Lecture 2 – Modes of Operation and Cryptographic Reductions

François Dupressoir

2023

We've seen how to build enciphering schemes that are perfectly secure. We've also seen that "perfectly secure" means both "insecure in practice" and "impractical" (a happy combination if you think about it!). We then considered another way of defining security for enciphering schemes, which allows keys to be reused and weaken the "perfect" requirement into a "computational" requirement, moving from "it should be impossible for an adversary to break this" to "it should be infeasible for a reasonable adversary to break this".

Let's now see how we can construct practical *encryption schemes* from those *blockciphers*, and how we can reason about the fact that the construction does not weaken security too much. As before, we'll define things somewhat formally, consider generic attacks to figure out the best we can hope for and define our objectives, then we'll get to work.

2.1 Nonce-Based Encryption

We have a building block which allows us to use a single, relatively short key, to encrypt multiple messages—as long as they fit in a block and are never repeated. We now take our final step towards the construction of an encryption primitive: we *use* blockciphers in structured ways to *encrypt* long messages while allowing repetitions. We do so by instead requiring that some public value called a *nonce* (number used only once) never be repeated instead—this is safer because the nonce can be entirely controlled by the cryptographic layer above, whereas plaintexts come from strange and unknown distributions—you might, for example, be hard-pressed to send three distinct messages from the set $\{Yes, No\}$.

Definition 2.1 (Nonce-Based Encryption Scheme)**.** A *nonce-based encryption scheme* E is a triple of algorithms $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, where Kg randomly generates a key $k \in \mathcal{K}$, Enc takes a key k, a nonce $n \in \mathcal{N}$, and a message $m \in \mathcal{M}$ to output ciphertext $c \leftarrow \mathsf{Enc}_k^n(m) \in \mathcal{C}$, and Dec takes a nonce n, a ciphertext $c \in \mathcal{C}$ and key k to output a purported message $m' \leftarrow \mathsf{Dec}_k^n(c)$.

E is said to be *correct* iff, for all $k \leftarrow_{\$} \mathsf{Kg}$, $n \in \mathcal{N}$, and $m \in \mathcal{M}$, $\mathsf{Dec}_k^n(\mathsf{Enc}_k^n(m)) = m$.

Definition 2.2 (Nonce-Based Indistinguishability)**.** Let E be a nonce-based encryption scheme. We define the *advantage of* $\mathbb{A}$ *in distinguishing* E *from random ciphertexts* as follows, where experiments $\mathsf{Exp}_E^{\text{(n)ind-real}}(\mathbb{A})$ and $\mathsf{Exp}_E^{\text{(n)ind-ideal}}(\mathbb{A})$ are defined in Figure 2.1.

$$\mathsf{Adv}_E^{\text{(n)ind}}(\mathbb{A}) = \Pr\left[\mathsf{Exp}_E^{\text{(n)ind-real}}(\mathbb{A}) : \widehat{b} = 1\right] - \Pr\left[\mathsf{Exp}_E^{\text{(n)ind-ideal}}(\mathbb{A}) : \widehat{b} = 1\right]$$

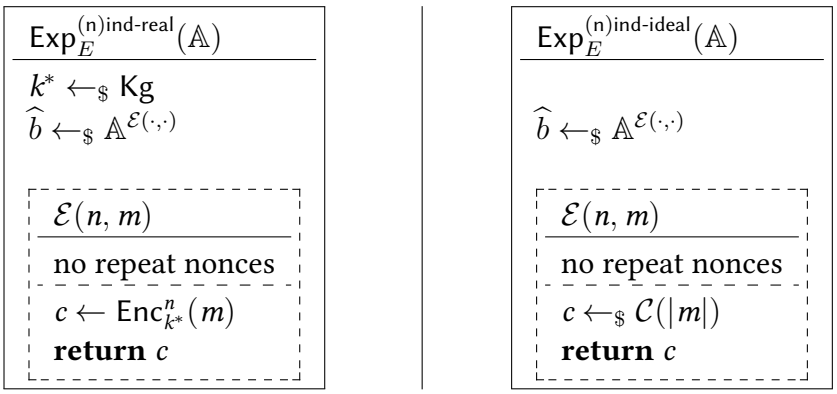

Figure 2.1: The real and ideal nonce-based indistinguishability experiments.

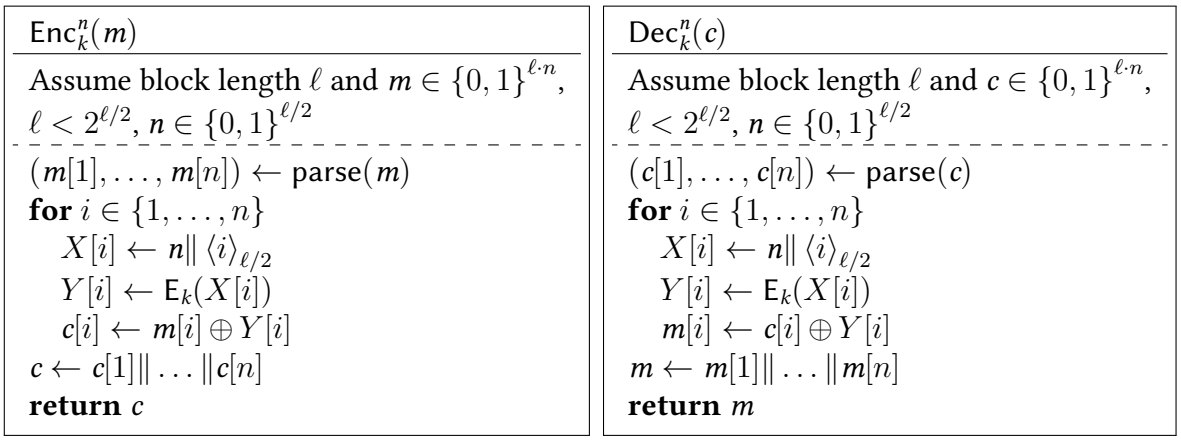

Figure 2.2: Nonce-Based Counter Mode (CTR) over a blockcipher $E = (\mathsf{Kg}, \mathsf{E}, \mathsf{D})$; key generation is that of the blockcipher

E is said to be a (t, q, ϵ)-*indistinguishable nonce-based encryption scheme* if, for every algorithm $\mathbb{A}$ running in time at most t and making at most q queries to its CPA oracle $\mathcal{E}(\cdot, \cdot)$, we have $\mathsf{Adv}^{\text{(n)ind}}_E(\mathbb{A}) \leq \epsilon$.

2.1.1 Modes of Operation

All that is left for us to do (before we can prove something useful) is to *generically* build nonce-based encryption from any blockcipher. This is done using a *mode of operation*.

Counter mode (or CTR), shown in Figure 2.2, is the most basic mode of operation given what we've already seen: use the blockcipher to expand the nonce into as many blocks of pseudorandom bits as needed, then use those as a one-time pad on the message.

It is nonce-based indistinguishable from random as long as the blockcipher it is constructed upon is pseudorandom. After a quick aside, we'll consider how to prove this.

Other Modes of Operation Other modes of operation exist. Some should not be used (Electronic Codebook, or ECB), some are so secure we can't even talk about their security

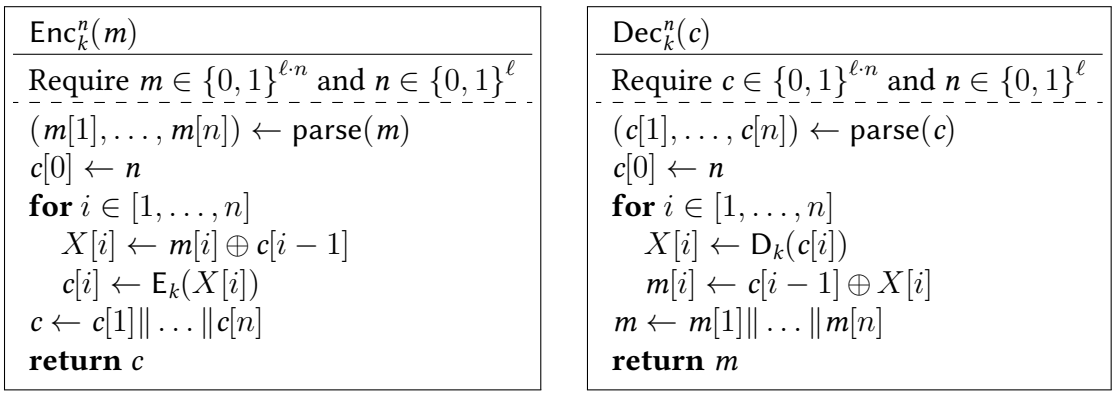

Figure 2.3: Cipher Block Chaining Mode (CBC) over a blockcipher $E = (\mathsf{Kg}, \mathsf{E}, \mathsf{D})$; key generation is that of the blockcipher

until later in the unit (GCM, OCB), others yet are not nonce-based secure, but are secure under some additional conditions on the nonce.

The most notorious of these—for having been used in TLS, and for being used in SSH—is Cipher Block Chaining mode (CBC), which is shown in Figure 2.3. We discuss it a bit in the problem sheet—mostly, again, destructively.

All those modes of operation—and more!—have their performance and use case advantages and drawbacks. Exploring all of them is not particularly useful for generalist cryptographers, although knowing that the variety exists is.

2.1.2 Reductions

Let's get back to CTR: how do we prove the earlier statement we made about its security—that if a blockcipher E is pseudorandom, then CTR over E is nonce-based secure?

Let's consider again the statement "if 'A' is secure against this, then 'B' is secure against that." Logically, this is equivalent to "if 'B' is not secure against that, then 'A' is not secure against this." By definition, not being secure corresponds to the existence of a successful adversary, so we can restate to "if there is a successful that-adversary against 'B', then there is a successful this-adversary against 'A'." Finally, we have arrived at a statement we can deal with constructively. We will assume the existence of some $\mathbb{A}_{\text{b,that}}$ and use it to construct an adversary $\mathbb{B}_{\text{a,this}}$ where we can relate the respective adversarial advantages.

We won't prove CTR secure just yet, but we'll illustrate the concept of a reduction by proving some relations between the one-time security notions we came across in Lecture 1. The relevant notions and their relations are summarized in Figure 2.4.

From strong to weak powers. To start, we keep the security goal the same and look at what happens when the adversary gets more or less power. This corresponds to the horizontal implications in Figure 2.4. Intuitively, more power should help an adversary, so security against "stronger" adversaries should imply security against "weaker" adversaries.

For this example, we will construct a reduction showing that (t, ϵ)-KR-1CPA security im-

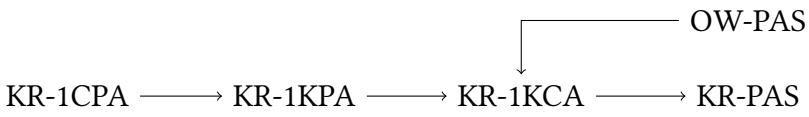

Figure 2.4: Relations between one-time security notions; arrows correspond to security implications (omitting those obtained by transitivity).

plies (t, ϵ)-KR-1KPA-security.[1] Recall the logic—so we can recall what we assume, and what we construct.

i. If E is (t, ϵ)-KR-1CPA secure then it is (t, ϵ)-KR-1KPA secure.

ii. If E is (t, ϵ)-KR-1KPA *insecure* then it is (t, ϵ)-KR-1CPA *insecure*

iii. If there exists a KR-1KPA adversary against E that runs in time at most t and wins with an advantage greater than ϵ, then there exists a KR-1CPAadversary against it that runs in time at most t and wins with an advantage greater than ϵ.

Thus, given a KR-1KPA adversary $\mathbb{A}_{\text{kr-1kpa}}$, we need to construct a KR-1CPA adversary $\mathbb{B}_{\text{kr-1cpa}}$ in such a way that:

1. $\mathbb{B}_{\text{kr-1cpa}}$ is (roughly) as efficient as $\mathbb{A}_{\text{kr-1kpa}}$; and
2. $\mathsf{Adv}^{\text{kr-1kpa}}_{E}(\mathbb{A}_{\text{kr-1kpa}}) \leq \mathsf{Adv}^{\text{kr-1cpa}}_{E}(\mathbb{B}_{\text{kr-1cpa}})$.

Here $\mathbb{B}_{\text{kr-1cpa}}$ is called the *reduction*, and the two claims relating to efficiency and advantage are the *analysis* of the reduction. Figure 2.5 shows the reduction (in the dashed box headed $\mathbb{B}_{\text{kr-1cpa}}$). We are now left to analyse its efficiency and advantage.

- $\mathbb{B}_{\text{kr-1cpa}}$ runs $\mathbb{A}_{\text{kr-1kpa}}$ once, with the only overhead being that of sampling a message when $\mathbb{A}_{\text{kr-1kpa}}$ makes an oracle query—so $\mathbb{B}_{\text{kr-1cpa}}$ runs (roughly) in time t if $\mathbb{A}_{\text{kr-1kpa}}$ runs in time t;
- $\mathbb{B}_{\text{kr-1cpa}}$ and $\mathbb{A}_{\text{kr-1kpa}}$ are facing experiments with the same challenge key k^*, and share also their key guess, so whenever one wins, the other does as well, and we have

$$\mathsf{Adv}^{\text{kr-1kpa}}_{E}(\mathbb{A}_{\text{kr-1kpa}}) = \mathsf{Adv}^{\text{kr-1cpa}}_{E}(\mathbb{B}_{\text{kr-1cpa}})$$

From hard to easy goals. The same way adversary capabilities can be ranked, there is a hierarchy of goals as well. Typically,[2] indistinguishability notions are strongest, key recovery is weakest, and one-wayness sits in the middle. We will prove that (t, ϵ)-OW-PAS security implies (t, ϵ)-KR-1KCA security using a reduction.

First, we figure out the logic of the reduction. We are given an adversary $\mathbb{A}_{\text{kr-1kca}}$ and need to create a reduction $\mathbb{B}_{\text{ow-pas}}$. The 'skin' of the reduction is shown in the left pane of Figure 2.6: $\mathbb{B}_{\text{ow-pas}}$ must simulate $\mathbb{A}_{\text{kr-1kca}}$'s one-time KCA oracle (which gives it a valid ciphertext under

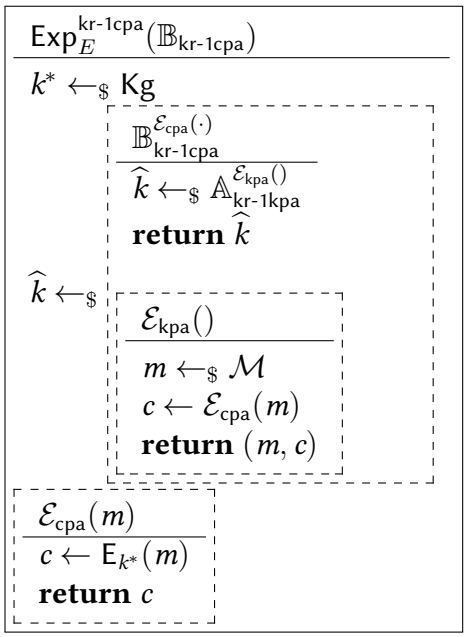

Figure 2.5: A reduction for KR-1CPA ⇒ KR-1KPA.

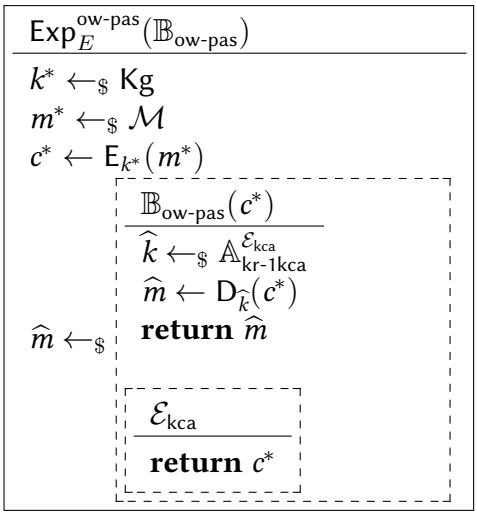

Figure 2.6: Reduction for OW-PAS ⇒ KR-1KCA.

the challenge key), and must somehow turn $\mathbb{A}_{\text{kr-1kca}}$'s output—a key guess—into a message guess.

The overall reduction is shown in Figure 2.6, and we can analyse it. Again, the running time of $\mathbb{B}_{\text{ow-pas}}$ is essentially that of $\mathbb{A}_{\text{kr-1kca}}$ as the overhead is minimal. Whenever $\mathbb{A}_{\text{kr-1kca}}$ wins by outputting the correct key, then $\mathbb{B}_{\text{ow-pas}}$ is guaranteed to win as well. Additionally, $\mathbb{B}_{\text{ow-pas}}$ might end up lucky even if $\mathbb{A}_{\text{kr-1kca}}$ doesn't return the correct key, so we have

$$\mathsf{Adv}_E^{\text{kr-1kca}}(\mathbb{A}_{\text{kr-1kca}}) \leq \mathsf{Adv}_E^{\text{ow-pas}}(\mathbb{B}_{\text{ow-pas}})$$

This is exactly what we needed to prove.

[1]Note the same t and ϵ; this is happy land.
[2]of those we discuss in this unit

Bibliography