Introduction

In this work sheet, we investigate authenticated modes of operation and generic composition. We will also consider a bit more in depth the power of *chosen ciphertext attacks*, using a weak notion of one-wayness to show that even modes that are indistinguishable from random against chosen plaintext attack fail on weaker security goals when decryption queries are allowed.

1 Understanding CCA (In)Security

Consider the weak CCA-like one-way security experiment and advantage shown in Figure 1. We then define weak-OW-CCA security as normal by bounding the advantage of any bounded adversary.

► Note that the adversary here is weaker than the standard CCA adversary seen, for example, in (N)IND-CCA: the attacks we consider do not require the adversary to control the nonce (so we use random IVs), or to make encryption queries (so we do not give the adversary an encryption oracle). This notion is not very interesting for its own sake, and you don't have to remember it beyond the end of this problem sheet.

$\mathsf{Exp}^{\text{weak-ow-cca}}_{\text{ENC}}(\mathbb{A})$

$k \leftarrow_\$ \mathsf{Kg}$
$n^* \leftarrow_\$ \mathcal{N}$
$m^* \leftarrow_\$ \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}_k^{n^*}(m^*)$
$\widehat{m} \leftarrow_\$ \mathbb{A}^{\mathcal{D}(\cdot,\cdot)}(n^*, c^*)$

random key, nonce, msg

adversary tries to guess message
· can see nonce and ciphertext
· can decrypt any ciphertext besides the actual one

$\mathcal{D}(n, c)$

require $(n, c) \neq (n^*, c^*)$
$m \leftarrow \mathsf{Dec}_k^n(c)$
return m

$$\mathsf{Adv}^{\text{weak-ow-cca}}_{\text{ENC}}(\mathbb{A}) = \Pr\left[\mathsf{Exp}^{\text{weak-ow-cca}}_{\text{ENC}}(\mathbb{A}) : \widehat{m} = m^*\right]$$

Figure 1: A weak notion of one-wayness against chosen ciphertext attacks.

1. ⋆⋆ Show that CBC Mode is not weak-OW-CCA-secure. You may assume that the challenge message consists of two blocks, without imposing a similar limit on the ciphertexts you can query the decryption oracle on.

Let k, n^*, $m^* = m_1^* \| m_2^*$, and $c^* = c_1^* \| c_2^*$ be as in Figure 1.
The adversary can first decrypt c_1^* using the given nonce: $\hat{m}_1 \leftarrow D(n^*, c_1^*)$.
Note that this recovers the first block of plaintext in full, i.e. $\hat{m}_1 = m_1^*$.

Next, the adversary can decrypt c_2^* as follows: $\hat{m}_2 \leftarrow D(c_1^*, c_2^*)$. From the way CBC decryption works, with the previous block of ciphertext being used as a nonce, this will give the 2nd block of plaintext: $\hat{m}_2 = m_2^*$.
Thus the adversary has recovered $m^* = \hat{m}_1 \| \hat{m}_2$.

2. ⋆⋆ Show that CTR Mode is not weak-OW-CCA-secure. You may assume that the challenge message consists of two blocks and try to come up with an attack that only request decryptions of two-block ciphertexts.

Let K, n^*, $m^* = m_1^* \| m_2^*$, and $c^* = c_1^* \| c_2^*$ be as in Figure 1.

The adversary can basically just run the decryption algorithm twice, once for each block of plaintext.

The first time, they do $\hat{m}_1 \| \hat{m}_2 \leftarrow D(c_1^* \| x, n^*)$, where x is any ciphertext block of the correct length (for example, all zeroes). This will give $\hat{m}_1 = m_1^*$, as CTR mode processes each block individually. $\hat{m}_2$ can be discarded.

Next, the adversary runs $\hat{m}_1' \| \hat{m}_2' \leftarrow D(x \| c_2^*, n^*)$. As before, this gives $\hat{m}_2' = m_2^*$.

Thus the adversary has recovered $\hat{m}_1 \| \hat{m}_2' = m^*$.

?

2 Understanding AE (In)Security

Figure 2 shows all three generic composition modes with the explicit nonce-authentication "greyed out". From the three types of generic composition, we saw that encrypt-then-mac (the middle panel) was the preferred option. For encrypt-then-mac, it is crucial that the nonce is not just used for encryption, but is also explicitly authenticated. In this question we will look how leaving out nonce authentication, affects the integrity of ciphertexts, and the overall security of the constructed encryption scheme.

$\mathrm{MtE}^{n}_{k_a,k_e}(m)$	$\mathrm{EtM}^{n}_{k_a,k_e}(m)$	$\mathrm{E{+}M}^{n}_{k_a,k_e}(m)$
$t \leftarrow \mathsf{Tag}_{k_a}(n, m)$	$c \leftarrow \mathsf{Enc}_{k_e}(n, m)$	$c \leftarrow \mathsf{Enc}_{k_e}(n, m)$
$c \leftarrow \mathsf{Enc}_{k_e}(n, m\|t)$	$t \leftarrow \mathsf{Tag}_{k_a}(n, c)$	$t \leftarrow \mathsf{Tag}_{k_a}(n, m)$
return c	**return** $c\|t$	**return** $c\|t$

Figure 2: Generic composition without nonce authentication

3. ⋆ Consider Encrypt-then-Mac without nonce authentication (middle of Figure 2). Define decryption for this mode. Think about how you determine the validity of ciphertexts.

$\mathrm{Dec}^{n}_{K_a,K_e}(c\|t)$

$t' \leftarrow \mathrm{Tag}_{K_a}(c)$
if $t \neq t'$:
 return $\perp$
$m \leftarrow \mathrm{Dec}_{K_e}(n, c)$
return m

can't compute tag directly, but can verify

if $\mathrm{Vfy}_{K_a}(c, t) == \perp$:
 return $\perp$

4. ⋆⋆ Consider a valid nonce–ciphertext pair (n^*, c^*). Find another valid nonce–ciphertext pair.

(x, c^*), where x is any item in $\mathcal{N}$ (i.e. a valid nonce)
This works because the tag doesn't depend on the nonce, so as long as it's the same ciphertext, the same tag will be output.

$(x \neq n^*)$

5. ⋆⋆ What can you conclude about the security of the Encrypt-then-Mac without nonce authentication (middle of Figure 2) as an authenticated encryption scheme?

It is not AE-secure: an adversary can encrypt a message m with a random nonce:

$$m \xleftarrow{\$} \mathcal{M}$$
$$n \xleftarrow{\$} \mathcal{N}$$
$$c \| t \xleftarrow{\$} \mathcal{E}(n, m)$$

Then, the adversary attempts to decrypt the resulting ciphertext, using a new random nonce:

$$n' \xleftarrow{\$} \mathcal{N} \quad \text{(repeat until } n \neq n'\text{)}$$
$$m \xleftarrow{\$} \mathcal{D}(n', c).$$

Note that this is a valid use of $\mathcal{D}(\cdot,\cdot)$, since c was not output by $\mathcal{E}(n', c)$.

Then the adversary returns whether they succeeded:

return $m = \perp$.

In the real world, decryption will never fail, so

$$\Pr[\mathrm{Exp}^{\text{ae-real}}_{\mathrm{Enc}}(A) : \hat{b} = 1] = 1.$$

In the ideal world, decryption always fails, so

$$\Pr[\mathrm{Exp}^{\text{ae-ideal}}_{\mathrm{Enc}}(A) : \hat{b} = 1] = 0.$$

Thus $\mathrm{Adv}(A) = 1$.

6. ⋆⋆⋆ Prove that Encrypt-then-Mac without nonce authentication (middle of Figure 2) is nonce-based indistinguishable from random if the encryption scheme it uses is nonce-based indistinguishable from random. Make sure to make the (t, q, ϵ) parameters explicit in your final statement.

Will prove the contrapositive: if an adversary $\mathbb{A}$ achieves advantage $Adv(\mathbb{A})$ (running in time $\le t$ and making $\le q$ queries) against Encrypt-then-Mac, then it can achieve an equal or greater advantage against the encryption scheme used.

Let $\mathcal{E} = (Kg, Enc, Dec)$ be an encryption scheme.
Suppose $\mathbb{A}$ is an adversary against $\mathcal{E}$+M with $Adv(\mathbb{A}) > \varepsilon$, running in time t and making q queries.
Then define

Not sure how to simulate EtM such that it acts as real or ideal world in correct situations

$\underline{Exp_{\mathcal{E}}^{(n)\text{-ind}}(\mathbb{B}_{(n)\text{ind}})}$

$K^* \xleftarrow{\$} Kg$

$\hat{b} \leftarrow$

$\underline{\mathbb{B}_{(n)\text{ind}}^{\mathcal{E}_B(\cdot,\cdot)}}$

~~$K_a \xleftarrow{\$} Kg$~~ $t^* \xleftarrow{\$} T$

$\hat{b} \xleftarrow{\$} \mathbb{A}^{\mathcal{E}_A(\cdot,\cdot),\, \mathcal{D}_A(\cdot,\cdot)}$

$\underline{\mathcal{E}_A(n, m)}$

no repeat nonces

$c \xleftarrow{\$} \mathcal{E}_B(n, m)$

~~$t \leftarrow Tag_{K_a}(c)$~~

return $c \| t^*$

$\underline{\mathcal{D}_A(n, c\|t)}$

c not output by $\mathcal{E}_A(n, \cdot)$

~~$t' \leftarrow Tag_{K_a}(c)$~~

if $t \ne t^*$:

  return $\perp$

$m \leftarrow Dec_{K^*}(n, c)$

return m

can we do this?

Here $\mathbb{B}$ is in the real world if and only if $\mathbb{A}$ is in the real world. We can see this as follows:

- if $\mathbb{B}$ is in the real world:

  → $\mathcal{E}_B(n,m)$ will return ~~the~~ actual encryption $Enc^n_{k^*}(m)$. Then $\mathcal{E}_A$ will return that ciphertext, along with a valid tag. Note that the same tag is always used, but this is still technically a valid tag. This then mimics how the EtM encryption oracle would work.

  → . . .

- if $\mathbb{B}$ is in the ideal world, then $\mathcal{E}_B(n,m)$ will return a random ciphertext. This means $\mathcal{E}_A$ will return a random ciphertext paired with a correct tag for that ciphertext - seems to contradict what we'd expect from $\mathcal{E}_A$ in this case