CS276: Cryptography	Due date: October 17, 2017

Problem Set 3

Instructor: Alessandro Chiesa *GSI: Benjamin Caulfield*

Problem 1

Let (G, E, D) be a secure public-key encryption scheme. Define the pair (S, R) as follows:

$$S(1^k, x) \equiv \{(c, d) \text{ where } (\mathsf{PK}, \mathsf{SK}) \leftarrow G(1^k) \ ; \ z \leftarrow E(\mathsf{PK}, x) \ ; \ c \leftarrow (\mathsf{PK}, z) \ ; \ d \leftarrow \mathsf{SK}\} \ ,$$

$$R(1^k, c, x, d) \equiv \begin{cases} 1 & \text{if } D(\mathsf{SK}, z) = x \\ 0 & \text{otherwise} \end{cases} \ .$$

Prove or disprove that the fact that (S, R) is a string commitment scheme. (If it is, state whether its hiding and binding properties are computational or perfect.)

Problem 2

Prove that commitment schemes that are both perfectly hiding and perfectly binding do not exist.

Problem 3

Definition 1. Let f_0, f_1 be polynomial-time computable, injective and length-preserving functions from $\{0,1\}^*$ to $\{0,1\}^*$. We say that (f_0, f_1) are claw-free permutations, if $\forall \text{PPT} A, \forall c > 0, \forall s.l.\ k$,

$$\Pr[(x_0, x_1) \leftarrow A(1^k) : f_0(x_0) = f_1(x_1)] < k^{-c}.$$

Definition 2. Let H be a sequence of functions, $H = \{H_k\}_{k=1,2,\ldots}$, $H_k : \{0,1\}^* \rightarrow \{0,1\}^k$, such that there exists a polynomial-time computable function $f(\cdot,\cdot)$ such that $\forall k > 0, \forall x \in \{0,1\}^*, f(1^k, x) = H_k(x)$. We say that H is a family of collision-resistant hash functions, if $\forall \text{PPT } B$, $\forall c > 0$, $\forall s.l.\ k$,

$$\Pr[(a, b) \leftarrow B(1^k) : (a \neq b) \wedge (H_k(a) = H_k(b))] < k^{-c}.$$

Prove that if claw-free permutations exist, then so do collision-resistant hash families.

Problem 4

Let (G, S, V) be a signature scheme, where S is deterministic, that is secure against existential forgery under chosen message attacks. Suppose that $|SK| = k$ where $(PK, SK) \leftarrow G(1^k)$, and $\forall SK, m \in \{0,1\}^k$, $|S_{SK}(m)| = \ell(k) \triangleq |S_{SK}(1^k)|$, i.e., the length of signature is fixed. Consider the function family $\{f_{s_1,s_2} : \{0,1\}^{|s_1|} \rightarrow \{0,1\}\}_{s_1,s_2}$, where s_1 is selected as SK according to $G(1^k)$ and $s_2 \leftarrow \{0,1\}^{\ell(k)}$, such that $f_{s_1,s_2}(\alpha) = S_{s_1}(\alpha) \cdot s_2$, where "$\cdot$" is the inner product modulo 2.

Prove that this function family is pseudorandom (although it is not length preserving).