Cryptography Part II: One-Time Pad

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read Chapter 2 of the course textbook by Katz and Lindell

Recall Slide 11 from Crypto I Lecture

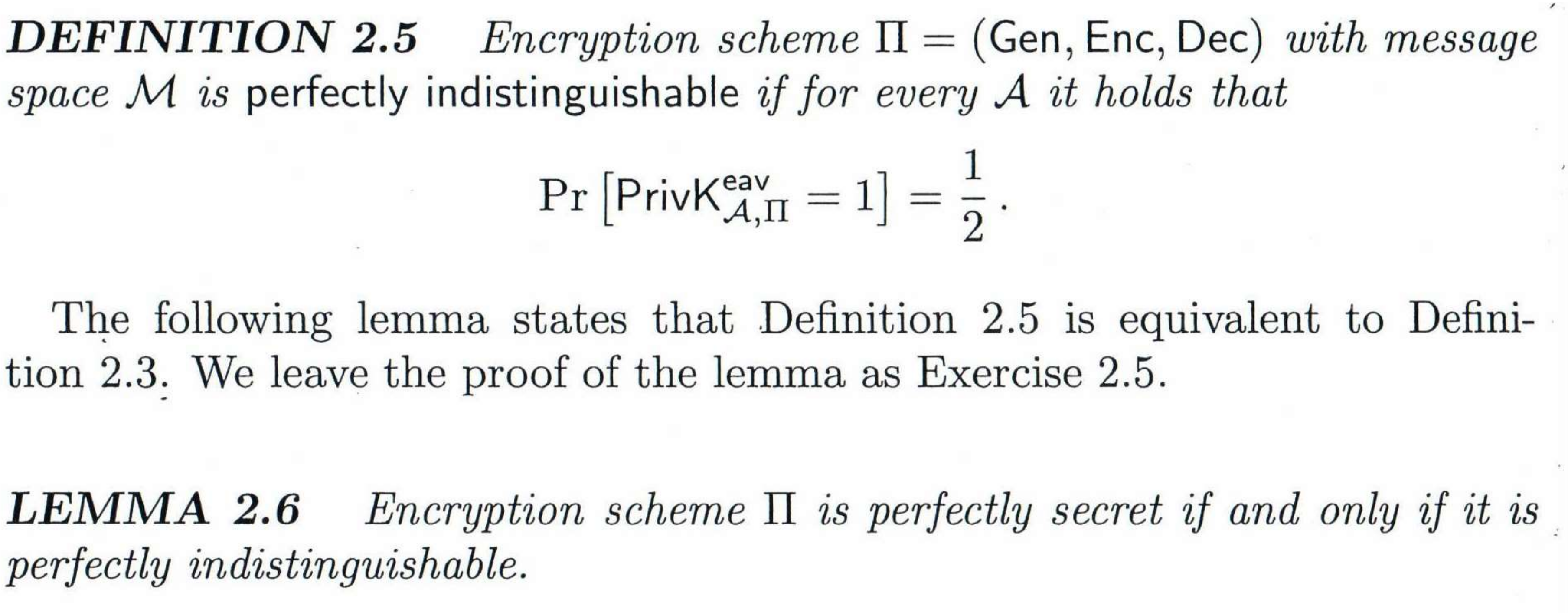
- M is a set of all possible messages, i.e., the message space
- C is a set of all possible ciphertexts, i.e., the ciphertext space
- *Gen* is a key generation procedure
  - The output of *Gen* is key k
  - *Gen* may or may not require an input

Now We Add the Following

- K is a set of all possible keys, i.e., the key space
- In the one-time pad, $|K| = |M| = |C| = \ell$

DEFINITION 2.3 *Encryption scheme* π = (Gen, Enc, Dec) *with message space* M *is* **perfectly secret** *if for every probability distribution over* M*, every message* $m \in M$*, and every ciphertext* $c \in C$ *for which* $\Pr\,[C = c] > 0$:

$$\Pr\,[M = m | c \in C] = \Pr\,[M = m\,].$$



DEFINITION 2.5 *Encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *is* perfectly indistinguishable *if for every* $\mathcal{A}$ *it holds that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}\,.$$

The following lemma states that Definition 2.5 is equivalent to Definition 2.3. We leave the proof of the lemma as Exercise 2.5.

LEMMA 2.6 *Encryption scheme* Π *is perfectly secret if and only if it is perfectly indistinguishable.*

Notation

- 1^n denotes 1 repeated *n* times, e.g., for *n* = 5 then we have that $1^n = 11111$
  - Note that in Professor Mooney's opinion sometimes Katz and Lindell use 1^n when *n* would have been just as clear (or even more clear!)
- b is a bit, i.e., it is possible that $b = 1$ or $b = 0$
- b' is a bit, i.e., it is possible that $b' = 1$ or $b' = 0$
  - Note that in Katz and Lindell the apostrophe $'$ does not signify complementation!
  - In other words, b' is just another variable such as $\tilde{b}$
  - As a result, it is possible to have both $b = 1$ and $b' = 1$
  - It is also possible to have both $b = 0$ and $b' = 0$

Formally, let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\mathcal{M}$. Let $\mathcal{A}$ be an adversary, which is formally just a (stateful) algorithm. We define an experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ as follows:

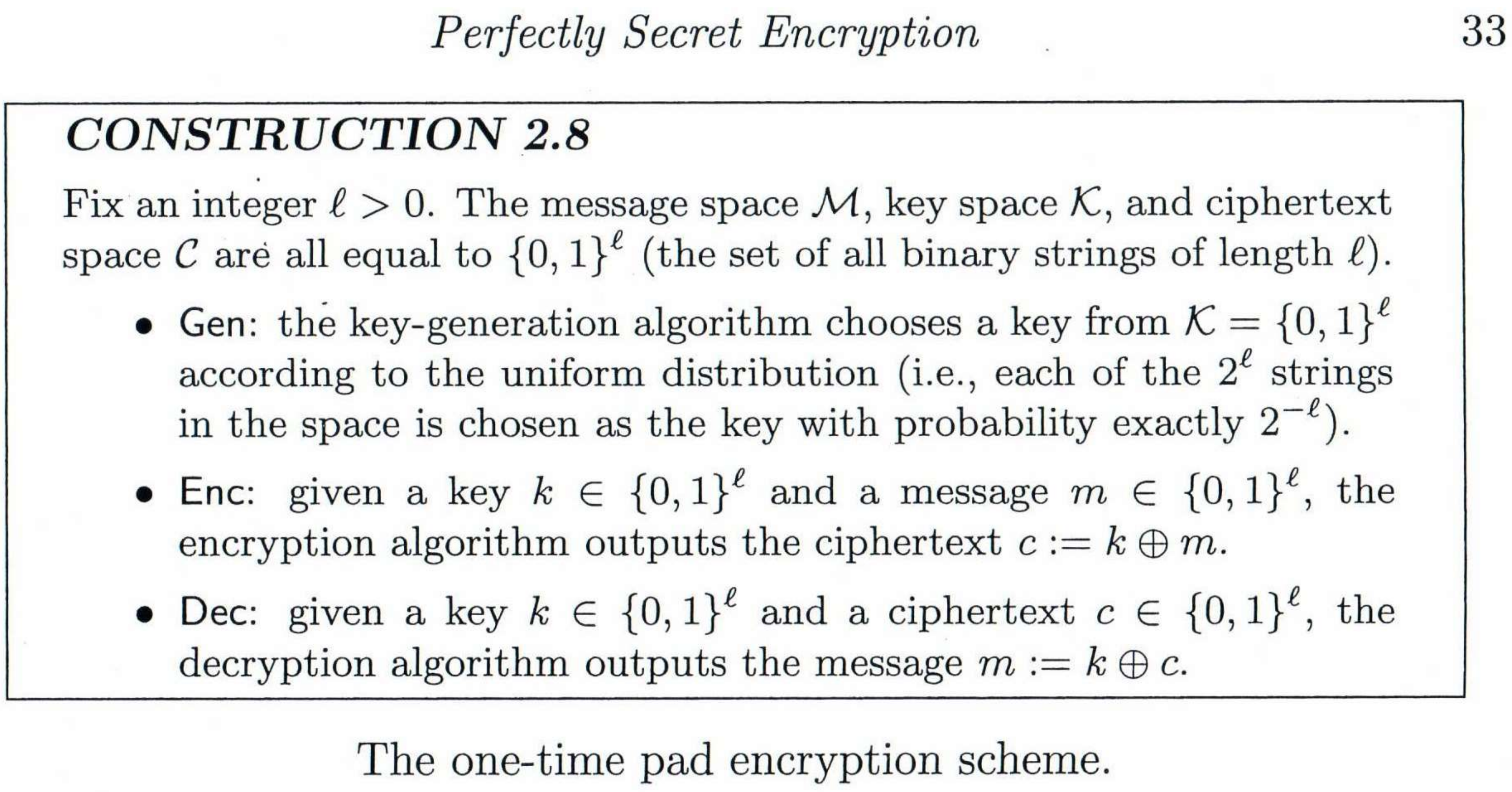
The adversarial indistinguishability experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$:

1. *The adversary $\mathcal{A}$ outputs a pair of messages $m_0, m_1 \in \mathcal{M}$.*
2. *A key k is generated using* Gen*, and a uniform bit $b \in \{0,1\}$ is chosen. Ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. We refer to c as the* challenge ciphertext.
3. *$\mathcal{A}$ outputs a bit b'.*
4. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1$ if the output of the experiment is 1 and in this case we say that $\mathcal{A}$* succeeds.

As noted earlier, it is trivial for $\mathcal{A}$ to succeed with probability $1/2$ by outputting a random guess. Perfect indistinguishability requires that it is impossible for any $\mathcal{A}$ to do better.

DEFINITION 2.5 *Encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is* perfectly indistinguishable *if for every $\mathcal{A}$ it holds that*

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}.$$



Perfectly Secret Encryption 33

CONSTRUCTION 2.8

Fix an integer $\ell > 0$. The message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^{\ell}$ (the set of all binary strings of length ℓ).

- Gen: the key-generation algorithm chooses a key from $\mathcal{K} = \{0,1\}^{\ell}$ according to the uniform distribution (i.e., each of the 2^{ℓ} strings in the space is chosen as the key with probability exactly $2^{-\ell}$).
- Enc: given a key $k \in \{0,1\}^{\ell}$ and a message $m \in \{0,1\}^{\ell}$, the encryption algorithm outputs the ciphertext $c := k \oplus m$.
- Dec: given a key $k \in \{0,1\}^{\ell}$ and a ciphertext $c \in \{0,1\}^{\ell}$, the decryption algorithm outputs the message $m := k \oplus c$.

The one-time pad encryption scheme.