End Semester - Fall, 2023
M. Tech. Cryptology & Security
Advanced Cryptology

November 30, 2023

Maximum Marks: 50
Maximum Time: 3.5 hr (strict)
Open note/book Exam

Instructions

- Maximum marks is 50. Total marks provided in the paper: 65.
- Be short and precise. Partial marking will be provided for a partially correct answer/attempt.
- You can use any book/notes during the exam, but *not internet*.
- You must comply with the rules and regulations (including the provided seating arrangements) of ISI.

Notations. The set of all integers are denoted by $\mathbb{Z}$ and all natural numbers as $\mathbb{N}$. The ring of all integers modulo n is denoted by $\mathbb{Z}_n$. Below $\kappa \in \mathbb{N}$ denotes the security parameter throughout (for example, if 128 bit security is desired from the system, then κ is set to 128, this is often equal to the key-length). A uniform random sample from a domain D is denoted as $s \leftarrow_{\$} D$. We assume $\mathbb{G}$ to be a cyclic group of prime order p. Let g be a generator of the group.

1. Let $(\mathsf{KGEN}, \mathsf{ENC}, \mathsf{DEC})$ be a PKE scheme.

   Consider the following algorithms:

   - $\mathsf{ADD}(c_1, c_2)$ which takes two ciphertexts as input and outputs the pair (c_1, c_2).
   - MUL which is the same as ADD.
   - $\mathsf{DEC}'_{\mathsf{sk}}(c_1, c_2, f)$ which runs $m_1 := \mathsf{DEC}_{\mathsf{sk}}(c_1)$ and $m_2 := \mathsf{DEC}_{\mathsf{sk}}(c_2)$ and output $f(m_1, m_2)$ for any function f.

   Is $(\mathsf{KGEN}, \mathsf{ENC}, \mathsf{DEC}')$, equipped with ADD and MUL procedures, a fully homomorphic encryption? Provide arguments for your answer.

   (5)

2. Given an FHE scheme $(\mathsf{KGEN}, \mathsf{ENC}, \mathsf{DEC})$:

   (a) Design a two-party protocol to compute any function f.

   (b) Prove that the protocol is secure against semi-honest corruption.

   (c) If the FHE scheme is lattice-based, and the function f has high multiplicative depth, that is you need to do many sequential multiplications, then what technique you might need? Describe the technique in detail. In that case what additional security assumption (beyond lattice-based assumptions) would be needed?

   (5+7+8 = 20)

3. Consider four parties P_1, P_2, P_3, P_4. If I want to construct a 3 out of 4 secret sharing scheme, then any three parties can reconstruct the secret. But I want a slightly different access structure, where parties have different weights: P_i has weight $w_i \in \mathbb{N}$ and so on. The threshold weight to recover secret would be W. That means parties $\{P_i\}_{i \in I}$ would only reconstruct if $\sum_{i \in I} w_i \geq W$ and has no information if $\sum_{i \in I} w_i < W$. For example, the weights can be $P_1 \leftarrow 3$, $P_2 \leftarrow 1$, $P_3 \leftarrow 2$, $P_4 \leftarrow 1$ and threshold $W = 4$. In this case parties P_1, P_2 can recover the secret as their total weight is 4, but P_2, P_3 can not, as their total weight is 3, but P_2, P_3, P_4 can jointly recover as their total weight is $1 + 2 + 1 = 4$. Construct a (weighted) threshold secret sharing schemes for the four parties with the weights given above. (The scheme should be easily extended to any n parties, but it is ok to just describe one with respect to the specific example given).

(10)

4. Recall the definition of message authentication code: it consists of three algorithms (i) KGEN; (ii) MAC and (iii) Verify, such that $\mathsf{KGEN}(1^\kappa)$ outputs a secret key sk, and for any message m we have that: $\mathsf{Verify}(\mathsf{sk}, m, \mathsf{MAC}_{\mathsf{sk}}(m)) = 1$. Furthermore, no PPT adversary can forge a tag τ for any given message m without having sk, such that $\mathsf{Verify}_{\mathsf{sk}}(\mathsf{sk}, m, \tau) = 1$ except with a negligible probability in the security parameter.

   (a) Describe a security game for a (n, t)-threshold MAC

   (b) Propose a design for (n, t)-threshold MAC

   (c) Prove that design is secure with respect to the proposed definition.

   Hint: think about threshold BLS.

(5+7+8 = 20)

5. Consider the following arithmetic circuit over $\mathbb{Z}_p$ for a prime p. Consider three parties P_1, P_2, P_3 such that each party P_i has input x_i. What MPC protocol would you use if at most 1 party is corrupt by an adversary with unlimited computational power? Write each step of the protocol for this particular circuit.

(2+8 = 10)