CS 395T: Topics in Cryptography **Spring 2024**

Exercise Set 1

Due: January 26, 2024 at 11:59pm (Submit on Gradescope) **Instructor:** David Wu

Instructions. You **must** typeset your solution in LaTeX using the provided template:

https://www.cs.utexas.edu/~dwu4/courses/sp24/static/homework.tex

You must submit your problem set via Gradescope (accessible through Canvas).

Collaboration Policy. You may discuss your general approach with other students, but you may not share written documents. You should not search online for solutions to these problems. If you do consult external sources, you must cite them in your submission. You must include the names of all of your collaborators with your submission. Refer to the official course policies for the full details.

Problem 1: Understanding Bilinearity [20 points]. Let $(\mathbb{G}, \mathbb{G}_T, e)$ be a symmetric *composite-order* pairing group of order $N = pq$ where p, q are primes (i.e., $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups with order N). Let g be a generator of $\mathbb{G}$. In this problem, we will explore some useful properties of composite-order bilinear maps. In all of the problems below, it is useful to recall that $\mathbb{G}$ is cyclic: for all $h \in \mathbb{G}$, there exists an $\alpha \in \mathbb{Z}_N$ such that $h = g^\alpha$.

(a) **Symmetry:** Show that the pairing is symmetric. Namely, for all $u, v \in \mathbb{G}$, $e(u, v) = e(v, u)$. (**Note:** this is also true for prime-order pairing groups.)

(b) **Bilinearity:** Show that for all $s, t, u, v \in \mathbb{G}$, it holds that $e(st, uv) = e(s, u)e(s, v)e(t, u)e(t, v)$. (**Note:** this is also true for prime-order pairing groups.)

(c) **Prime-order subgroup:** Recall that $\mathbb{G} = \{g^0, g^1, \ldots, g^{N-1}\}$. Let $\mathbb{G}_p \subset \mathbb{G}$ be a subgroup of $\mathbb{G}$ of order p and $\mathbb{G}_q \subset \mathbb{G}$ be a subgroup of order q. Let $g_p := g^{\alpha_p}$ be a generator of $\mathbb{G}_p$ and $g_q := g^{\alpha_q}$ be a generator of $\mathbb{G}_q$. What is (one possible) value for α_p, α_q in terms of N, p, q?

(d) **Orthogonality:** Suppose $u \in \mathbb{G}_p$ and $v \in \mathbb{G}_q$. Show that $e(u, v) = 1$. Here, "1" denotes the identity element in $\mathbb{G}_T$.

(e) **Projection:** Show that $e(g_p, g^\alpha) = e(g_p, g)^{\alpha \bmod p}$. Namely, pairing with g_p "projects" the exponent α into its mod p subgroup.

We will see many applications of these properties later in this course. **Note:** Each of the properties above can be shown by a 1-2 line calculation.

Challenge Problem: Tight Reduction for BLS [Optional]. In our security proof for BLS signatures, we showed that for every signature adversary $\mathcal{A}$, there exists a CDH adversary $\mathcal{B}$ such that

$$\mathsf{SigAdv}[\mathcal{A}] \leq \mathrm{poly}(Q) \cdot \mathsf{CDHAdv}[\mathcal{B}],$$

where Q is the number of queries algorithm $\mathcal{A}$ makes in the security game. We refer to the $\mathrm{poly}(Q)$ term as the "security loss" in the reduction. Namely, an adversary that breaks the signature scheme with advantage ε implies one that breaks CDH with a much *smaller* advantage $\varepsilon/\mathrm{poly}(Q)$. Show how to modify the BLS signature scheme to have a *randomized* signing algorithm which allows for a *tight* reduction to CDH. Namely, for every signature adversary $\mathcal{A}$ for your revised scheme, there exists a CDH adversary $\mathcal{B}$ such that

$$\mathsf{SigAdv}[\mathcal{A}] \leq O(1) \cdot \mathsf{CDHAdv}[\mathcal{B}].$$

Hint: Consider a variant of BLS where there are two valid signatures for each message.

Optional Feedback. Please answer the following *optional* questions to help design future exercise sets. You do not need to answer these questions. However, we do encourage you to provide us feedback on how to improve the course experience.

(a) How long did you spend on this exercise set?

(b) Do you have any feedback for this exercise set?

(c) Do you have any feedback on the course so far?

(d) Are there specific topics that you are interested in seeing in this course?