Dept. of Computer Science and Engineering, National Sun Yat-sen Univ.

Second Semester of 2022 PhD Qualifying Exam

Subject: Cryptography

Problem 1: (10 points) Please define formally the security of pseudorandom function.

Problem 2: (10 points) Please describe how a man-in-the-middle attack in Diffie-Hellman key agreement protocol is practiced and how to prevent from such attack. (Note: Need to describe the design of a protocol by using an existing cryptosystem in detail.)

Problem 3: (10 points) Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem. Then $H(\mathbb{K}|\mathbb{C}) = H(\mathbb{K}) + H(\mathbb{P}) - H(\mathbb{C})$.

Problem 4: (10 points) Prove that $H(X, Y) = H(Y) + H(X|Y)$. Then show as a corollary that $H(X|Y) \leq H(X)$, with equality if and only if X and Y are independent.

Problem 5: (10 points) Please define anonymity (unlinkability) for mutual authentication formally.

Problem 6: (10 points) Please define semantic security for attribute-based encryption formally.

Problem 7: (15 points) Please design a user anonymous authenticated key exchange protocol for two entities, where both entities have to authenticate each other mutually and public-key cryptosystem is allowed to be utilized. (Notes: please also specify clearly what kind of security has to be achieved for the used cryptosystem in the proposed protocol.)

Problem 8: (10 points) Please define the basic security features of a group signature scheme, i.e., unforgeability, anonymity and traceability.

Problem 9: (15 points) Suppose there are three entities A, B, and C, and they are untrusted to each other. Moreover, A and C, and B and C, share common secret keys, K_{AC} and K_{BC}, respec-

tively. Please design a three-party authenticated key exchange protocol with forward secrecy using only symmetry-based encryption, cryptographic hash function, and Diffie-Hellman key agreement. (Note: The security feature of mutual authentication, session key exchange, and forward secrecy should be achieved among A and B).