Modern Complexity Theory (CS1.405)

End Semester Examination (Monsoon 2025)

International Institute of Information Technology, Hyderabad

Time: 3 hours Total Marks: 60

Instructions: This is a closed book and notes examination.
Regular calculator is allowed.
NO query in examination hall is allowed.

Group A

Answer *ANY FOUR* questions from this group.

1. (a) Show that if $NP = P^{SAT}$, then NP = coNP.

   (b) A linear bounded automaton (LBA) is a one-tape one-head non-deterministic Turing machine (TM) with the tape finite and just big enough to hold the entire input. If an LBA tries to move its head outside its tape at either end, some mechanism prevents it from doing so, and the head remains in the old position. Define the following language:

   $$A_{LBA} := \{\langle M, \alpha\rangle | \text{the LBA } M \text{ accepts } \alpha\}.$$

   Prove that A_{LBA} is PSPACE-complete.

   [4 + 6 = 10]

2. (a) Define the class: EXPSPACE-complete. Let $\uparrow$ represent the exponentiation operation. If R is a regular expression and k is a non-negative integer, $R \uparrow k$ is equivalent to the concatenation of R with itself k times. In other words,

   $$R^k = R \uparrow k = R \circ R \circ \cdots R \,(k \text{ times}).$$

   Let $EQ_{REX\uparrow} = \{\langle Q, R\rangle | Q \text{ and } R \text{ are equivalent regular expressions with exponentiation}\}$.

   Prove that $EQ_{REX\uparrow}$ is in EXPSPACE.

   (b) Define the classes: ZPP, RP and coRP. Prove that ZPP = RP $\cap$ coRP.

   [5 + 5 = 10]

3. (a) Let

   $$\text{BOTH\_NFA} = \{\langle M_1, M_2\rangle \mid M_1 \text{ and } M_2 \text{ are NFAs and } L(M_1) \cap L(M_2) \neq \varnothing\}.$$

   Show that BOTH_NFA is NL-complete.

   (b) Define the class: BQP. Explain the Shor's algorithm for integer factorization. Prove that this algorithm belongs to BQP.

   [5 + 5 = 10]

4. **(a) Define the generalized geography game (GG) as follows:** $GG := \{\langle G, b\rangle |$ Player I has a winning strategy for the generalized geography game played on a directed graph G starting at node $b\}$. Prove that GG is PSPACE-hard.

(b) Prove or disprove that the intersection of two NL-complete languages (over the same alphabet) is also NL-complete.

[6 + 4 = 10]

5. (a) State the time hierarchy theorem. Use it to prove that P $\subset$ EXPTIME.

(b) Explain the RSA public key encryption algorithm and its connection in security with the integer factorization problem (IFP).

[5 + 5 = 10]

6. **(a)** Explain the Pollard $p - 1$ factorization method for factoring a composite integer n into prime factors. What is the time complexity of this algorithm.

(b) The ***circuit-satisfiable*** problem tests whether a circuit is satisfiable. Define the following language:

$$\text{CIRCUIT-SAT} := \{\langle C\rangle | C \text{ is a satisfiable Boolean circuit}\}.$$

Prove that CIRCUIT-SAT is NP-complete.

[5 + 5 = 10]

Group B

Answer *ALL* questions from this group.

7. **(a)** In a lattice, we require a basis. Show that the set of vectors $\{(1, 2, 1), (2, 1, 0), (1, -1, 2)\}$ form a basis of the vector space V_3 over the field of real numbers.

(b) Define the following hard problems in lattice-based cryptography:

- Shortest Vector Problem (SVP)
- Closest Vector Problem (CVP)
- Learning With Errors (LWE) Problem

Prove that SVP $\leq_p$ LWE.

[5 + 5 = 10]

8. Consider the following case study: "Post-Quantum Secure Lattice-Based Authentication Scheme for IoT-Enabled Contactless Smart Payments" that was discussed in the class:

Abhishek Kumar Pandey, Prithwi Bagchi, Debnath Ghosh, Ashok Kumar Das, Ravi Kumar Kappagantu, Srinivas V Katakam, and Jitendra Chougala. "Post-Quantum Secure Lattice-Based Authentication Scheme for IoT-Enabled Contactless Smart Payments," in *7th IEEE Computers, Communications and IT Applications Conference (ComComAp 2025)*, 14-17 December 2025, Madrid, Spain.

With respect to this case study, answer the following questions:

(a) Explain briefly with a diagram for the NFC-enabled IoT-based wearable secure payment architecture.

(b) The following are the phases used in this case study:

System Initialization Phase: This phase is executed by the CA in an offline mode as follows.

• CA selects a security parameter $n \in \mathbb{Z}$ such that $n = 2^{\alpha}$ for some $\alpha > 0$, a polynomial ring $R_q = \frac{\mathbb{Z}_q[x]}{\langle x^n+1 \rangle}$, and also a discrete Gaussian distribution χ_σ, where σ denotes the standard deviation with $q > 16\sigma^2.n^{3/2}$.

• The CA generates its own long-term lattice-based private and public keys as follows. It first selects random polynomial $s \in_R R_q$, the private key as $pr_{CA} = (pr_{CA,1}, pr_{CA,2}) \in_R \chi_\sigma \times \chi_\sigma$, and then calculates the respective public key as $Pub_{CA} = s \cdot pr_{CA,1} + 2.pr_{CA,2} \pmod{x^n + 1}$. Additionally, the CA picks a cryptographically secure and quantum-resistant hash function $H(\cdot)$ (e.g., "National Institute of Standards and Technology (NIST)" recommended "Secure Hash Algorithm (SHA-256) which outputs 256-bit message digest").

• CA finally publishes the public parameters $pp = \{q, n, R_q, s, Pub_{CA}, H(\cdot)\}$, while keeping the private key $pr_{CA} = (pr_{CA,1}, pr_{CA,2})$ as secret.

Registration Phase: The certificate authority CA is responsible for registering the wearable device WD_i of a user U_i, and other entities in the payment network, including the issuing bank, payment gateway, and acquirer bank.

Wearable Devices Enrollment: The steps are essential to perform the enrollment of each wearable device, say WD_i, associated with the user U_i:

Step 1. The user U_i selects an identity ID_{U_i}, generates a random 6-digit PIN PIN_{U_i}, a random nonce $r_{U_i} \in \mathbb{Z}_q$ and imprints his/her personal biometrics (for instance, it can be fingerprint) BIO_{U_i} at a specific terminal. U_i computes $(bk_{U_i}, ph_{U_i}) = Gen(BIO_{U_i})$ using the fuzzy extractor $Gen(\cdot)$ function, where bk_{U_i} and ph_{U_i} denote the biometric secret key of length l bits and public helper data (production parameter), respectively, and then sends the registration information $\langle ID_{U_i}, H(PIN_{U_i}||bk_{U_i}) \oplus r_{U_i} \rangle$ to the CA securely.

Step 2. The CA generates the pseudo-identity of U_i as $PID_{U_i} = H(ID_{U_i} ||pr_{CA,1}|| pr_{CA,2})$ and $X_{U_i} = H(pr_{CA,1}|| pr_{CA,2} ||RTS_{U_i}) \oplus H(PIN_{U_i}||bk_{U_i}) \oplus r_{U_i}$, where the registration timestamp for U_i is represented by RTS_{U_i}. It then sends the information $\langle PID_{U_i}, X_{U_i} \rangle$ to U_i securely.

Step 3. U_i computes the masked PID as $PID^*_{U_i} = PID_{U_i} \oplus H(bk_{U_i}||ID_{U_i}||PIN_{U_i})$. U_i then generates private and public key pairs as $pr_{U_i} = (pr_{U_i,1}, pr_{U_i,2}) \in_R \chi_\sigma \times \chi_\sigma$ and $Pub_{U_i} = s \cdot pr_{U_i,1} + 2.pr_{U_i,2} \pmod{x^n + 1}$, and calculates $pr^*_{U_i,1} = pr_{U_i,1} \oplus H(PID_{U_i}||PIN_{U_i}||bk_{U_i})$, $pr^*_{U_i,2} = pr_{U_i,2} \oplus H(PIN_{U_i}||bk_{U_i}||PID_{U_i})$, $X^*_{U_i} = X_{U_i} \oplus r_{U_i} = H(pr_{CA,1}|| pr_{CA,2} ||RTS_{U_i}) \oplus H(PIN_{U_i}||bk_{U_i})$, and $Y_{U_i} = H(PID_{U_i} ||bk_{U_i} ||PIN_{U_i} ||pr_{U_i,1} ||pr_{U_i,2} ||X^*_{U_i})$.

Finally, U_i stores the credentials $\langle PID^*_{U_i}, pr^*_{U_i,1}, pr^*_{U_i,2}, X^*_{U_i}, pp \rangle$, and publishes the public key Pub_{U_i} as public.

POS Terminal Registration: The POS terminal is registered and issued by the respective bank. The information stored in POS terminal by the bank includes: i) merchant information, such as "Merchant ID", "Terminal ID", "Merchant category code", "Store/branch identifiers"; ii) Bank/Acquirer information, such as "Acquirer institution ID", "Bank host communication details (IP/domain, port number, or dial-up numbers for legacy terminals)" and "Settlement bank account details (for routing funds)"; iii) Cryptographic and security credentials, such as "initial lattice-based encryption keys", "lattice-based certificates for secure authentication" and 'key exchange parameters"; iv) Transaction parameters, like "supported card schemes/networks (Visa, Mastercard, RuPay, etc.)", "transaction limits", and "currency codes and country codes"; v) Configuration and software parameters.

After POS terminal registration, the bank generates its own private and public key pair as $pr_{POS} = (pr_{POS,1}, pr_{POS,2}) \in_R \chi_\sigma \times \chi_\sigma$ and $Pub_{POS} = s \cdot pr_{POS,1} + 2.pr_{POS,2} \pmod{x^n + 1}$, and then stores the private key while publishes its public key.

Similarly, the registration of other entities, like the issuing bank, payment gateway, and acquirer bank, is done by the CA, where the lattice-based certificates issued to them are generated by the

CA's private key $pr_{CA} = (pr_{CA,1}, pr_{CA,2})$.

Login and Authentication Phase: This phase discusses how a registered user can securely perform contactless payment at a particular POS terminal. The following steps are important to perform such a secure payment:

Step 1. At first, the registered user U_i keeps his/her wearable device WD_i within the NFC communication range of a particular POS terminal (e.g., a counter in a shopping mall), and inputs his/her identity ID_{U_i}, PIN PIN_{U_i}, and imprints biometrics template BIO'_{U_i} at the sensor of WD_i. WD_i then calculates the following: $Rep(BIO'_{U_i}, ph_{U_i}) = bk_{U_i}$, $PID_{U_i} = PID^*_{U_i} \oplus H(bk_{U_i} || ID_{U_i} || PIN_{U_i})$, $pr_{U_i,1} = pr^*_{U_i,1} \oplus H(PID_{U_i} || PIN_{U_i} || bk_{U_i})$, $pr_{U_i,2} = pr^*_{U_i,2} \oplus H(PIN_{U_i} || bk_{U_i} || PID_{U_i})$, $A_i = X^*_{U_i} \oplus H(PIN_{U_i} || bk_{U_i})$, and $Y'_{U_i} = H(PID_{U_i} || bk_{U_i} || PIN_{U_i} || pr_{U_i,1} || pr_{U_i,2} || X^*_{U_i})$. If $Y'_{U_i} = Y_{U_i}$, the user U_i is authenticated by the wearable device WD_i. Otherwise, the payment process is terminated.

Step 2. WD_i now generates random secrets $(pr_{WD,1}, pr_{WD,2}) \in_R \chi_\sigma \times \chi_\sigma$ and calculates the corresponding public value as $RPub_{WD} = s \cdot pr_{WD,1} + 2.pr_{WD,2} \pmod{x^n + 1}$, $B_i = H(A_i || bk_{U_i} || PIN_{U_i} || TS1) \oplus H(\eta_{wp} || PID_{U_i} || RPub_{WD} || TS1)$, where $TS1$ is the current timestamp, $\triangle_{wp} = Cha(\psi_{wp})$, $\psi_{wp} = pr_{U_i,1} \cdot Pub_{POS}$ and $\eta_{wp} = Mod_2(\psi_{wp}, \triangle_{wp})$, and $Ver_i = H(B_i || TS1 || RPub_{WD} || \eta_{wp} || PID_{U_i})$, and sends the message $MSG1 = \langle PID_{U_i}, TS1, B_i, RPub_{WD}, Ver_i \rangle$ to the targeted POS terminal via NFC channel.

Step 3. If the message $MSG1$ is received at time $TS1'$, the validity of the timestamp $TS1$ is done by the POS terminal with the condition: $|TS1' - TS1| < \Delta T$, where ΔT denotes the "maximum allowable delay for a message". If the message is fresh, the POS terminal calculates $\triangle_{pw} = Cha(\psi_{pw})$, $\psi_{pw} = pr_{POS,1} \cdot Pub_{U_i}$, $\eta_{pw} = Mod_2(\psi_{pw}, \triangle_{pw})$, and $Ver'_i = H(B_i || TS1 || RPub_{WD} || \eta_{pw} || PID_{U_i})$, and then verifies if $Ver'_i = Ver_i$ holds or not. If the condition is valid, the message is treated as an authentic one. The POS terminal generates the current timestamp $TS2$, random secrets $(r_{POS,1}, r_{POS,2}) \in_R \chi_\sigma \times \chi_\sigma$ and calculates the corresponding public value as $RPub_{POS} = s \cdot r_{POS,1} + 2.r_{POS,2} \pmod{x^n + 1}$, $C_i = H(A_i || bk_{U_i} || PIN_{U_i} || TS1) = B_i \oplus H(\eta_{pw} || PID_{U_i} || RPub_{WD} || TS1)$, $r\triangle_{pw} = Cha(r\psi_{pw})$, $r\psi_{pw} = r_{POS,1} \cdot RPub_{WD}$, $r\eta_{pw} = Mod_2(r\psi_{pw}, r\triangle_{pw})$, the session key shared with U_i's WD_i as $sk_{pw} = H(\eta_{pw} || r\eta_{pw} || PID_{U_i} || TS1 || TS2 || C_i)$ and its verifier as $skv_{pw} = H(sk_{pw} || TS2)$. The POS terminal sends the message $MSG2 = \langle RPub_{POS}, TS2, skv_{pw} \rangle$ to WD_i via NFC channel.

Step 4. After the freshness check of the message $MSG2$, WD_i proceeds to calculate $r\psi_{wp} = pr_{WD,1} \cdot RPub_{POS}$, $r\triangle_{wp} = Cha(r\psi_{wp})$, $r\eta_{wp} = Mod_2(r\psi_{wp}, r\triangle_{wp})$, the session key shared with the POS terminal as $sk_{wp} = H(\eta_{wp} || r\eta_{wp} || PID_{U_i} || TS1 || TS2 || H(A_i || bk_{U_i} || PIN_{U_i} || TS1))$ and its verifier as $skv_{wp} = H(sk_{wp} || TS2)$. If the verification condition: $skv_{wp} = skv_{pw}$ is satisfied, both WD_i and POS terminal share the same (common) session key sk_{wp} $(= sk_{pw})$ for their secure payment.

(i) Prove the correctness of the session key establishment during the *Login and Authentication Phase*.

(ii) Explain how the Ring-LWE lattice hard problem is associated with this scheme in post-quantum security point of view.

[5 + 5 = 10]

********** **End of Question Paper** **********