

Assignment 4

OWFs, PKE, Key Exchange

Instructor: Sruthi Sekar

Problem 1 (One way or not?). Let $F = \{f_k : \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a length-preserving pseudorandom permutation. Are the following functions one-way? If yes, prove it via a reduction; else show an attack.

- (a) $f(x, y) := f_x(y)$
- (b) $f(y) := f_{0^n}(y)$ (where $n = |y|$).
- (c) $f(x) := f_x(0^n)$ (where $n = |x|$).
- (d) $f(x) := g(g(x))$ for one way function g .
- (e) $f(x) := g(x) || g(g(x))$ for one way function g .
- (f) f is a one-to-one function which has a hard-core predicate hc .

Problem 2 (CRHF from Discrete Log Assumption). Let discrete log problem be hard relative $\mathcal{G}$. Prove that each of the following $(\text{Gen}, H_{\text{dl}})$ is a collision resistant hash function.

- (a) Define $(\text{Gen}, H_{\text{dl}} : \mathbb{Z}_q \times \mathbb{Z}_q \rightarrow \mathbb{G})$ as follows:
 - $\text{Gen}(1^n)$: Let $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ and generate $h \in_R \mathbb{G}$. Output $k = (\mathbb{G}, q, g, h)$.
 - $H_{\text{dl}}^k(\alpha, \beta) := g^\alpha h^\beta$.
- (b) For $t = \text{poly}(n)$, define $(\text{Gen}, H_{\text{dl}} : \mathbb{Z}_q^t \rightarrow \mathbb{G})$ as follows:
 - $\text{Gen}(1^n)$: Let $(\mathbb{G}, q, h_1) \leftarrow \mathcal{G}(1^n)$ and generate $h_2, \dots, h_t \in_R \mathbb{G}$. Output $k = (\mathbb{G}, q, (h_1, \dots, h_t))$.
 - $H_{\text{dl}}^k(x_1, \dots, x_t) := \prod_i h_i^{x_i}$.

Problem 4 (CRHF from RSA assumption) [Hard]. Let RSA problem be hard relative to GenRSA . Prove that $(\text{Gen}, H_{\text{rsa}})$ defined below is a collision resistant hash function.

- $\text{Gen}(1^n)$: Let $(N, e, d) \leftarrow \text{GenRSA}(1^n)$, where e is a prime and pick a random $y \in_R \mathbb{Z}_N^*$. Output $k = (N, e, y)$
- $H_{\text{rsa}}^k : (\mathbb{Z}_N^* \times \mathbb{Z}_e) \rightarrow \mathbb{Z}_N^*$, defined as: $H_{\text{rsa}}^k(a, b) := a^e y^b \pmod N$.

As a stepping stone, prove the following Shamir's trick: Given $w \in \mathbb{Z}_N^*$ and k with $\gcd(k, e) = 1$ such that $w^e = y^k \pmod N$, it is possible to efficiently compute x such that $x^e = y \pmod N$.

Problem 3 (Key Exchange). Consider the following key exchange protocol:

- Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s := k \oplus r$ to Bob.
- Bob chooses uniform $t \in \{0,1\}^n$, and sends $u := s \oplus t$ to Alice.
- Alice computes $w := u \oplus r$ and sends w to Bob.
- Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

Problem 4 (All about PKEs). The following questions will help you understand IND-CPA/IND-CCA security of PKE a little better.

- a) Show that any two-round key-exchange protocol, where Alice sends one message and Bob replies with another message before they output the keys, can be converted into an IND-CPA secure public key encryption scheme.
- b) Let $\Pi_{bit} = (\text{Gen}, \text{Enc}, \text{Dec})$ be an IND-CPA secure PKE for $\mathcal{M}_{bit} = \{0, 1\}$ (single bit). Can you construct a Π' using Π such that Π' is IND-CPA secure PKE for $\mathcal{M} = \{0, 1\}^n$ (n -bit strings). Describe the construction and give a proof of security via a hybrid argument.
- c) Consider *one-wayness* under CPA (OW-CPA), an alternative security notion for PKE defined as follows:
 - Eve is given pk , generated as $(pk, sk) \leftarrow \text{Gen}(1^n)$.
 - For $m \leftarrow \mathcal{M}_n$, Eve is given $c \leftarrow \text{Enc}(pk, m)$ as the challenge ciphertext.
 - Eve outputs m' and breaks if $m' = m$.

A PKE Π is OW-CPA-secure if for all PPT eavesdroppers Eve, the probability with which Eve breaks Π as above is negligible. Now answer the following questions about IND-CPA and OW-CPA.

- i) Show formally that IND-CPA implies OW-CPA. That is, *any* PKE that is IND-CPA-secure is also OW-CPA-secure.
- ii) What about the opposite direction? Show either that
 - OW-CPA implies IND-CPA; or
 - Come up with a counterexample, i.e., a PKE Π that is OW-CPA-secure but not IND-CPA-secure.
- d) Consider the following attempt at transforming a CPA-secure scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ to a CCA-secure one. Let $(\text{Gen}_M, \text{Mac}, \text{Vrfy})$ be an EU-SCMA secure MAC. Construct $\Pi^{hyb} := (\text{Gen}, \text{Enc}^{hyb}, \text{Dec}^{hyb})$ as follows (with the same Gen as in Π):
 - $\text{Enc}^{hyb}(pk, m)$: pick $k \leftarrow \text{Gen}_M$, generate $c \leftarrow \text{Enc}(pk, (k, m))$ and $t \leftarrow \text{Mac}(k, c)$. Output (c, t) .
 - $\text{Dec}^{hyb}(sk, (c, t))$: Recover $(k, m) := \text{Dec}(sk, c)$. Output $\begin{cases} m, & \text{if } \text{Vrfy}(k, (c, t)) = 1 \\ \perp, & \text{o.w.} \end{cases}$.

Show a CPA-secure encryption Π for which Π^{hyb} is not CCA-secure (for any choice of MAC).