

Assignment 6 (Tutorial)

Instructor: Sruthi Sekar

TAs: Lakshya Gadhwal, Ravi B Prakash

Problem 1: Hybrid Argument

(Single-bit to Multi-bit Encryption). Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be an IND-CPA secure PKE for $\mathcal{M} = \{0, 1\}$ (single-bit). Define $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ for $\mathcal{M}' = \{0, 1\}^\ell$ (multi-bit):

- $\text{Gen}'(1^n)$: $(pk, sk) \leftarrow \text{Gen}(1^n)$. Output (pk, sk) .
- $\text{Enc}'(pk, m)$: For $m = m_1 || m_2 || \dots || m_\ell$, with $m_i \in \{0, 1\}$ for each i :
Output $c = (\text{Enc}(pk, m_1) || \text{Enc}(pk, m_2) || \dots || \text{Enc}(pk, m_\ell))$.
- $\text{Dec}'(sk, c)$: For $c = c_1 || c_2 || \dots || c_\ell$, compute $m'_i = \text{Dec}(sk, c_i)$ for all $i \in [\ell]$.
Output $m' = (m'_1 || \dots || m'_\ell)$.

Show that Π' is IND-CPA secure PKE for $\mathcal{M}'$.

Problem 2: Digital Signatures

(Randomized $\rightarrow$ Deterministic). Given an EU-CMA secure digital signature with a randomized signing $\Pi^R = (\text{Gen}^R, \text{Sign}^R, \text{Vrfy}^R)$, i.e., Sign^R takes some randomness $r \in \{0, 1\}^n$ to generate: $\sigma := \text{Sign}^R(sk, m; r)$. Let $F := \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a pseudorandom function. Define a deterministic digital signature scheme $\Pi^D = (\text{Gen}^D, \text{Sign}^D, \text{Vrfy}^D)$ using Π^R and F as follows:

- $\text{Gen}^D(1^n)$: $(pk, sk) \leftarrow \text{Gen}^R(1^n)$, $k \in_R \{0, 1\}^n$. Output $(pk' = pk, sk' = (sk, k))$.
- $\text{Sign}^D(sk', m)$: Given $sk' = (k, sk)$, compute $r = f_k(m)$ and output $\sigma := \text{Sign}^R(sk, m; r)$.
- $\text{Vrfy}^D(pk, m, \sigma)$: output the bit output by $\text{Vrfy}^R(pk, m, \sigma)$.

Prove that Π^D is EU-CMA secure.

Problem 3: Attack or not?

- Order-preserving Encryptions.** The attempt is to look at the possibility of a PKE where the ciphertexts follow the same lexicographic order as the messages. This property would be useful for computing on encrypted databases. Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a public key encryption for $\mathcal{M}$ such that: for each $m_1, m_2 \in \mathcal{M}$, if $m_1 \leq m_2$, then $\text{Enc}(pk, m_1) \leq \text{Enc}(pk, m_2)$, where $(pk, sk) \leftarrow \text{Gen}(1^n)$. Is such a Π IND-CPA secure?
- Committed or not?** Define a commitment scheme $\Pi^{\text{com}} = (\text{Commit}, \text{Receive})$ using a length-tripling PRG G as follows:

- $\text{Commit}(1^n, b; r)$: For random $r \in \{0, 1\}^n$ and bit b output

$$\text{com} := \begin{cases} G(r), & \text{if } b = 0 \\ G(r) \oplus 1^{3n}, & \text{if } b = 1 \end{cases}$$

- **Receive**(com, b, r) : If com = $G(r)$, set $b' = 0$, else if com = $G(r) \oplus 1^{3n}$, set $b' = 1$.
Output 1 iff $b' = b$.

Is Π^{com} computational hiding and perfect binding? If not perfect binding, is it computational binding?

Problem 4: ZKP from FHE

Recall that FHE is a PKE $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ equipped with an additional public evaluation algorithm **Eval** with the syntax: on input ciphertext c corresponding to a message m under some public key pk and a function f , it outputs $c' \leftarrow \text{Eval}(pk, c, f)$. Now, consider an interactive protocol $\Pi^{IP} = (P, V)$ based on FHE $\Pi = (\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$ described below. The prover P and verifier V share an instance $x \in L$ for an NP language L with corresponding relation $\mathcal{R}$ ($x \in L$ iff $\exists w: (x, w) \in \mathcal{R}$). Prove that Π^{IP} is a computational honest verifier ZKP for L .

- i) P computes a witness w for x .
- ii) P samples a key pair $(pk, sk) \leftarrow \text{Gen}(1^{|x|})$ and sends $c \leftarrow \text{Enc}(pk, w)$ to V .
- iii) V tosses $b \in_R \{0, 1\}$ and sends c' to P , where
 - if $b = 1$, $c' \leftarrow \text{Eval}(pk, c, C_{\mathcal{R}}(x, \cdot))$
(Here, $C_{\mathcal{R}}(x, w)$ outputs 1 if $(x, w) \in \mathcal{R}$ and 0, otherwise.)
 - if $b = 0$, $c' \leftarrow \text{Enc}(pk, 0)$
- iv) P decrypts $b' = \text{Dec}(sk, c')$ and sends b' to V .
- v) V accepts if and only if $b' = b$.

Problem 5: PQC: Understanding LWE

- a) Recall the (n, m, q, χ) -DLWE assumption from [Lec 22](#): for all quantum polynomial **Evelyn**, $\exists$ negligible negl s.t. for all n :

$$\left| \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ \mathbf{s} \in_R \mathbb{Z}_q^n, \mathbf{e} \leftarrow \chi^m}} [\text{Evelyn}(A, A\mathbf{s} + \mathbf{e}) = 1] - \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ \mathbf{r} \in_R \mathbb{Z}_q^m}} [\text{Evelyn}(A, \mathbf{r}) = 1] \right| \leq \text{negl}(n)$$

Now, consider the *worst-case* (for secrets $\mathbf{s}$) version of this assumption denoted by (n, m, q, χ) -DLWE': for all quantum polynomial **Evelyn** and all $\mathbf{s} \in \mathbb{Z}_q^n$, $\exists$ negligible negl s.t. for all n :

$$\left| \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ \mathbf{e} \leftarrow \chi^m}} [\text{Evelyn}(A, A\mathbf{s} + \mathbf{e}) = 1] - \Pr_{\substack{A \in_R \mathbb{Z}_q^{m \times n} \\ \mathbf{r} \in_R \mathbb{Z}_q^m}} [\text{Evelyn}(A, \mathbf{r}) = 1] \right| \leq \text{negl}(n)$$

Show that (n, m, q, χ) -DLWE' $\implies$ (n, m, q, χ) -DLWE. (**Hint:** Exploit linearity).

- b) Consider the short integer solution (SIS) problem:

- **Input:** $A \leftarrow \mathbb{Z}_q^{n \times m}$, with $m \geq \lceil n \log p \rceil$.
- **Solution:** non-zero vector $\mathbf{x} \in \{0, \pm 1\}^m$ in A 's kernel, i.e. $A\mathbf{x} = 0 \pmod q$.

A solution is guaranteed to exist. Why? Show that a (n, m, q) -SIS-solver will give an (n, m, q, χ) -LWE-solver.