Quantum Aspects of Cryptography

Assignment 3—Classical Cryptography Review
(topics from Lecture 5)

VER:α

Instructions. Same as those in previous assignments.

1. If your name is *Alice* and you're submitting answers to *Assignment 3*, use `Alice3.pdf` as your filename when submitting.

2. Submit your assignment using this OneDrive link for Assignment 3.

Please let me know if you spot a mistake or if something is unclear or feels suspicious.

Exercise 1 (Conceptual question about hiding the message)**.** Consider a one-time pad encryption which instead of the binary alphabet, uses the English alphabet and is defined for messages of length 5 (i.e. each message is a 5 letter string). For example, if $\mathsf{Gen}(1^n)$ returns a string like sk = 'AQDCR' and the message is m = 'BBBBB', then m is encrypted as a ciphertext c = 'BREDS' = $\mathsf{Enc}_{\mathsf{sk}}(m)$ (i.e. we treat letters 'A', 'B', 'C' ... as 0, 1, 2 ... and perform addition modulo 26). Call this scheme $\mathcal{S} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

Now since $\mathcal{S}$ is a one-time pad, Gen returns every 5 letter string with equal probability—including the string sk = 'AAAA'.

1. If the message m = 'HELLO' and sk = 'AAAA', what is the cipher text?

2. Consider a scheme $\mathcal{S}' = (\mathsf{Gen}', \mathsf{Enc}, \mathsf{Dec})$ where Gen' uniformly samples an element from the set of all 5 letter strings, excluding the string 'AAAA'. Is $\mathcal{S}'$ as secure $\mathcal{S}$? If yes, prove that $\mathcal{S}'$ satisfies semantic security. If not, prove that $\mathcal{S}'$ does not satisfy semantic security.

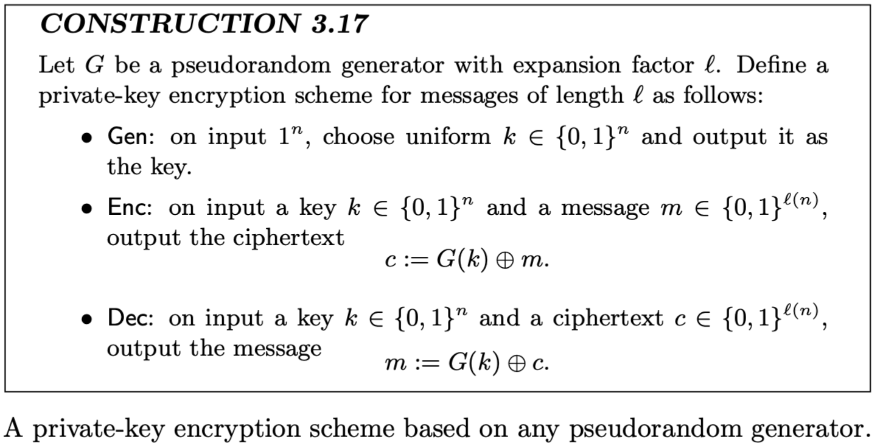
Exercise 2 (Basics about the One-Time Pad)**.** Recall the notation for the One-Time pad from class (or see Section 2.2, The One-Time Pad in [KL14]) where $\Pr[M = m]$ and $\Pr[C = c]$ were introduced to denote the probability that the message sent was m and the corresponding ciphertext used was m.

1. In class, we assumed that
$$\Pr[M = m | C = c] = \Pr[M = m] \tag{1}$$
is equivalent to
$$\Pr[C = c | M = m_0] = \Pr[C = c | M = m_1].$$
   (a) Try proving this yourself first and look at the text if needed.
   (b) In words, explain how you would interpret this result.

2. Suppose the One-Time Pad is used as a 'Two-Time Pad', i.e. suppose the same key is used to encrypt two different messages m_A and m_B. Suppose it is known that m_A and m_B are independently uniformly sampled to be 0 or 1.
   (a) Can Equation (1) hold in this case? Prove it either way.
   (b) What does your answer say about the security of the 'Two-Time Pad'?

3. Informally, we say an operation $\star$ can be implemented homomorphically if for any two messages, it holds that $m_1 \star m_2 = \mathsf{Dec}(\mathsf{Enc}(m_1) * \mathsf{Enc}(m_2))$ where $*$ is an operation acting on the ciphertexts and we suppressed the encryption/decryption keys from Enc and Dec.
   (a) Is there any non-trivial operation $\star$ that one can apply homomorphically using the one-time pad?
   (b) If so, what is the $*$ operation in your example?

Exercise 3. Towards computational security.



CONSTRUCTION 3.17

Let G be a pseudorandom generator with expansion factor ℓ. Define a private-key encryption scheme for messages of length ℓ as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it as the key.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^{\ell(n)}$, output the ciphertext
$$c := G(k) \oplus m.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{\ell(n)}$, output the message
$$m := G(k) \oplus c.$$

A private-key encryption scheme based on any pseudorandom generator.

Figure 1: Encryption scheme using a PRG. Taken from [KL14]

1. Can any encryption scheme on message space $\mathcal{M}$ be secure (against unbounded adversaries) if the key space $\mathcal{K}$ is smaller than the message space, i.e. if $|\mathcal{K}| < |\mathcal{M}|$? See Theorem 2.10 from [KL14] if you get stuck—but this should be quite straightforward to prove.

2. In view of the above, in class, we discussed two relaxations to our security requirement we started with for the one-time pad. What were these two relaxations? Define any new terms you use (semi-formal definitions are enough).

3. Recall the three security games formalising security against computationally bounded adversaries that we discussed in class:

   (a) Single ciphertext security, equivalently semantic security (IND; §3.2 [KL14])

   (b) Chosen Plaintext Security (IND-CPA; §3.4.2 [KL14])

   (c) Chosen Ciphertext Security (IND-CCA; §3.7.1 [KL14])

   Write these games down as we did in class—with the challenger on the (say) left and the adversary on the right. Also, briefly justify why each of these notions capture successively stronger notions of security.

Exercise 4 (IND secure encryption)**.** Consider the encryption scheme $\mathcal{S}$ in Figure 1.

1. How does [KL14] define a secure pseudorandom generator (with expansion factor ℓ)? What is the intuition behind the definition, i.e. what is this definition trying to capture?

2. Prove that if a G is a secure pseudorandom generator, then the scheme $\mathcal{S}$ satisfies semantic security (i.e. game (a) in Exercise 3). Try proving this yourself.

If needed, look at the proof in the book but understand it and write it in your words.

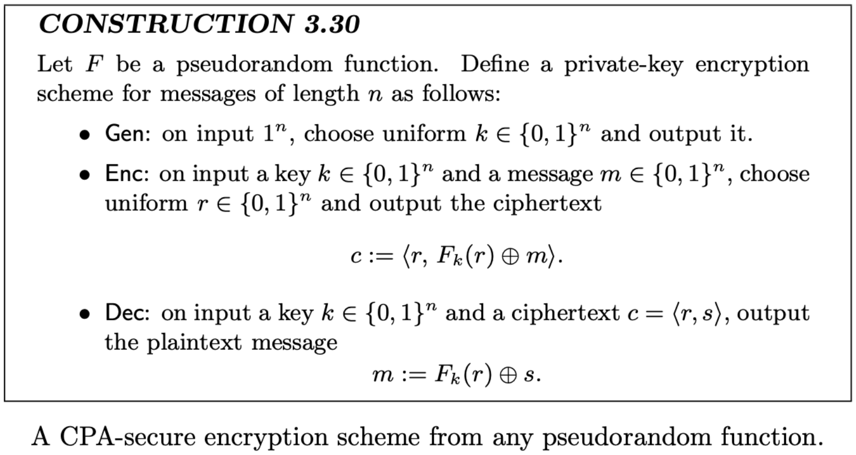
Exercise 5 (CPA secure encryption)**.** Same as the exercise above, except for CPA security. Consider the encryption scheme $\mathcal{S}$ in Figure 2.

1. How does [KL14] define a pseudorandom function? Again, what is the intuition behind the definition?

2. Prove that if F is satisfied the definition of a pseudorandom function, then the scheme discussed in class satisfies CPA security (i.e. game (b) in Exercise 3).

3. Suppose Enc samples the same r when invoked separately to encrypt messages m_1 and m_2. What does this observation say about the security of the scheme? Explain how your response here is consistent with your response to Exercise 2, question 2.

Exercise 6. Let us look at some basic consequences of how CPA and CCA security games are defined.



CONSTRUCTION 3.30

Let F be a pseudorandom function. Define a 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 plaintext message

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

A CPA-secure encryption scheme from any pseudorandom function.

Figure 2: CPA secure encryption scheme using

1. Consider an encryption scheme $\mathcal{S} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where $\mathsf{Gen}(1^\lambda)$ returns a random key sk but given the secret key sk, $\mathsf{Enc}_{\mathsf{sk}}$ is a determinist function. Suppose someone claims $\mathcal{S}$ is a CPA secure encryption scheme. Do you need more information to determine if their clam is valid? If not, why not?

2. Consider a variant $\mathcal{S}'$ of the scheme $\mathcal{S}$ in figure 2: $\mathcal{S}'$ is the same as $\mathcal{S}$ except that $\mathcal{S}'$ uses Enc'. The scheme $\mathcal{S}'$ is designed to be used as follows:

   (a) A single party uses Enc' and this party keeps a counter r' that is incremented every time a message is encrypted (starting from $r' = 0$).

   (b) Enc' is the same as Enc except that r' is used instead of r.

   (c) In the CPA security definition, assume that the 'encryption oracle' essentially asks this party to produce encryptions.

   Do you think this scheme is CPA secure, given the constraints above? Give a semi-formal proof of your conclusion. Explain how your answer is consistent with your answer to question 1 above.

3. Recall that in Exercise 2, question 3, we informally discussed what it means for an encryption scheme to be homomorphic. Suppose an encryption scheme satisfies the homomorphic property for $\star$ where $\star$ is an operation satisfying the following: there exists m_{zero} such that $m \star m_{\mathsf{zero}} = m$ for all messages m. Do you see any reason why such a scheme cannot satisfy CPA security? How about CCA security? If you claim that security is impossible in either case, prove it. Semi-formal reasoning suffices.

Exercise 7 (Basing cryptography on OWFs)**.** From [KL14], read the following sections. You can come and discuss with me if something is not clear.

- 7.1 (can skip 7.1.2).
  You should understand one-way functions (OWFs) and hard-core predicates

- 7.2.
  How OWFs can be used to extract randomness.

- 7.3 until 7.3.1; can skip the rest.
  Explains how constructing hardcore predicates is not easy and yet, there is a 'universal construction'

- 7.4 until 7.4.1; In 7.4.2, the full details can be skipped but try to understand the construction in Figure 7.1 and how security is proved using hybrid arguments
  Shows how to use OWFs to construct PRGs

- 7.5 (skim through the proof if you find it too easy)
  Shows how to use PRGs to construct PRFs

- 7.7. (ignore the parts that mention authentication; we have not yet looked at this in class yet)
  Shows how OWFs are the most basic primitive in classical cryptography

Based on your reading, answer the following questions

1. Formally define the following and explain what these objects are meant to represent, intuitively:
   (a) One-way function
   (b) Hard-core predicate
2. Is it known that for every one-way function, one can construct a hard-core predicate? What is the Goldreich-Levin theorem?
3. Give a construction for the following, along with a brief justification for why they work:
   (a) a PRG from a OWF; explain Figure 7.1 in the text
   (b) a PRF from a PRG; explain Figure 7.2 in the text.
4. Is a PRF not just a PRG with an expansion factor of $n \cdot 2^n$? Why do we need a separate construction for PRFs then?
5. Show that
   (a) a PRG implies a OWF exists.
   Do this formally, it is relatively simple.
   (b) an IND secure encryption scheme (where messages are twice as long as the key) implies a OWF exists.
   An informal argument here suffices.

References

[KL14] Jonathan Katz and Yehuda Lindell, *Introduction to modern cryptography, second edition*, 2nd ed., Chapman & Hall/CRC, 2014.