

Problem Set 5

Instructions: You **must** typeset your solution in LaTeX using the provided template. Please submit your problem set via Gradescope. Include your name and the names of any collaborators at the top of your submission.

Problem 1: Pairing Conceptual Questions [6 points]. For each of the following statements, say whether it is TRUE or FALSE and briefly explain why.

- (a) Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a pairing for an elliptic curve group \mathbb{G} . If the discrete log problem in \mathbb{G} is easy, then the BDDH problem for e is easy as well.
- (b) Let $\mathbb{G} = \langle g \rangle$ be a group of prime order q , and suppose there exists a pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ of the sort we use to instantiate BLS signatures. Then, the group \mathbb{G} is safe to use for standard two-party Diffie-Hellman key agreement:

That is, Alice sends $g^a \in \mathbb{G}$ for $a \stackrel{\text{R}}{\leftarrow} \mathbb{Z}_q$, Bob sends $g^b \in \mathbb{G}$ for $b \stackrel{\text{R}}{\leftarrow} \mathbb{Z}_q$, and Alice and Bob use $H(g^{ab})$ as their shared secret, where $H : \mathbb{G} \rightarrow \mathbb{G}$ is a hash function that we model as a random oracle.

Problem 2: Asymmetric Pairings [10 points]. All the pairing-based schemes we saw in class used *symmetric* pairings $e : \mathbb{G} \times \mathbb{G} \rightarrow G_T$, but in practice we often use *asymmetric* pairings. These are pairings of the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow G_T$ where \mathbb{G}_1 and \mathbb{G}_2 are different groups. Let $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ be generators of these groups.

- (a) Describe the BLS signature scheme in a setting that uses asymmetric pairings. You may assume you have access to a hash function $H : \{0, 1\}^* \rightarrow \mathbb{G}_1$ modeled as a random oracle. Be sure to specify which group each element used belongs to.
Note: This will require almost no changes to the protocol.
- (b) Give a version of the pairing-based three-party key exchange protocol from lecture that works using asymmetric pairings.
Note: This will require some changes to the protocol.

Problem 3: Regev Encryption [10 points]. For this question, consider the Regev encryption scheme covered in class.

- (a) The Regev encryption shown in class only supported encryption of ciphertexts $\{0, 1\}$. Show how to extend this to $\{0, \dots, 15\}$. The same principle should apply for any sufficiently small domain.
- (b) Show that this scheme is additively homomorphic. Mention any changes needed to make it additively homomorphic, if needed.

Problem 4: OT/2PC Conceptual Questions [12 points].

- (a) For each of the following statements, say whether it is TRUE or FALSE. Write *at most one sentence* to justify your answer.
- i) In Yao's protocol for secure two-party computation of a function $f(\cdot, \cdot)$ (as described in lecture), the two parties must exchange a number of bits that is at least as large as a Boolean circuit computing f .
 - ii) Say that Alice, with input $x \in \{0, 1\}$, and Bob, with input $y \in \{0, 1\}$, use Yao's protocol to compute $f(x, y) \in \{0, 1\}$, for some function $f : \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$. Then, under reasonable computational assumptions, the protocol must hide y from Alice—that is, Alice's probability of guessing Bob's bit after running the protocol is at most $1/2 + \text{negl}(\lambda)$ for all functions $f : \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$ and a security parameter λ .
- (b) List the computational assumptions needed to prove the security of the Yao's garbled circuits scheme we saw in class and briefly state why each one is necessary.

Optional Feedback [5 points]. Please answer the following questions to help design future problem sets. You are not required to answer these questions (the points are free), and if you would prefer to answer anonymously, please use the anonymous feedback form. However, we do encourage you to provide feedback on how to improve the course experience.

- (a) Roughly how long did you spend on this problem set?
- (b) What was your favorite problem on this problem set?
- (c) What was your least favorite problem on this problem set?
- (d) Any other feedback for this problem set? Was it too easy/difficult?
- (e) Any other feedback on the course so far?