# Exercise Sheet 10

Prof. Kenny Paterson, F. Günther
M. Backendal, M. Filić

**Discussion Questions (Random Oracle Model).**

(a) In the lectures, you have seen schemes like DHIES and a simple RSA-based KEM that are secure in the so-called Random Oracle Model (ROM). In the ROM, we model a hash function $H$ as a random function which the adversary cannot compute itself, but has to query the challenger/reduction on some input $x$ in order to learn $H(x)$.

- Is this a realistic model for a hash function? Can a hash function be a random oracle?
- If it is not realistic, why do we use it?
- If it is realistic, can you think of an informal explanation of what a security proof in the ROM tells us?

---

**Suggested focus.** Attempt these problems

before class: Problem 3 (a) & (b), Problem 1 (a) & (b).
in class: Problem 1 (c), Problem 2, Problem 3 (c).

**Suggested reading.** Reading the following sections in the Boneh-Shoup book [1] might help with the problems on this exercise sheet: Section 10.3 (for RSA basics), Section 10.5 (for random self-reducibility), Section 11.3 (for IND-CPA security of PKE), Section 11.5 (for ElGamal encryption).

**Problem 1 (Random self-reducibility).** Let $\mathbb{G}$ be a cyclic group of prime order $q$ with a generator $g \in \mathbb{G}$. Consider the following two security games.

| Game $\mathbf{CDH}(\mathcal{A}, \mathbb{G})$ | Game $\mathbf{SquareDH}(\mathcal{B}, \mathbb{G})$ |
|---|---|
| $x, y \leftarrow\!\!\$\ \mathbb{Z}_q$ | $x \leftarrow\!\!\$\ \mathbb{Z}_q$ |
| $X \leftarrow g^x\ ;\ Y \leftarrow g^y$ | $X \leftarrow g^x$ |
| $Z \leftarrow\!\!\$\ \mathcal{A}(X, Y)$ | $Z \leftarrow\!\!\$\ \mathcal{B}(X)$ |
| Return $Z = g^{x \cdot y}$ | Return $Z = g^{x \cdot x}$ |

The left panel defines the **computational Diffie–Hellman (CDH) problem** (also presented in lectures) for $\mathbb{G}$ with $\mathcal{A}$'s advantage in solving CDH defined as

$$\mathbf{Adv}^{\mathrm{CDH}}_{\mathbb{G}}(\mathcal{A}) = \Pr\left[\,\text{Game } \mathbf{CDH}(\mathcal{A}, \mathbb{G}) \Rightarrow \mathsf{true}\,\right].$$

For the sake of this exercise, the right panel defines the less-common "square Diffie–Hellman problem" (SquareDH) with $\mathcal{B}$'s advantange

$$\mathbf{Adv}^{\mathrm{SquareDH}}_{\mathbb{G}}(\mathcal{B}) = \Pr\left[\,\text{Game } \mathbf{SquareDH}(\mathcal{B}, \mathbb{G}) \Rightarrow \mathsf{true}\,\right].$$

Let $\mathcal{A}$ be any adversary attacking the CDH problem (in group $\mathbb{G}$ as per above). Consider the following adversary $\mathcal{B}$ against the SquareDH problem:

Adversary $\mathcal{B}(X)$
$Z \leftarrow\!\!\$\ \mathcal{A}(X, X)$
Return $Z$

(a) Assume that $\mathbf{Adv}^{\mathrm{CDH}}_{\mathbb{G}}(\mathcal{A}) = 1$. Show that $\mathbf{Adv}^{\mathrm{SquareDH}}_{\mathbb{G}}(\mathcal{B}) = 1$.

(b) Build an *inefficient* adversary $\mathcal{A}$ such that $\mathbf{Adv}^{\mathrm{CDH}}_{\mathbb{G}}(\mathcal{A}) = 1 - \varepsilon$ for some "small" $\varepsilon$, but $\mathbf{Adv}^{\mathrm{SquareDH}}_{\mathbb{G}}(\mathcal{B}) = 0$.

(c) Part (b) illustrates that the "intuitive" reduction strategy of $\mathcal{B}$ above doesn't work in general, as the CDH adversary might not work if $X = Y$ (which, in the CDH problem, happens only with small probability).

Build a new adversary $\mathcal{B}'$ such that $\mathbf{Adv}^{\mathrm{SquareDH}}_{\mathbb{G}}(\mathcal{B}') \geq \mathbf{Adv}^{\mathrm{CDH}}_{\mathbb{G}}(\mathcal{A})$ is always true.

**Hint:** Consider how you might produce a *random* instance of the CDH problem from an instance of the SquareDH problem, so that $\mathcal{A}$ cannot check for $X = Y$ anymore.

**Problem 2 (IND-CPA security of ElGamal PKE).** Let $\mathbb{G}$ be a cyclic group of prime order $q$ with a generator $g \in \mathbb{G}$. For a given adversary $\mathcal{A}$, define the following game.

Game $\mathbf{DDH}(\mathcal{A}, \mathbb{G})$
$b \leftarrow\!\!\$\ \{0,1\}$
$x, y, z \leftarrow\!\!\$\ \mathbb{Z}_q$
$X \leftarrow g^x\ ;\ Y \leftarrow g^y$
if $b = 0$
  then $Z \leftarrow g^{xy}$
else $Z \leftarrow g^z$
$b' \leftarrow\!\!\$\ \mathcal{A}(X, Y, Z)$
Return $b = b'$

The game defines the **decisional Diffie–Hellman (DDH) problem** for $\mathbb{G}$ with $\mathcal{A}$'s advantage in solving DDH defined as

$$\mathbf{Adv}^{\mathrm{DDH}}_{\mathbb{G}}(\mathcal{A}) = 2 \cdot \left| \Pr\left[\,\text{Game } \mathbf{DDH}(\mathcal{A}, \mathbb{G}) \Rightarrow \mathsf{true}\,\right] - \frac{1}{2} \right|.$$

(You can think of the DDH problem as the decisional variant of the computational Diffie–Hellman problem you saw in Problem 1.)

Show that if the DDH assumption holds in the group $\mathbb{G}$, then the ElGamal PKE (as described in the lectures) when instantiated with $\mathbb{G}$ is IND-CPA secure. To be specific, show that the advantage of any adversary $\mathcal{A}$ in breaking the IND-CPA security of the ElGamal PKE (with a *single* encryption query) is bounded by the advantage of an adversary $\mathcal{B}$ against the DDH game above.

**Problem 3 (Anonymous PKE).** Suppose two people, Bob and Charlie, publish their public keys $pk_0$ resp. $pk_1$. Alice sends an encrypted message to one of them, say Bob, but she wants to ensure that no one (other than Bob and Charlie) can tell which of the two users is the intended recipient. (You may assume that decrypting Alice's message with a different secret key yields an error.)

(a) Define a security experiment and the corresponding adversarial advantage that captures this requirement. The adversary should be given public keys $pk_0, pk_1$ and it then chooses the message $m$ that Alice sends. Upon receiving a challenge ciphertext, the adversary should learn nothing about which of the two 'public' keys is the intended recipient. A system that has this property is said to be an *anonymous* public-key encryption scheme.

(b) Argue (at least informally) why the textbook RSA PKE (as described in the lectures) is not anonymous. You can assume that the public keys are generated using the same parameters, namely they have a common encryption exponent $e$ and a common bit-size $k$ of their respective moduli. You can also assume that $e$ is sufficiently small and the RSA moduli are sufficiently large.

(c) Let $\mathbb{G}$ be a cyclic group of prime order $q$ with a generator $g \in \mathbb{G}$. Show that the ElGamal PKE (as described in the lectures) when instantiated with the group $\mathbb{G}$ is (one-time) anonymous if the DDH assumption holds in $\mathbb{G}$. Towards this, state and prove a concrete security reduction in a similar vein as for Problem 2 above.

**Acknowledgements.** This exercise sheet is in part inspired by (and adapted from) problems by Simon Blackburn, Daniel Slamanig, and Mihir Bellare, as well as the book "A Graduate Course in Applied Cryptography" by Dan Boneh and Victor Shoup.

# References

[1] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography.* Online, version 0.6 edition, Jan. 2023.