

**2022201041**

**Use the CPA security and secure MAC to design a provably CCA-secure encryption scheme**

To obtain a CPA-secure encryption scheme using PRF, Let  $F$  be a PRF. First, one needs

to define a private-key encryption scheme for messages of length  $n$ .

The encryption scheme is a collection of three algorithms, namely, key generation algorithm (Gen), encryption algorithm (Enc) and decryption algorithm (Dec). The Gen

gives key to both the sender and receiver, the Enc with key, plain text and local randomness gives the ciphertext as the output, and Dec takes the ciphertext and key to

output the message.

For the CPA-secure encryption :

1. Gen : on input  $1n$ , choose  $k \leftarrow \{0,1\}^n$  uniformly at random and output it as the key
2. Enc : on input a key where  $k$  is belonging to  $\{0,1\}^n$  and a message ' $m$ ' belonging to  $\{0,1\}^n$ , choose  $r \leftarrow \{0,1\}^n$  uniformly at random and output the ciphertext  
 $c := \langle r, F_k(r) \oplus m \rangle$
3. Dec : on input a key ' $k$ ' belonging to  $\{0,1\}^n$  and a ciphertext  $c = \langle r, s \rangle$ , output the

plaintext message

$$m := F_k(r) \oplus s$$

By following the above mentioned instructions, a CPA-secure encryption scheme from

any pseudorandom function can be obtained.

A MAC is Message Authentication Codes. The components of the authentication protocol involves :

1. A key generation algorithm that returns a secret key ' $k$ '
2. A MAC generating algorithm that returns a tag for a given message ' $m$ ' where the tag ' $t$ ' = MAC  $k(m)$

3. A verification algorithm that returns a bit  $b = \text{Verify}_k(m_1, t_1)$ , given a message  $m_1$

and a tag  $t_1$ .

4. If the message is not modified then with high probability, the value of  $b$  is true otherwise false.

A MAC( $\text{Gen}$ ,  $\text{MAC}$ ,  $\text{Verify}$ ) is secure if for all probabilistic polynomial-time adversaries  $A$ :

$$\Pr[\text{MAC-Game}(n) = 1] \leq \text{negl}(n)$$

To build a provably secure CCA-secure private-key encryption scheme( $\text{Gen}'$ ,  $\text{Enc}'$ ,  $\text{Dec}'$ ), the following instructions will be helpful.

Let a private-key encryption scheme be ( $\text{GenE}$ ,  $\text{Enc}$ ,  $\text{Dec}$ ) and a message authentication

code be ( $\text{GenM}$ ,  $\text{Mac}$ ,  $\text{Vrfy}$ )

1.  $\text{Gen}'$  : on input  $1^n$ , run  $\text{GenE}(1^n)$  and  $\text{GenM}(1^n)$  to obtain keys  $k_1, k_2$ , respectively. 2.  $\text{Enc}'$  : on input a key  $(k_1, k_2)$  and a plaintext message  $m$ , compute  $c \leftarrow \text{Enc}_1(m)$

and  $t \leftarrow \text{Mac}_2(c)$  and output the ciphertext  $\langle c, t \rangle$

3.  $\text{Dec}'$  : on input a key  $(k_1, k_2)$  and a ciphertext  $\langle c, t \rangle$ , first check whether  $\text{Vrfy}_2(c, t)$

$= 1$ . If yes, then output  $\text{Dec}_1(c)$ .

**CONSTRUCTION 3.28**

Let  $F$  be a pseudorandom function. Define a fixed-length, private-key encryption scheme for messages of length  $n$  as follows:

- Gen: on input  $1^n$ , choose uniform  $k \in \{0, 1\}^n$  and output it.
- Enc: on input a key  $k \in \{0, 1\}^n$  and a message  $m \in \{0, 1\}^n$ , choose uniform  $r \in \{0, 1\}^n$  and output the ciphertext

$$c := \langle r, F_k(r) \oplus m \rangle.$$

- Dec: on input a key  $k \in \{0, 1\}^n$  and a ciphertext  $c = \langle r, s \rangle$ , output the message

$$m := F_k(r) \oplus s.$$

A CPA-secure encryption scheme from any pseudorandom function.

**To prove the security of an encryption scheme under CCA, we need to show that an attacker who can obtain ciphertexts of their choice cannot learn any information about the plaintexts, except for what they can learn by observing the ciphertexts.**

**THEOREM 4.18** *Assume that  $\Pi_E = (\text{Gen}_E, \text{Enc}, \text{Dec})$  is a CPA-secure encryption scheme and that  $\Pi_M = (\text{Gen}_M, \text{Mac}, \text{Vrfy})$  is a secure message authentication code with unique tags. Then, Construction 4.17 is a CCA-secure encryption scheme.*

**PROOF** The idea behind the proof of this theorem is as follows. Since  $(\text{Gen}_M, \text{Mac}, \text{Vrfy})$  is a secure message authentication code, we can assume that all queries to the decryption oracle are *invalid*, unless the queried ciphertext was previously obtained by the adversary from its encryption oracle. Therefore, the security of the scheme  $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$  in Construction 4.17 is reduced to the CPA-security of  $(\text{Gen}_E, \text{Enc}, \text{Dec})$  (because the decryption oracle is effectively useless). In more detail, we first prove that except with negligible probability, the only valid queries made by the adversary to the decryption oracle are ciphertexts that were previously obtained from the encryption oracle. Then, given this claim, we prove that if the CCA-secure scheme is not secure, then neither is the underlying CPA-scheme  $(\text{Gen}_E, \text{Enc}, \text{Dec})$ . This is due to the fact that an adversary for the CPA-secure scheme can actually simulate a decryption oracle for the CCA adversary. This simulation works by returning  $\perp$  if the received ciphertext was never queried before, and returning the appropriate message if the ciphertext was generated by querying the encryption oracle. The validity of this simulation follows from the above claim. We now proceed to the formal proof.

Let  $\mathcal{A}$  be any probabilistic polynomial-time CCA adversary attacking Construction 4.17. Define  $\text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)$  to be the event that in the experiment  $\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n)$ , the adversary  $\mathcal{A}$  generates a query  $(c, t)$  to the decryption oracle that was not obtained from the encryption oracle and does not result in an oracle reply  $\perp$ . We claim that  $\Pr[\text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)]$  is at most negligible. Intuitively, this is due to the fact that if the oracle does not reply  $\perp$ , then  $t$  is a valid MAC tag for  $c$ . Thus, if  $(c, t)$  was not obtained by querying the encryption oracle, this means that  $\mathcal{A}$  must have forged a MAC. Formally, we prove that if the probability that  $\text{VALID-QUERY}$  occurs is non-negligible, then we can construct an adversary  $\mathcal{A}_{\text{mac}}$  that breaks the MAC as follows. Let  $q(\cdot)$  be a polynomial that upper-bounds the running-time of  $\mathcal{A}$  (and thus the number of oracle queries it makes). Then, adversary  $\mathcal{A}_{\text{mac}}$ , interacting in  $\text{Mac-forge}_{\mathcal{A}_{\text{mac}}, \Pi_M}(n)$ , chooses a random key  $k_1$  for  $\text{Enc}$  and a random value



---

$i \leftarrow \{1, \dots, q(n)\}$ , and invokes the CCA-adversary  $\mathcal{A}$ . Adversary  $\mathcal{A}_{\text{mac}}$  then simulates the encryption and decryption oracles for  $\mathcal{A}$ . The way it does this is to use  $k_1$  and its MAC-generating oracle to simulate the encryption oracle for  $\mathcal{A}$ . Regarding the decryption oracle, all but the  $i^{\text{th}}$  query will be assumed to be invalid, and  $\mathcal{A}_{\text{mac}}$  will “hope” that the  $i^{\text{th}}$  query is valid. In this case,  $\mathcal{A}_{\text{mac}}$  will hope to have obtained a forged tag. More specifically, when  $\mathcal{A}$  queries the encryption oracle with  $m$ , adversary  $\mathcal{A}_{\text{mac}}$  computes  $c = \text{Enc}_{k_1}(m)$  and requests a tag  $t$  for  $c$ . Adversary  $\mathcal{A}_{\text{mac}}$  then returns the pair  $(c, t)$  to  $\mathcal{A}$  as its oracle reply. In contrast, in every decryption oracle query  $(c, t)$  from  $\mathcal{A}$  *apart from the  $i^{\text{th}}$  one*, adversary  $\mathcal{A}_{\text{mac}}$  first checks if  $(c, t)$  was ever generated from an encryption query. If yes,  $\mathcal{A}_{\text{mac}}$  returns the plaintext  $m$  that was queried by  $\mathcal{A}$  when  $(c, t)$  was generated. If not,  $\mathcal{A}_{\text{mac}}$  returns  $\perp$ . In contrast, for the  $i^{\text{th}}$  decryption oracle query  $(c, t)$ , adversary  $\mathcal{A}_{\text{mac}}$  outputs  $(c, t)$  as its MAC forgery and halts. (We remark that the generation of the challenge ciphertext from the pair  $(m_0, m_1)$  is also carried out by  $\mathcal{A}_{\text{mac}}$  for  $\mathcal{A}$  as in the CCA experiment.)

Clearly  $\mathcal{A}_{\text{mac}}$  runs in probabilistic polynomial-time. We now analyze the probability that  $\mathcal{A}_{\text{mac}}$  generates a good forgery, and so succeeds in **Mac-forge**. By our contradicting assumption, with non-negligible probability, adversary  $\mathcal{A}$  generates a query  $(c, t)$  to the decryption oracle that was not obtained from the encryption oracle, and does not return  $\perp$ . We remark that since  $(\text{Gen}_M, \text{Mac}, \text{Vrfy})$  has unique tags, it follows that the query  $c$  was never asked by  $\mathcal{A}_{\text{mac}}$  to its MAC-tag oracle (because  $(c, t)$  was not obtained from an encryption query and there is only a single possible  $t$  that is a valid MAC tag for  $c$ ). Therefore, such a pair  $(c, t)$  is a “good forgery” for  $\mathcal{A}_{\text{mac}}$ . Now, if all the decryption oracle queries generated by  $\mathcal{A}$  up until the  $i^{\text{th}}$  one were indeed invalid, then the simulation by  $\mathcal{A}_{\text{mac}}$  for  $\mathcal{A}$  up until the  $i^{\text{th}}$  query is perfect. Furthermore, the probability that the  $i^{\text{th}}$  query is the *first* valid one generated by  $\mathcal{A}$  is at least  $1/q(n)$  because  $\mathcal{A}$  makes at most  $q(n)$  oracle queries, and one of these is the first valid one. Therefore, the probability that  $\mathcal{A}_{\text{mac}}$  succeeds in **Mac-forge** is at least  $1/q(n)$  times the probability that the **VALID-QUERY** event occurs. Since  $\mathcal{A}_{\text{mac}}$  can succeed in **Mac-forge** with at most negligible probability, it follows that **VALID-QUERY** occurs with at most negligible probability. That is, we have that for some negligible function  $\text{negl}$ ,

$$\Pr [\text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] < \text{negl}(n).$$

Given that **VALID-QUERY** occurs with at most negligible probability, we now show that Construction 4.17 is CCA-secure. In this part of the proof, we reduce the security to the CPA-security of  $(\text{Gen}_E, \text{Enc}, \text{Dec})$ . Specifically, let  $\mathcal{A}$  be any probabilistic polynomial-time adversary for  $\text{PrivK}^{\text{cca}}$ . We use  $\mathcal{A}$  to construct an adversary  $\mathcal{A}_{\text{enc}}$  for the CPA experiment with  $(\text{Gen}_E, \text{Enc}, \text{Dec})$ . Adversary  $\mathcal{A}_{\text{enc}}$  chooses a key  $k_2$  and invokes the adversary  $\mathcal{A}$ . Whenever  $\mathcal{A}$  asks an encryption query  $m$ , adversary  $\mathcal{A}_{\text{enc}}$  queries its encryption oracle with  $m$  and receives back some  $c$ . Then  $\mathcal{A}_{\text{enc}}$  computes  $t = \text{Mac}_{k_2}(c)$  and hands  $\mathcal{A}$  the pair  $(c, t)$ . Whenever  $\mathcal{A}$  asks for a decryption query  $(c, t)$ ,  $\mathcal{A}_{\text{enc}}$  checks if



( $c, t$ ) where  $t = \text{Mac}_{k_2}(c)$ .  $\mathcal{A}_{\text{enc}}$  then sends the value  $m$  to the decryption oracle. If the oracle returns a response,  $\mathcal{A}_{\text{enc}}$  outputs 1. Otherwise, it outputs 0. This implies that  $\mathcal{A}_{\text{enc}}$  succeeds in  $\text{PrivK}^{\text{cpa}}$  with non-negligible advantage over  $1/2$ . Since this contradicts the CPA-security of  $\Pi_E = (\text{Gen}_E, \text{Enc}, \text{Dec})$ , we conclude that Construction 4.17 is CCA-secure.  $\blacksquare$

same pair and receives back a challenge ciphertext  $c$ . As above,  $\mathcal{A}_{\text{enc}}$  hands  $\mathcal{A}$  the challenge ciphertext  $(c, t)$  where  $t = \text{Mac}_{k_2}(c)$ . Notice that  $\mathcal{A}_{\text{enc}}$  does not need a decryption oracle because it assumes that any new query is always invalid. Furthermore,  $\mathcal{A}_{\text{enc}}$  runs in probabilistic polynomial-time because it just invokes  $\mathcal{A}$  and adds MAC tags (that are efficiently computable because  $\mathcal{A}_{\text{enc}}$  chose  $k_2$ ). It is straightforward to see that the success of  $\mathcal{A}_{\text{enc}}$  in  $\text{PrivK}^{\text{cpa}}$  when VALID-QUERY does not occur *equals* the success of  $\mathcal{A}$  in  $\text{PrivK}^{\text{cca}}$  when VALID-QUERY does not occur. That is,

$$\begin{aligned} \Pr[\text{PrivK}_{\mathcal{A}_{\text{enc}}, \Pi_E}^{\text{cpa}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \\ = \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \end{aligned}$$

implying that

$$\begin{aligned} \Pr[\text{PrivK}_{\mathcal{A}_{\text{enc}}, \Pi_E}^{\text{cpa}}(n) = 1] \\ \geq \Pr[\text{PrivK}_{\mathcal{A}_{\text{enc}}, \Pi_E}^{\text{cpa}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \\ = \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \end{aligned} \quad (4.5)$$

Assume now by contradiction that there exists a *non-negligible function*  $\varepsilon$  such that

$$\Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1] = \frac{1}{2} + \varepsilon(n).$$

By the fact that  $\Pr[\text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)]$  is negligible, we have that it is smaller than  $\varepsilon(n)/2$ . This in turn implies that

$$\Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] < \varepsilon(n)/2$$

and so

$$\begin{aligned} \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1] &= \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \\ &\quad + \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] \\ &< \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] + \frac{\varepsilon(n)}{2}. \end{aligned}$$

Rearranging the above, and using the fact that  $\mathcal{A}$  succeeds in  $\text{PrivK}^{\text{cca}}$  with probability  $1/2 + \varepsilon(n)$ , we have that

$$\begin{aligned} \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1 \wedge \neg \text{VALID-QUERY}_{\mathcal{A}, \Pi'}(n)] &> \Pr[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cca}}(n) = 1] - \frac{\varepsilon(n)}{2} \\ &= \frac{1}{2} + \frac{\varepsilon(n)}{2}. \end{aligned}$$

Combining this with Equation (4.5), we have that

$$\Pr[\text{PrivK}_{\mathcal{A}_{\text{enc}}, \Pi_E}^{\text{cpa}}(n) = 1] > \frac{1}{2} + \frac{\varepsilon(n)}{2}$$