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 2
October 17 - 21

Theory Exercises

Exercise 1 (Ex. 11.6 in Katz and Lindell [KL21])**.** Consider a cyclic group $\mathbb{G}$ of prime order p and let $\mathbf{g}$ be a generator of $\mathbb{G}$. We look at the following PKE scheme for bits. The public key is $\mathsf{pk} = (\mathbf{g}, \mathbf{h} = \mathbf{g}^x)$, the secret key is $\mathsf{sk} = x$. In order to encypt a bit b the sender does the following:

case $b = 0$: Choose a uniform $y \in \mathbb{Z}_p$ and compute $c_1 := \mathbf{g}^y$ and $c_2 := \mathbf{h}^y$. Output the ciphertext (c_1, c_2).

case $b = 1$: Choose uniform $y, z \in \mathbb{Z}_p$ and compute $c_1 := \mathbf{g}^y$ and $c_2 := \mathbf{g}^z$. Output the ciphertext (c_1, c_2).

Prove that this encryption scheme is IND-CPA secure if **DDH** is hard in $\mathbb{G}$. Name two disadvantages of this scheme, compared to the standard ElGamal PKE.

Exercise 2. Consider the following signature schemes:

$\Sigma_1 = (\mathsf{KeyGen}_1, \mathsf{Sign}_1, \mathsf{Verify}_1)$ over a group $\mathbb{G}$ of prime order p with generator $\mathbf{g}$ works as follows:

KeyGen_1 sample $x \xleftarrow{\$} \mathbb{Z}_p$. Set $\mathsf{sk} = x$ and $\mathsf{pk} = \mathbf{g}^x$.

$\mathsf{Sign}_1(\mathsf{sk} = x, m)$ for a message $m \in \mathbb{Z}_p$ it computes $\sigma = x + m$ and outputs σ.

$\mathsf{Verify}_1(\mathsf{pk}, m, \sigma)$ outputs 1 iff $\mathbf{g}^m \cdot \mathsf{pk} = \mathbf{g}^\sigma$.

$\Sigma_2 = (\mathsf{KeyGen}_2, \mathsf{Sign}_2, \mathsf{Verify}_2)$ over a group $\mathbb{G}$ of prime order p with generator $\mathbf{g}$ works as follows:

KeyGen_2 sample $x \xleftarrow{\$} \mathbb{Z}_p$. Set $\mathsf{sk} = x$ and $\mathsf{pk} = \mathbf{g}^x$.

$\mathsf{Sign}_2(\mathsf{sk} = x, m)$ For a message $m = (m_1, m_2) \in \mathbb{G} \times \mathbb{G}$ computes $\sigma = m_1^{-x} \cdot m_2$ and outputs σ. We note that this corresponds to the decryption algorithm of ElGamal.

$\mathsf{Verify}_2(\mathsf{pk}, m, \sigma)$ outputs 1 iff $\mathsf{ElGamal.Enc}(\mathsf{pk}, \sigma) = m$.

Answer the following questions about the schemes:

(a) Is the scheme correct?

(b) If the scheme is correct, assuming that the discrete logarithm problem is hard in $\mathbb{G}$, is the scheme EUF-NMA secure?

(c) If the scheme is correct, assuming that the discrete logarithm problem is hard in $\mathbb{G}$, is it EUF-CMA secure?

Exercise 3. Given an IND-CCA secure PKE scheme E_0 construct:

(a) a PKE scheme E_1 that is IND-CPA secure but not IND-CCA1 secure

(b) a PKE scheme E_2 that is IND-CCA1 secure but not IND-CCA secure

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.