MAMME FME **Codes and Cryptology**

Cryptography Part

Exam 23 December 2015

Choose three of the four exercises.

1. Consider the function families $\mathcal{F} = \{f_k : \mathcal{X}_k \to \mathcal{Y}_k\}_{k\in\mathcal{K}}$, $\mathcal{G} = \{g_k : \mathcal{X}_k \to \mathcal{Z}_k\}_{k\in\mathcal{K}}$ and $\mathcal{H} = \{h_k : \mathcal{X}_k \to \mathcal{Y}_k \times \mathcal{Z}_k\}_{k\in\mathcal{K}}$, where $h_k(x) = (f_k(x), g_k(x))$. Show whether the following implications are true or false (by giving either a reduction or a counterexample):

   (a) $\mathcal{H}$ is one-way implies $\mathcal{F}$ is also one-way.

   (b) $\mathcal{F}$ is one-way implies $\mathcal{H}$ is also one-way.

   Assume now that each $\mathcal{X}_k$ is a cyclic group (in additive notation) and $\mathcal{F} = \{f_k : \mathcal{X}_k \to \mathcal{X}_k\}_{k\in\mathcal{K}}$ are group homomorphisms, and define the composition $\mathcal{F} \circ \mathcal{F} = \{f_k \circ f_k : \mathcal{X}_k \to \mathcal{X}_k\}_{k\in\mathcal{K}}$. Prove that:

   (c) $\mathcal{F}$ is one-way implies $\mathcal{F} \circ \mathcal{F}$ is also one-way.

   (d) $\mathcal{F} \circ \mathcal{F}$ is one-way implies $\mathcal{F}$ is also one-way (**Hint:** perhaps the reduction will make two calls to the adversary inverting $\mathcal{F}$, beware the independence!).

2. Let $\mathcal{G}$ be a cyclic group of prime order q, and consider a generator $g \in \mathcal{G}$. We define the 2-SCasc public key encryption scheme as follows:

   - **Key Generation:** As in ElGamal encryption scheme, $y = g^x$ is the public key, and x is the secret key.
   - **Encryption:** A ciphertext for $m \in \mathcal{G}$ is computed as $c = (g^r, g^s y^r, m y^s)$, for random $r, s \in \mathbb{Z}_q^\times$.

   (a) Give a decryption procedure for 2-SCasc PKE.

   (b) Give the homomorphic properties of the encryption scheme. Consider the strong homomorphic case (i.e., the resulting ciphertext has the proper probability distribution, and it is independent of the input ciphertexts).

   (c) Write a game between a challenger and an adversary showing the OW-CPA security definition.

   (d) Show a reduction from OW-CPA security of 2-SCasc to the CDH problem, and analyze the success probabilities (**Hint:** perhaps the reduction will make two calls to the CDH solver, beware the independence!).

3. Let us consider the Schnorr signature scheme and two variants of it. The three schemes have the same mathematical setting. The key generation protocol always produces a secret key $x \in_R \mathbb{Z}_p$, a public key $y = g^x$ and a hash function $H : \{0,1\}^* \to \mathbb{Z}_p$. For Variant 1, furthermore, there is an additional public key value $y_2 = y^x$. Regarding the signature and verification protocols, the three schemes work as follows:

   - **Schnorr:** to sign m, choose $r \in_R \mathbb{Z}_p$ and output $\sigma = (R, s)$, where $R = g^r$ and $s = r + x \cdot H(m, R) \mod p$. To verify a signature $\sigma = (R, s)$ on a message m for a public key y, check if the equation $g^s = R \cdot y^{H(m,R)}$ holds.
   - **Variant 1:** to sign m, choose $r \in_R \mathbb{Z}_p$ and output $\sigma = (R, s)$, where $R = y^r$ and $s = r + x \cdot H(m, R) \mod p$. To verify a signature $\sigma = (R, s)$ on a message m for a public key (y, y_2), check if the equation $y^s = R \cdot y_2^{H(m,R)}$ holds.
   - **Variant 2:** to sign m, choose $r \in_R \mathbb{Z}_p$ and output $\sigma = (R, s)$, where $R = g^r$ and $s = (r + x) \cdot H(m, R) \mod p$. To verify a signature $\sigma = (R, s)$ on a message m for a public key y, check if the equation $g^s = (R \cdot y)^{H(m,R)}$ holds.

   The goal is to decide whether Variants 1 and 2 are secure signature schemes.

   (a) The three signature schemes are obtained by applying the Fiat-Shamir heuristic to some zero-knowledge proof of knowledge (with 3 steps) of the discrete logarithm of y (in the case of Variant 1, the value $y_2 = y^x$ is also part of the public description of the language). Write these zero-knowledge proofs of knowledge for the case of Variants 1 and 2.

   (b) Do these two protocols satisfy the three properties required for a zero-knowledge proof of knowledge ? Prove them, if the answer is yes.

   (c) In case some of the protocols does not satisfy all the three properties, this may mean that the corresponding signature scheme is NOT secure. Try to find an attack against it. [**Hint:** a single query to the signing oracle should suffice to produce a valid forgery.]

4. Let p be a prime and let $q = p^r$ for some positive integer $r \in \mathbb{Z}^+$. Let $\mathcal{P}$ be a set of participants and $\Gamma \subset 2^{\mathcal{P}}$ be a monotone increasing access structure.

   (a) Prove that if Γ admits a vector space secret sharing scheme over $\mathbb{F}_p$, then Γ admits a vector space secret sharing scheme over $GF(q)$. [**Hint:** consider $GF(q) = \mathbb{F}_p[x]/g(x)$, for some irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ of degree r.]

   (b) To prove that the opposite implication is not true, consider the threshold access structure for $n = 4$ and $t = 2$. Show that this access structure cannot admit a vector space secret sharing scheme over $\mathbb{F}_2$, but it admits a vector space secret sharing scheme (which one?) over $GF(2^3)$.

   (c) For the access structure Γ of part (b), let us define the adversary structure $\mathcal{A} = \Gamma^c = \{B \subset \mathcal{P} \mid B \notin \Gamma\}$. Which kind of adversaries can you tolerate if you want to design a multiparty computation protocol secure against an adversary who can corrupt one subset of players in $\mathcal{A}$?