**NTNU**
Norwegian University of
Science and Technology

Department of Mathematical Sciences

# Examination paper for **TMA4160 Cryptography**

**Academic contact during examination:** Jiaxin Pan

**Phone:**

**Examination date:** 16. December 2020

**Examination time (from–to):** 09:00–13:00

**Permitted examination support material:** Home examination

**Other information:**
Annen info? Hvilken annen info?

**Language:** English

**Number of pages:** 3

**Number of pages enclosed:** 0

**Checked by:**

Date Signature

**Informasjon om trykking av eksamensoppgave**
**Originalen er:**
**1-sidig** ☐ **2-sidig** ☒
**sort/hvit** ☒ **farger** ☐
**skal ha flervalgskjema** ☒

**Problem 1** **(PRG)** For each of the following PRG, can you state whether it is a secure PRG or not? Please justify your answers. For all the PRGs, suppose $\lambda$ is a large positive integer (e.g. 1024) and $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$. When we write $s_1||s_2$, each of $s_1$ and $s_2$ is a bit-string with $\lambda$ bits (i.e. $s_1, s_2 \in \{0,1\}^\lambda$). (The system randomly selects 2 out of 5. 10 points in total)

(1) $H(s_1||s_2) := G(s_1) \oplus G(s_2) \oplus 1^{3\lambda}$ where $1^{2\lambda}$ is $2\lambda$-bit string with all 1.

(2) $H(s_1||s_2) := (s_1, G(s_1 \oplus s_2))$

(3) $H(s_1||s_2) := (s_1 \oplus s_2, G(s_1))$

(4) $H(s_1||s_2) := (s_1 \oplus 1^\lambda, G(s_1))$

(5) $H(s_1||s_2) := (s_1 \oplus s_2, G(s_1 \oplus s_2))$

**Problem 2** **(Negligible functions)**

(1) Which of the following function is negligible in $\lambda$ and which is not? Please justify your answers. (The system randomly selects 2 out of 5. 10 points in total)

   (a) $\frac{1}{\lambda^{\log(\lambda)}}$

   (b) $\frac{\log(\lambda)}{2^\lambda}$

   (c) $\frac{1}{\lambda^{\frac{1}{\lambda}}}$

   (d) $\frac{1}{\sqrt{\lambda}}$

   (e) $\frac{1}{2^{\log(\lambda^2)}}$

(2) Suppose $f$ and $g$ are negligible in $\lambda$ (The system randomly selects 1 out of 2. 5 points.)

   (a) Show that $f(\lambda) + g(\lambda)$ is negligible

   (b) Show that $f(\lambda) \cdot g(\lambda)$ is negligible

(3) Give an example of $f$ and $g$ such that $f$ and $g$ are both negligible but $f(\lambda)/g(\lambda)$ is not negligible. (5 points)

**Problem 3** **(MAC)** Let $H : \mathcal{M} \to \mathcal{X}$ be a collision resistant hash and let $f, f^{-1} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a secure block cipher. Consider the encrypted-hash MAC system $(S, V)$ defined by $S(k, m) := f(k, H(m))$.

(1) (3 points) Define the algorithm $V$ and show the correctness of the encrypted-hash MAC system.

(2) (10 points) Show the encrypted-hash MAC system is a UF-CMA secure MAC.

**Problem 4** **(Trapdoor collision)** Consider the two collision-resistant hash functions based on the DLog and RSA assumptions from our lecture. In this problem, we show that if an adversary knows some trapdoor then it can compute a collision. Thus, these two hash functions are only computationally secure.

(1) (10 points) Let $\mathbb{G}$ be a cyclic group of prime order $p$ generated by $g$. $h$ is an arbitrary element from $\mathbb{G}$. Recall that $H_{dl} : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{G}$ as

$$H_{dl}(a, b) := g^a h^b.$$

Show that if an adversary knows the trapdoor $x \in \mathbb{Z}_p$ such that $h = g^x$ then it can break the 2nd pre-image resistance. Namely, given $(a, b)$ and $x$, the adversary can compute a different $(a', b') \neq (a, b)$ but $H_{dl}(a, b) = H_{dl}(a', b')$

(2) (The system randomly selects 1 out of. 10 points) Let $N$ be an RSA modulus and $e$ be an RSA function (public) key. In particular, $e$ is a prime. $y$ is an arbitrary element from $\mathbb{Z}_N^*$. Recall that $H_{rsa} : \mathbb{Z}_N^* \times \mathbb{Z}_e \to \mathbb{Z}_N^*$ as

$$H_{rsa}(a, b) := a^e \cdot y^b \bmod N$$

(a) Show that if an adversary knows the trapdoor $x \in \mathbb{Z}_N^*$ such that $x^e = y \bmod N$ then it can break the 2nd pre-image resistance.

(b) Show that if an adversary knows the factorization of $N$ (namely, the prime factors $P, Q$ such that $N = P \cdot Q$) then it can invert the function $H_{rsa}$. Namely, given $h \in \mathbb{Z}_N^*$ and the factors $P, Q$, an adversary can compute some $(a, b) \in \mathbb{Z}_N^* \times \mathbb{Z}_e$.

**Problem 5 (ElGamal)**

(1) (5 points.) Recall the ElGamal PKE ciphertext as $(c_1, c_2) := (g^r, g^{rx} \cdot m)$. Show that if an adversary learns the randomness $r$ then it can decrypt the ciphertext and get $m$ without using the secret key.

(2) (The system randomly selects 1 out of 2. 5 points)

(a) Suppose you are given an honestly generated ElGamal ciphertext of an unknown $m \in \mathbb{G}$. Show how to construct a different ciphertext that also decrypts to $m$

(b) Suppose you are given two honestly generated ElGamal ciphertext of unknown $m_1, m_2 \in \mathbb{G}$, respectively. Show how to construct a ciphertext that decrypts to their product $m_1 \cdot m_2$.

**Problem 6 (Schnorr-related one-time signature.)** Let $\mathbb{G}$ be a cyclic group of prime order $p$ generated by $g$. Let $H : \mathcal{M} \to \mathbb{Z}_p$ be a hash function. We define the following signature scheme $(\text{Gen}, \text{Sign}, \text{Ver})$ with message space $\mathcal{M}$:

- $\text{Gen}(1^\lambda)$: choose $a, b$ from $\mathbb{Z}_p$ uniformly at random and compute $A := g^a$ and $B := g^b$. Return the public key $pk := (A, B) \in \mathbb{G}^2$ and secret key $sk := (a, b) \in \mathbb{Z}_p^2$.
- $\text{Sign}(sk, m)$: compute $h := H(m)$ and $\sigma := h \cdot a + b$. Return the signature $\sigma$.

(1) (3 points) Define the verification algorithm, Ver, and show the correctness of the signature scheme.

(2) (10 points) This is a one-time secure scheme (namely, in the UF-CMA security game, the adversary can only ask one signing query). Show that, in the random oracle model (namely, $H$ is modeled as a random oracle), if the DLog assumption holds for $\mathbb{G}$, then this signature is one-time secure.

(3) (7 points) Show why this scheme is not 2-time secure.

(4) (7 points) Modify this scheme to get a 2-time secure scheme.

(Hints: For the 2-time secure scheme, the public key is in $\mathbb{G}^3$, the signature is in $\mathbb{Z}_p$, and the hash function is $H : \mathcal{M} \to \mathbb{Z}_p^2$.)