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.

(2pts)
One can see that when an adversary *wins* in the IND-CCA-2 game, it also wins in the IND-CCA-1 game (i.e. the winning condidition is more restrictive in the former). Therefore, for any $\mathcal{A}$, $\Pr\left[\text{IND-CCA-2}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] \leq \Pr\left[\text{IND-CCA-1}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right]$. Hence, for any ppt $\mathcal{A}$, we have

$$\mathsf{Adv}^{\mathrm{ind-cca-2}}_{\mathcal{A},\mathsf{PKE}} \leq \mathsf{Adv}^{\mathrm{ind-cca-1}}_{\mathcal{A},\mathsf{PKE}} \ .$$

Therefore, if the scheme is IND-CCA-1 secure (i.e. the right-handside is negligible for all ppt $\mathcal{A}$), it is also IND-CCA-2 secure.

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

(3pts)
We are going to construct an IND-CCA-3 adversary $\mathcal{B}$ from an IND-CCA-1 one $\mathcal{A}$ as follows.

$\mathcal{B}(\mathcal{A})$	**Oracle** $\mathsf{ODec2'}(\mathsf{ct})$
// first phase:	**if** $\mathsf{ct} = \mathsf{ct}^*$:
$\mathcal{B}$ runs $\mathcal{A}$ and replies to its queries with its own oracle $\mathsf{ODec1}$	**return** $\perp$
// second phase:	$\mathsf{pt}' \leftarrow \mathsf{ODec2}(\mathsf{ct})$
$\mathcal{B}$ runs $\mathcal{A}$ and replies to its queries with the oracle $\mathsf{ODec2'}$	**return** pt'

We see that $\mathcal{B}$ never queries $\mathsf{ODec2}(\mathsf{ct}^*)$ and thus it is a valid IND-CCA-3 adversary. Moreover, whenever $\mathcal{A}$ wins in the IND-CCA-1 game, $\mathcal{B}$ wins in the IND-CCA-3 game. Hence, as in the previous question, we have that for all ppt adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ s.t.

$$\mathsf{Adv}^{\mathrm{ind-cca-1}}_{\mathcal{A},\mathsf{PKE}} \leq \mathsf{Adv}^{\mathrm{ind-cca-3}}_{\mathcal{B},\mathsf{PKE}} .$$

Thus, IND-CCA-3 security implies IND-CCA-1 security.
Note: It is important that $\mathcal{B}$ **never** queries $\mathsf{ODec2}(\mathsf{ct}^*)$, even when it is going to lose. Otherwise it is not a valid adversary, and thus we cannot say that its advantage is negligible if the scheme is IND-CCA-3 secure.

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.

(3pts)
First, we modify the game IND-CCA-1 into another game Γ' as follows. After computing ct^*, we check whether $\mathsf{ct}^* \in \mathcal{L}_1$ and if it is, we **abort** the game. Let's call this event bad and let $\mathcal{L}_1 = \{\mathsf{ct}_1, \ldots, \mathsf{ct}_q\}$ for some $\mathsf{ct}_i, 1 \leq i \leq q$. We have

$$\Pr[\mathsf{bad}] = \Pr\left[\bigvee_{i=1}^{q} \mathsf{ct}^* = \mathsf{ct}_i\right] \leq \sum_{i=1}^{q} \Pr[\mathsf{ct}^* = \mathsf{ct}_i] \leq q\gamma$$

where we used the union bound and the defition of γ-spreadness. Now, by the difference lemma (slide 109), we have

$$\left|\Pr\left[\text{IND-CCA-1}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] - \Pr\left[\Gamma'_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right]\right| \leq \Pr[\mathsf{bad}] \leq q\gamma \ .$$

Finally, note that whenever $\mathcal{A}$ wins the Γ' game, bad does not occur and therefore it also wins the IND-CCA-2 game. Hence,

$$\Pr\left[\Gamma'_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] \leq \Pr\left[\text{IND-CCA-2}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] \ .$$

Putting it all together we have

$$\begin{aligned}\Pr\left[\text{IND-CCA-1}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] &\leq \left|\Pr\left[\text{IND-CCA-1}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] - \Pr\left[\Gamma'_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right]\right| \\ &\quad + \Pr\left[\Gamma'_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right] \\ &\leq q\gamma + \Pr\left[\text{IND-CCA-2}_{\mathsf{PKE}}(\mathcal{A}) \Rightarrow \mathbf{true}\right]\end{aligned}$$

and therefore

$$\mathsf{Adv}^{\text{ind-cca-1}}_{\mathcal{A},\mathsf{PKE}} \leq 2q\gamma + \mathsf{Adv}^{\text{ind-cca-2}}_{\mathcal{A},\mathsf{PKE}} \ .$$

Hence, if the PKE is well spread (i.e. γ, thus $2q\gamma$, is negligible) and IND-CCA-2 secure, it is also IND-CCA1 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?

(2pts)
We follow the hint and we assume that it is easy to find ct' s.t. $\Pr[\mathsf{Enc}(\mathsf{pk}, \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}')) = \mathsf{ct}'] = 1$. Then a first phase adversary $\mathcal{A}_1$ can submit ct' to the decryption oracle and obtain the corresponding pt' and output $(\mathsf{pt}', \mathsf{pt}_2)$ where pt_2 is random and different than pt'. If $\mathsf{ct}^* = \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}')$, we will have $\mathsf{ct}^* = \mathsf{ct}'$ and the adversary can distinguish and win the IND-CCA-1 game, as $\mathsf{ct}^* = \mathsf{ct}'$ will not be in $\mathcal{L}_2$. As it is in $\mathcal{L}_1$, it would not win the IND-CCA-2 game though.

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).

(2pts)
We can transform the IND-CCA game of the slides into an equivalent game of similar shape as the ones in Figure 1, see slide 76 for example. Then, the equivalence is simple. Clearly, a successful IND-CCA-3 adversary will also win the IND-CCA game. For the

other direction, one can build an IND-CCA-3 adversary from an IND-CCA one in a similar fashion as in Question 2.

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

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

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.

(3pts)
We are going to use extensively the equality

$$g^{x\lambda} = (1+n)^x = (1+xn) = (1+(x \bmod n)n) \bmod n^2 \ .$$

If one can factor n, one can compute $\lambda(n)$. Therefore, a DLMODN adversary $\mathcal{A}(n,g,h)$ can compute

$$h^\lambda = g^{x\lambda} = (1+(x \bmod n)n) \bmod n^2 \ .$$

Thus, $h^\lambda - 1 \bmod n^2 = (x \bmod n)n$ where modn^2 is the modulo operation. Hence, $\mathcal{A}$ computes

$$\frac{h^\lambda - 1 \bmod n^2}{n} = x \bmod n \ .$$

and wins the DLMODN game.

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 $a \leftarrow_\$ \{1,\dots,|QR_{n^2}|\}$. 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 $r \leftarrow_\$ \{1,\dots,|QR_{n^2}|\}$ 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.

(2pts)
We can define $\mathsf{Dec}(a,(U,V)) : \frac{VU^{-a} - 1 \bmod n^2}{n}$. Clearly, $VU^{-a} - 1 = h^r(1+mn)h^{-r} - 1 = (m \bmod n)n \bmod n^2$ and thus the decryption is correct as $m \in \mathbb{Z}_n$.

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.

(2pts)
The goal of this question is just to explicitly write the OW-CPA game with the functions of our PKE:

$\underline{\mathrm{OW}_{\mathsf{QRPKE}}(\mathcal{A})}$

$(g, n) \leftarrow_{\$} \mathsf{ParGen}(1^\lambda)$
$a, r \leftarrow_{\$} \{1, \ldots, |QR_{n^2}|\}$
$h \leftarrow g^a \bmod n^2$
$m \leftarrow_{\$} \mathbb{Z}_n$
$U = g^r \bmod n^2$
$V = h^r(1 + mn) \bmod n^2$
$m' \leftarrow \mathcal{A}((n, g, h), (U, V))$
return $m' == m \bmod n$

And the advantage is

$$\mathsf{Adv}^{\mathrm{ow}}_{\mathcal{A},\mathsf{QRPKE}} = \Pr[\mathsf{QRPKE}(\mathcal{A}) \Rightarrow 1] \ .$$

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.

(3pts)
As before, if one can factor, one can compute $\lambda(n)$. Then, by Question 1, given $h^r = g^{ar}$, one can compute $\alpha \leftarrow ar \bmod n$ and write $ar = \alpha + \beta n$ for some β. Then,

$$\left(\frac{V}{g^\alpha}\right)^\lambda = g^{\beta n \lambda}(1 + m\lambda n) = (1 + (m\lambda \bmod n)n) \bmod n^2$$

where we used $g^{n\lambda} = 1$. Thus,

$$\frac{\left(\frac{V}{g^\alpha}\right)^\lambda - 1}{n} = \lambda m \bmod n$$

and

$$\frac{\left(\frac{V}{g^\alpha}\right)^\lambda - 1}{n} \cdot (\lambda^{-1} \bmod n) = m \bmod n$$

Note that $\gcd(\lambda, n) = 1$, therefore $\lambda^{-1} \bmod n$ exists. Hence, if one can factor, one can decrypt and win the OW game.

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.

$\underline{\mathrm{QRDH}(\mathcal{A})}$

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

(3pts)
Given any OW adversary $\mathcal{A}$, one can construct the following QRDH adversary $\mathcal{B}$.

$\underline{\mathcal{B}^{\mathcal{A}}(n, g, X, Y, z)}$

$m \leftarrow\!\!\$\ \mathbb{Z}_n$
$h \leftarrow X; U \leftarrow Y$
$V \leftarrow z(1 + mn)$
$M \leftarrow \mathcal{A}((n, g, h), (U, V))$
$Z \leftarrow z(1 + (m - M)n)$
return Z

The OW adversary $\mathcal{A}$ will return M s.t.

$$V = h^y(1 + Mn) = U^x(1 + Mn) = g^{xy}(1 + Mn) = Z(1 + Mn) \bmod n^2 \ .$$

Hence, $V = z(1 + mn) = Z(1 + Mn) = Z + (Z \bmod n)Mn = Z + zMn$ and thus $Z = z(1 + (m - M)n) \bmod n^2$. Therefore, when $\mathcal{A}$ outputs the decryption of (U, V), $\mathcal{B}$ recovers $Z = g^{xy}$ and

$$\mathsf{Adv}^{\mathrm{ow}}_{\mathcal{A},\mathsf{QRPKE}} \leq \mathsf{Adv}^{\mathrm{qrdh}}_{\mathcal{B}} \ .$$

which concludes the proof.
To be complete however, one should prove that the inputs of $\mathcal{A}$ in the reduction follow the same distribution as the inputs when $\mathcal{A}$ plays the OW game. It is straightforward to see that it is the case for (n, g, h, U). Then, V is of the form $z(1 + mn)$. One can write $Z = z + \alpha n$ for some α and we have

$$Z(1 + (m - z^{-1}\alpha)n) = (z + \alpha n)(1 + (m - z^{-1}\alpha)n) = z(1 + mn) = V \bmod n^2 \ .$$

Thus, V is of the form $Z(1+Mn)$ with $M = m - z^{-1}\alpha$ which is uniformly distributed when m is uniformly distributed. Note that $z^{-1} \bmod n$ exists as $Z \in \mathbb{Z}^*_{n^2}$, which implies $\gcd(Z, n) = 1$ and thefore $\gcd(z, n) = 1$. Hence, V follows the correct ditribution.