Advanced Cryptography — Midterm Exam

Serge Vaudenay

27.4.2023

- duration: 1h45
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Computing Squares in Exponent Domain

We consider an algorithm $\mathsf{Setup}(1^s) \xrightarrow{\$} \mathsf{pp}$ based on a security parameter s which generates public parameters pp which include a group element g, the order q of g in the group (assumed to be an odd prime), and materials to be able to do group operations. We define the following three games.

Game CDH
1: $\mathsf{Setup}(1^s) \xrightarrow{\$} \mathsf{pp}$
2: pick $x, y \in \mathbf{Z}_q$
3: $X \leftarrow g^x$, $Y \leftarrow g^y$
4: $\mathcal{A}(\mathsf{pp}, X, Y) \xrightarrow{\$} K$
5: **return** $1_{K=g^{xy}}$

Game CDH^*
1: $\mathsf{Setup}(1^s) \xrightarrow{\$} \mathsf{pp}$
2: pick $x, y \in \mathbf{Z}_q^*$
3: $X \leftarrow g^x$, $Y \leftarrow g^y$
4: $\mathcal{A}(\mathsf{pp}, X, Y) \xrightarrow{\$} K$
5: **return** $1_{K=g^{xy}}$

Game Sqr
1: $\mathsf{Setup}(1^s) \xrightarrow{\$} \mathsf{pp}$
2: pick $x \in \mathbf{Z}_q$
3: $X \leftarrow g^x$
4: $\mathcal{A}(\mathsf{pp}, X) \xrightarrow{\$} Y$
5: **return** $1_{Y=g^{x^2}}$

The hardness of a game means that for any PPT algorithm $\mathcal{A}$, the probability that the game returns 1 is a negligible function of s.

Q.1 Prove that the hardness of any of those games imply that $E(\frac{1}{q})$ is a negligible function of s.
HINT: construct an adversary who wins with advantage $E(\frac{1}{q})$.

Q.2 Prove that the hardness of CDH and of CDH^* are equivalent.

Q.3 Prove that the hardness of Sqr implies the hardness of CDH.
HINT: be careful about distributions.

Q.4 Prove that the hardness of CDH implies the hardness of Sqr.
HINT: be careful about distributions.

2 Proof of DDH

We consider a PPT algorithm $\mathsf{Setup}(1^s) \xrightarrow{\$} \mathsf{pp} = (\ldots, g, q)$ based on a security parameter s which generates public parameters pp which include a group element g, the order q of g in the group (assumed to be prime), and materials to be able to do group operations. We consider the two following relations:

$$R((\mathsf{pp}, X, Y, K), y) : Y = g^y \wedge K = X^y$$
$$R'((\mathsf{pp}, X, Y, K), (x, y)) : X = g^x \wedge Y = g^y \wedge K = g^{xy}$$

Q.1 Construct a Σ-protocol for the relation R. Carefully specify all elements required in a Σ protocol.

Q.2 Construct a Σ-protocol for the relation R'. Carefully specify all elements required in a Σ protocol.