Tutorial 8: ROM and CCA security

Exercise 1. *Pollard-rho*

Let $\mathbb{G}$ be a cyclic group generated by g, of (known) prime order q, and let h be an element of $\mathbb{G}$. Let $F : \mathbb{G} \to \mathbb{Z}_q$ be a nonzero function, and let us define the function $H : \mathbb{G} \to \mathbb{G}$ by $H(\alpha) = \alpha \cdot h \cdot g^{F(\alpha)}$. We consider the following algorithm (called *Pollard ρ Algorithm*).

Pollard ρ Algorithm

Input: $h, g \in \mathbb{G}$

Output: $x \in \{0, \ldots, q-1\}$ such that $h = g^x$ or FAIL.

1. $i \leftarrow 1$
2. $x \leftarrow 0$, $\alpha \leftarrow h$
3. $y \leftarrow F(\alpha)$; $\beta \leftarrow H(\alpha)$
4. **while** $\alpha \neq \beta$ do
5. $\quad x \leftarrow x + F(\alpha) \bmod q; \alpha \leftarrow H(\alpha)$
6. $\quad y \leftarrow y + F(\beta) \bmod q; \beta \leftarrow H(\beta)$
7. $\quad y \leftarrow y + F(\beta) \bmod q; \beta \leftarrow H(\beta)$
8. $\quad i \leftarrow i + 1$
9. **end while**
10. **if** $i < q$ **then**
11. $\quad$ **return** $(x - y)/i \bmod q$
12. **else**
13. $\quad$ **return** FAIL
14. **end if**

To study this algorithm, we define the sequence (γ_i) by $\gamma_1 = h$ and $\gamma_{i+1} = H(\gamma_i)$ for $i \geqslant 1$.

1. Show that in the **while** loop from lines 4 to 9 of the algorithm, we have $\alpha = \gamma_i = g^x h^i$ and $\beta = \gamma_{2i} = g^y h^{2i}$.

2. Show that if this loop finishes with $i < q$, then the algorithm returns the discrete logarithm of h in basis g.

3. Let j be the smallest integer such that $\gamma_j = \gamma_k$ for $k < j$. Show that $j \leqslant q + 1$ and that the loop ends with $i < j$.

4. Show that if F is a random function, then the average execution time of the algorithm is in $O(q^{1/2})$ multiplications in $\mathbb{G}$.

Exercise 2. *RO does not exist*

In this exercise we show a scheme that can be proven secure in the random oracle model, but is insecure when the random oracle model is instantiated with SHA-3 (or any fixed hash function). Let Π be a signature scheme that is secure in the standard model.

Construct a signature scheme Π_y where signing is carried out as follows: if $H(0) = y$ then output the secret key, if $H(0) \neq y$ then return a signature computed using Π.

1. Prove that for any value y, the scheme Π_y is secure in the random oracle model.

2. Show that there exists a particular y for which Π_y is insecure when the random oracle model is instantiated with a fixed function H.

Remark. Here, we assumed that H is a fixed function. In the definition of hash functions given in class, a hash function H^{s_0} is sampled at the beginning of the scheme, uniformly among an ensemble of hash functions $\{H^s, s \in S\}$. If we replace in the previous question the fixed function H by a uniformly chosen function H^s, then the construction given above is not necessarily insecure. However, there are more complex constructions that can be shown to be secure in the random oracle model but insecure when instantiated with any family of functions $\{H^s, s \in S\}$.[1]

Exercise 3. *PRF from a random oracle*

Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a random oracle. For $x \in \{0,1\}^n$ and $k \in \{0,1\}^n$, we define F_k as follows:

$$F_k(x) = H(k\|x).$$

The security of a PRF F_k is defined by the following game:

- A random function H, a random $k \in \{0,1\}^n$ and a uniform bit b are chosen.
- If $b = 0$, the adversary $\mathcal{A}$ is given access to an oracle for evaluating $F_k(\cdot)$. If $b = 1$ then $\mathcal{A}$ is given access an oracle for evaluating a random function mapping n-bit inputs to n-bit outputs (which is independent of H).
- $\mathcal{A}$ outputs a bit b', and succeeds if $b = b'$.

Note that during the second step, $\mathcal{A}$ can access H in addition to the function oracle provided by the experiment.

The function F_k is a PRF if for any polynomial-time adversary $\mathcal{A}$, the success probability of $\mathcal{A}$ in the preceding experiment is at most negligibly greater than $1/2$.

1. Show that F_k is a PRF.

Exercise 4. *IND-CPA schemes that are not CCA*

We recall the El Gamal public key encryption scheme, in a group G with generator $g \in G$ and order n.

- Keygen: sample x uniformly in $\mathbb{Z}/n\mathbb{Z}$. Set $sk = x$ and $pk = g^x$.
- $\mathsf{Enc}(pk, m)$: for any message $m \in G$, sample $r \leftarrow U(\mathbb{Z}_n)$ and output $(c_1, c_2) = (g^r, pk^r \cdot m)$.
- $\mathsf{Dec}(sk, c)$: for any $c = (c_1, c_2) \in G^2$, output $m = c_2 \cdot c_1^{-sk}$.

1. Show that if $(c_1, c_2) = \mathsf{Enc}(pk, m)$ and $(c_1', c_2') = \mathsf{Enc}(pk, m')$ then $(c_1 \cdot c_1', c_2 \cdot c_2')$ is a valid ciphertext for $m \cdot m'$. We say that the El Gamal encryption scheme is homomorphic for multiplication.

2. Show that this scheme is not CCA2-secure.

   We now recall the LWE-based public key encryption scheme seen in class, instantiated to encrypt only 1-bit messages.

[1] See [CGH08], https://arxiv.org/pdf/cs/0010019.pdf, for more details.

- Keygen: Let m, n, q, B be some integers such that $m > n$ and $q > 8mB^2$. Let χ be the distribution $U([-B, B-1] \cap \mathbb{Z})$. Sample $A \leftarrow U(\mathbb{Z}_q^{m \times n})$, $s \leftarrow \chi^n$ and $e \leftarrow \chi^m$. Output $sk = s$ and $pk = (A, b)$ with $b = As + e$.
- Enc(pk, m): for any message $m \in \{0,1\}$, sample $t \leftarrow \chi^m$, $f \leftarrow \chi^n$ and $f' \leftarrow \chi$. Output $(c_1, c_2) = (t \cdot A + f, t \cdot b + f' + \lfloor q/2 \rceil m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.
- Dec(sk, c): for any $c = (c_1, c_2) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, compute $x = c_2 - c_1 \cdot s$ and take for x the representative in $[-q/2, q/2]$. If $|x| < q/4$ output 0, otherwise output 1.

3. Show that this scheme is not CCA2-secure.

Exercise 5. *Cramer-Shoup*

We consider the following encryption scheme, proposed by Cramer and Shoup (and called "lite Cramer-Shoup") in 1998.

Keygen (1^λ)**:** Choose a cyclic group $\mathbb{G}$ of large prime order $q > 2^\lambda$. Choose generators $g, h \leftarrow U(\mathbb{G})$. Choose $\alpha, \beta, \gamma, \delta \leftarrow U(\mathbb{Z}_q)$ and compute $X = g^\alpha h^\beta$ and $Y = g^\gamma h^\delta$.

Define $PK := (g, h, X, Y)$, $SK := (\alpha, \beta, \gamma, \delta) \in \mathbb{Z}_q^4$.

Encrypt(PK, M)**:** In order to encrypt $M \in \mathbb{G}$, do the following.

1. Choose a random $r \leftarrow U(\mathbb{Z}_q)$ and compute
$$C = (C_0, C_1, C_2, C_3) = (M \cdot X^r,\ g^r,\ h^r,\ Y^r).$$
2. Output $C = (C_0, C_1, C_2, C_3)$.

Decrypt(SK, C)**:** Parse C as $(C_0, C_1, C_2, C_3) \in \mathbb{G}^4$ (and return $\perp$ if C is not in $\mathbb{G}^4$). If $C_3 \neq C_1^\gamma \cdot C_2^\delta$, return $\perp$. Otherwise, output $M = C_0 / (C_1^\alpha \cdot C_2^\beta)$.

1. Show that the scheme is *not* secure in the IND-CCA2 sense.

We now consider the problem of proving that the scheme provides IND-CCA1 security under the DDH assumption in $\mathbb{G}$.

2. Show that, if $(g, h, C_1, C_2) = (g, h, g^r, h^r)$ for some random $r \leftarrow U(\mathbb{Z}_q)$, then
$$(C_0, C_1, C_2, C_3) = (M \cdot C_1^\alpha C_2^\beta,\ C_1,\ C_2,\ C_1^\gamma C_2^\delta)$$
is distributed as a valid ciphertext.

3. Show that, if $(g, h, C_1, C_2) = (g, h, g^r, h^{r'})$ for some random $r \leftarrow U(\mathbb{Z}_q)$, $r' \leftarrow U(\mathbb{Z}_q \backslash \{r\})$, then
$$(C_0, C_1, C_2, C_3) = (M \cdot C_1^\alpha C_2^\beta,\ C_1,\ C_2,\ C_1^\gamma C_2^\delta)$$
for some random $\alpha, \beta, \gamma, \delta \leftarrow U(\mathbb{Z}_q)$, is statistically independent of $M \in \mathbb{G}$, even conditionally on the information that PK reveals about $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}_q^4$.

4. We consider the following variant of DDH.

DDH' consists in distinguishing between tuples of the form (g^a, g^b, g^{ab}) and $(g^a, g^b, g^{ab'})$ with a, b uniform modulo q and b' uniform in $\mathbb{Z}_q \backslash \{b\}$. Show that the scheme provides IND-CPA security under the DDH' assumption. (**Bonus:** Show that DDH reduces to DDH'.)

5. Show that, with high probability, decryption queries (which all occur before the adversary sees the challenge ciphertext) of the form $C = (C_0, g^r, h^{r'}, C_3)$ (with $r \neq r'$) always receive the response $\perp$. Deduce that the scheme is IND-CCA1-secure