Advanced Cryptography

Spring Semester 2021

Homework 1

- This homework contains two questions: (1) different flavours of IND-CCA and (2) a PKE in QR_{n^2}.
- You will submit a **report** that will contain all your answers and explanations. The report should be a PDF document. You can use any editor to prepare the report, but Latex is usually the best choice for typesetting math and pseudocode.
- We ask you to **work alone or in groups of 2**. No collaborations are allowed outside of your group. Register your group on `https://forms.gle/FgY2E2j41B8mV9nu9`. Feel free to ask questions to the T.A.
- We might announce some typos for this homework on Moodle in the news forum. Everybody is subscribed to it and does receive an email as well. If you decided to ignore Moodle emails we recommend that you check the forum regularly.
- The homework is due on Moodle on Friday, 19^{th} of March at 23h59. Please submit 1 report per group.

IND-CCA-$i_{\mathsf{PKE}}(\mathcal{A})$

$\mathcal{L}_1 \leftarrow \emptyset; \mathcal{L}_2 \leftarrow \emptyset$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow_\$ \mathsf{Gen}(1^\lambda)$
$b \leftarrow_\$ \{0,1\}$
$\mathsf{pt}_0, \mathsf{pt}_1, st \leftarrow_\$ \mathcal{A}^{\mathsf{ODec1}}(\mathsf{pk})$
$\mathsf{ct}^* \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$
$b' \leftarrow_\$ \mathcal{A}^{\mathsf{ODec2}}(\mathsf{pk}, \mathsf{ct}^*, st)$
return $b' == b \wedge \mathsf{ct}^* \notin \mathcal{L}_2$ // IND-CCA-1
return $b' == b \wedge \mathsf{ct}^* \notin \mathcal{L}_1 \cup \mathcal{L}_2$ // IND-CCA-2
return $b == b'$ // IND-CCA-3

Oracle ODec1(ct)

$\mathcal{L}_1 \leftarrow \mathcal{L}_1 \cup \{\mathsf{ct}\}$
$\mathsf{pt}' \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$
return pt'

Oracle ODec2(ct)

$\mathcal{L}_2 \leftarrow \mathcal{L}_2 \cup \{\mathsf{ct}\}$
$\mathsf{pt}' \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$
return pt'

Figure 1: IND-CCA-i games.

1 Flavours of IND-CCA

In this exercise, you will show implications between several variants of IND-CCA security for PKE (i.e. Public-Key Encryption scheme, same as PKC, see slide 87). More precisely, we consider the 3 games IND-CCA-$i, i \in \{1,2,3\}$ defined in Figure 1. For simplicity, we omit the security parameter λ as input of the games. Then, we can define IND-CCA-i security as follows.

Definition 1 (IND-CCA-1, IND-CCA-2)**.** We say a PKE PKE is IND-CCA-i secure for $i = 1, 2$ if for all ppt adversary $\mathcal{A}$ the advantage

$$\mathsf{Adv}^{\mathrm{ind-cca-i}}_{\mathcal{A},\mathsf{PKE}} := 2\Pr\left[\text{IND-CCA-}i_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] - 1$$

is negligible in λ.

Definition 2 (IND-CCA-3)**.** Let A be the set of ppt adversaries $\mathcal{A}$ s.t. $\mathcal{A}$ never queries the challenge ciphertext ct^* to $\mathsf{ODec2}$. In other words, the probability that $\mathcal{A} \in A$ queries $\mathsf{ODec2}(\mathsf{ct}^*)$ is null. Then, we say a PKE PKE is IND-CCA-3 secure if for all adversary $\mathcal{A} \in A$, the advantage

$$\mathsf{Adv}^{\mathrm{ind-cca-3}}_{\mathcal{A},\mathsf{PKE}} := 2\Pr\left[\text{IND-CCA-3}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] - 1$$

is negligible in λ.

Question 1. Explain why IND-CCA-1 security implies IND-CCA-2 security.

Question 2. Prove that IND-CCA-3 security implies IND-CCA-1 security.
Hint: A valid IND-CCA-3 adversary must be in A.

Question 3. We say a PKE scheme is γ-spread if for all public-key pk and plaintext pt

$$\max_{\mathsf{ct} \in \mathcal{C}} \Pr\left[\mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, \mathsf{pt})\right] \leq \gamma$$

where the probability is taken over the randomness of the encryption. If γ is negligible in the security parameter λ, we say the PKE is *well-spread*.

Show that a well-spread IND-CCA-2 secure PKE is also IND-CCA-1 secure.

Question 4. Explain in a few sentences why the well-spreadness property is needed in the previous question.
Hint: Assume an adversary can find a ciphertext ct' s.t. $\Pr[\mathsf{Enc}(\mathsf{pk}, \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')) = \mathsf{ct}'] = 1$ in the first phase. Can it break IND-CCA-1 security? Does it break IND-CCA-2 security?

Question 5 (bonus). Is IND-CCA-3 equivalent to the IND-CCA security notion seen in class (slide 95)? If it is, prove it, if not explain why.
Assume $|\mathsf{pt}_0| = |\mathsf{pt}_1|$ always holds (or forget about line 3 in slide 95).

2 A PKE in QR_{n^2}

In this exercise, we will work in the group of quadratic residues modulo n^2. More formally, we define the following procedure ParGen, which will output the different parameters needed.

Definition 3 ($\mathsf{ParGen}(1^\lambda)$)**.**

1. Find two safe primes p, q large enough. *Safe prime* means that they are of the form $p = 2p'+1$ and $q = 2q'+1$, where p' and q' are prime and p, q, p', q' are pairwise different.
2. Define n as $n = pq$.
3. Find a generator $g \in \mathbb{Z}^*_{n^2}$ of QR_{n^2}, where QR_{n^2} is the cyclic subgroup of quadratic residues modulo n^2.
4. Ouptut (g, n)

Moreover, **you can assume the following properties hold** for any $(g, n) \leftarrow\!\!\$\, \mathsf{ParGen}(1^\lambda)$.

- The order of QR_{n^2} (i.e. the order of g) is $n\lambda(n)/2 = pqp'q'$, where $\lambda = (\cdot)$ is the Carmichael function.
- $g^{\lambda(n)} = 1 + n \pmod{n^2}$ (this will simplify some computations).

We also define the *discrete logarithm modulo n* problem as follows.

Definition 4 (DL mod n problem)**.** Let $x \leftarrow\!\!\$\, \{1, \ldots, |QR_{n^2}|\}$. Given $(g, n) \leftarrow\!\!\$\, \mathsf{ParGen}(1^\lambda)$ and $h = g^x \bmod n^2$, find $x \bmod n$.
More formally, *the discrete logarithm modulo n* problem is hard if for any ppt adversary $\mathcal{A}$ the following advantage

$$\mathsf{Adv}^{\mathrm{dlmodn}}_{\mathcal{A}} := \Pr[\mathrm{DLMODN}(\mathcal{A}) \Rightarrow \mathbf{true}]$$

is negligible in λ, where the DLMODN game is described below.

DLMODN($\mathcal{A}$)

$(g, n) \leftarrow_\$ \mathsf{ParGen}(1^\lambda)$
$x \leftarrow_\$ \{1, \ldots, |QR_{n^2}|\}$
$h \leftarrow g^x \bmod n^2$
$x' \leftarrow \mathcal{A}(n, g, h)$
return $x' == x \bmod n$

Question 1. Show that if factoring is easy, one can solve the *discrete logarithm modulo n* problem.

We now define the following PKE, that we call QRPKE.

Definition 5 (QRPKE)**.**

- $\mathsf{Gen}(1^\lambda)$: Run $(g, n) \leftarrow_\$ \mathsf{ParGen}$ and sample $a \leftarrow_\$ \{1, \ldots, |QR_{n^2}|\}$. Set $h \leftarrow g^a \bmod n^2$. The public key is (g, h, n), the secret key is a.
- $\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{Z}_n)$: Sample $r \leftarrow_\$ \{1, \ldots, |QR_{n^2}|\}$ and set $U \leftarrow g^r \bmod n^2$. Set $V \leftarrow h^r(1 + mn) \bmod n^2$. Output the ciphertext (U, V).

Question 2. Describe the decryption algorithm of the previous PKE. Prove its correctness.

Question 3. Build a security game capturing the one-wayness (against chosen-plaintext attacks) property of QRPKE. That is, your game should capture the property that it is hard to decrypt a ciphertext output by QRPKE (in a CPA setting). Define the corresponding advantage.

Question 4. Prove that if one can factor n, one can decrypt any ciphertext output by QRPKE. I.e. if factoring is easy, QRPKE is not one-way.

Finally, we define the *QR Diffie-Hellman problem* problem as follows.

Definition 6 (QRDH problem)**.** Let $(g, n) \leftarrow_\$ \mathsf{ParGen}(1^\lambda)$ and $x, y \leftarrow_\$ \{1, \ldots, |QR_{n^2}|\}$. Given $X = g^x \bmod n^2, Y = g^y \bmod n^2$ and $Z \bmod n = g^{xy} \bmod n$, compute $Z = g^{xy} \bmod n^2$. Note that $Z \bmod n$ is given but the goal is to recover $Z \bmod n^2$.
More formally, the *QR Diffie-Hellman problem* is hard if for any ppt adversary $\mathcal{A}$ the following advantage

$$\mathsf{Adv}^{\mathrm{qrdh}}_{\mathcal{A}} := \Pr[\mathrm{QRDH}(\mathcal{A}) \Rightarrow \mathbf{true}]$$

is negligible in λ, where the QRDH game is described below.

QRDH($\mathcal{A}$)

$(g, n) \leftarrow\!\!\$\ \mathsf{ParGen}(1^\lambda)$
$x, y \leftarrow\!\!\$\ \{1, \ldots, |QR_{n^2}|\}$
$X \leftarrow g^x \bmod n^2$
$Y \leftarrow g^y \bmod n^2$
$Z \leftarrow g^{xy} \bmod n^2$
$Z' \leftarrow \mathcal{A}(n, g, X, Y, Z \bmod n)$
return $Z' == Z \bmod n^2$

Question 5. Prove that if the QR Diffie-Hellman problem is hard, QRPKE is one-way. Use your one-wayness definition from Question 3.