Week 1
October 10 - 14

Theory Exercises

Exercise 1. Prove that if $P = NP$ there does not exist a public key encryption (PKE) scheme which is IND-CPA secure.

Exercise 2. In the following, we want to consider how one can combine existing PKE schemes to build new ones.

(a) Consider two public-key encryption (PKE) schemes $E_i = (\mathsf{KeyGen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ for $i \in \{0,1\}$. Both E_0 and E_1 are correct and have the same message space $\mathcal{M}$. Assume only one of the schemes E_0 and E_1 is IND-CPA secure. Without knowing which scheme is secure, design a PKE scheme E_2 for $\mathcal{M}$ that uses E_0 and E_1 and is IND-CPA secure and provide a proof of IND-CPA security of your new scheme.

(b) Assume you have n PKE schemes $E_i = (\mathsf{KeyGen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ for $i \in \{1, \ldots, n\}$ with the same message space $\mathcal{M}$, all of which are correct, and at least one of which is IND-CPA secure (but you do not know which one). Use these schemes to construct a new scheme E_{n+1} that is IND-CPA secure. Provide a proof for the IND-CPA security of your new scheme.

Exercise 3. Consider a cyclic group $\mathbb{G}$ of known prime order $p > 2$ and let $\mathbf{g}$ be a generator of $\mathbb{G}$.

(a) You are given access to an oracle square which on input $\mathbf{g}^a$ outputs $\mathbf{g}^{(a^2)}$. Show that given access to square, there exists a polynomial-time algorithm that solves **DDH** in $\mathbb{G}$.

(b) You are given access to an oracle inv which on input $\mathbf{g}^a$ outputs $\mathbf{g}^{\frac{1}{a}}$. Show that given access to inv, there exists a polynomial-time algorithm that solves **DDH** in $\mathbb{G}$.

Exercise 4. Consider two digital signature schemes $\Sigma_i = (\mathsf{KeyGen}_i, \mathsf{Sign}_i, \mathsf{Verify}_i)$ for $i \in \{0,1\}$. You know that both of these signature schemes are correct, but only one of them is EUF-CMA secure. Using these two schemes, construct a new digital signature scheme Σ_2 that is EUF-CMA secure. Prove the security of your new scheme.

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* eng. Third edition. Chapman & Hall/CRC cryptography and network security. Boca Raton, Florida ; CRC Press, 2021. ISBN: 1-351-13303-9.