COMS30023 / Cryptology

Problem Sheet 6 – Authenticated Encryption

Dr François Dupressoir[*]

2025/26

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.

Remark 1. 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.

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.
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.

2 Understanding AE (In)Security

Figure 2 shows *BAD VERSIONS* of all three generic composition modes where nonces are not authenticated. 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 into how leaving out nonce authentication affects the integrity of ciphertexts, and the overall security of the constructed encryption scheme.

[*] Based on notes by Dr. Martijn Stam, Dr David Bernhard and others

```
$\mathsf{Exp}^{\text{weak-ow-cca}}_{\textsc{Enc}}(\mathbb{A})$
    $k \leftarrow_\$ \mathsf{Kg}$
    $n^* \leftarrow_\$ \mathcal{N}$
    $m^* \leftarrow_\$ \mathcal{M}$
    $c^* \leftarrow \mathsf{Enc}^{n^*}_k(m^*)$
    $\widehat{m} \leftarrow_\$ \mathbb{A}^{\mathcal{D}(\cdot,\cdot)}(n^*, c^*)$

    $\mathcal{D}(n, c)$
        require $(n, c) \neq (n^*, c^*)$
        $m \leftarrow \mathsf{Dec}^n_k(c)$
        return $m$
```

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

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

```
$\textsc{MtE}^n_{k_a,k_e}(m)$
    $t \leftarrow \mathsf{Tag}_{k_a}(m)$
    $c \leftarrow \mathsf{Enc}_{k_e}(n, m \| t)$
    return $c$

$\textsc{EtM}^n_{k_a,k_e}(m)$
    $c \leftarrow \mathsf{Enc}_{k_e}(n, m)$
    $t \leftarrow \mathsf{Tag}_{k_a}(c)$
    return $c \| t$

$\textsc{E+M}^n_{k_a,k_e}(m)$
    $c \leftarrow \mathsf{Enc}_{k_e}(n, m)$
    $t \leftarrow \mathsf{Tag}_{k_a}(m)$
    return $c \| t$
```

Figure 2: *Bad* generic composition without nonce authentication

3. $\star$ 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, and remember to validate ciphertexts *as soon as you have all you need!*

4. $\star\star$ Consider a nonce–ciphertext pair (n^*, c^*) for which decryption is successful. Construct *another* nonce–ciphertext pair whose decryption will be successful.

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

6. $\star\star\star$ Ask ChatGPT to prove that Encrypt-then-Mac without nonce authentication (middle of Figure 2) is nonce-based indistinguishable from random (you may call this “IND$-CPA-secure”) if the encryption scheme it uses is nonce-based indistinguishable from random. Reproduce ChatGPT’s answer in your answers, and explain why it is wrong.

   You may find it useful to 1) know that the theorem you asked ChatGPT to prove is in fact false, and 2) try and understand why it is false. (Recall our definition of indistinguishability, and note that we assume nothing of the MAC in this question.)