Quantum Aspects of Cryptography

Assignments 5, 6 and 7—Uncloneable Encryption
(topics from Lecture 9 to 15, or possibly even 16)
VERSION: $\alpha.1$—MARCH 5, 2025

Instructions. Same as those in previous assignments with *two changes.*

(i) Deadline flexibility. You can now take a total of 7 days past the due date over a given month (the month is determined based on when the assignment was given). These days can be distributed arbitrarily across the various assignments. You no longer need to seek permission in advance. Simply mark your submission day on the Google spreadsheet referred to below.

(ii) Grading. Most questions will now mostly involve reading, understanding and writing proofs/ideas in your words. Therefore some questions will carry much more weight, compared to others (e.g. I have written '10x' next to some questions; now even though we grade each question on a scale of 0 to 5, the points you get would be multiplied by this factor; so in the interval 0 to 50 in this example; by default, assume '1x').

The rest is unchanged.

1. If your name is *Alice* and you're submitting answers to *Assignment 5*, use `Alice5.pdf` as your filename when submitting.

2. Submit your assignment using the appropriate link below and add the submission date to this Google spreadsheet.[1]

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

[1] The system automatically adds a date-time stamp when you upload it to the OneDrive folder but I didn't want to spend time writing a script to fetch this data into Google sheets.

Assignment 5—UE basics

This is a simple but somewhat 'wordy' assignment.

- Submission link: OneDrive link for Assignment 5.
- Due: Thursday, **March 13**, 2025

Background reading

Exercise 1 (Random Oracle Methodology (**2x**))**.** The 'Random Oracle Methodology'. Read Section 5.5 from Ref [3]. Summarise the key points in your own words. In your summary, include

- the definition of a random oracle
- the relation between a random oracle and a one way function
- why the random oracle is used and why it is called a methodology or a heuristic.

Also briefly explain how this methodology extends to the quantum case.

Exercise 2 (Multiple encryptions and the hybrid argument (**3x**))**.** Section 11.2.2 Multiple Encryptions from Ref [3]. Summarise the key points in your own words. In your summary, please ensure you explain

- what an 'LR' oracle is,
- how it captures the notion of multiple encryptions, and
- how security of multiple encryptions follows from CPA security.

Exercise 3 (Conceptual understanding of uncloneable encryption)**.** Answer the following informally (you may refer to Section 1.4 of [1])

1. Explain the difference between uncloneable encryption and uncloneable indistinguishability.
2. Explain briefly, why coset states had to be introduced. What property of coset states are we using to build uncloneable encryption that BB84 states (equivalently Weisner encoding states) don't satisfy?

Exercise 4. State Theorem 2.1 in [1]. If you know that $\mathsf{TD}(|\phi_T\rangle, |\phi'_T\rangle) \geq \epsilon/2$, then what does Theorem 2.1 say about $\sum_{(i,y)\in F} W_y(|\phi_i\rangle)$?

Exercise 5. State and prove Lemma 2.3 and Corollary 2.4 in [1]. (Make sure your proof works for all relevant w, not just $w = 1/2$)

Example 6. Read Section 2.4 so that you understand Theorem 2.8 in [1]. State this theorem and explain, intuitively, what the theorem says. (It may help to look at the informal explanation right after Theorem 2.7)

Assignment 6—UE impossibility of deterministic schemes

- Submission link: OneDrive link for Assignment 6
- Due: Thursday, **March 20**, 2025

Exercise 7 (10x). Understand and write down the proof of Theorem 3.2 in [1] (Section 3). Formally state any statement you use (especially those you use without a proof) in your answer.

Exercise 8 (Coset States—basic properties)**.** Refer to Section 4 of [2] when necessary, and answer the following questions.

1. State the definition of a coset state and a subspace state.
2. Show that $H^{\otimes n} |A_{ss'}\rangle = |A^{\perp}_{s's}\rangle$.
3. Show that a coset state can be constructed efficiently.
4. State the definition of $\mathsf{Can}_A(\cdot)$ (as stated in [2]) and prove that it can be computed efficiently.

Assignment 7—UE construction in ROM

- Submission link: OneDrive link for Assignment 7
- Due: Thursday, **March 27**, 2025

Statements below are being referenced from [1].

Exercise 9. Answer the following.

1. Write down the formal definition of uncloneable indistiguishability (Definition 2.9 and 2.10).
2. Write down the uncloneable encryption scheme (in the random oracle model) in Section 5. Fill in the details about the decryption procedure.
3. Prove that this scheme does indeed satisfy uncloneable indistinguishability, assuming Theorem 4.8 is true. (**2x**)

Exercise 10. Understand and write down, in your own words, the following ingredients that go into the proof of Theorem 4.8

1. Write down the two hybrids (see page 26) diagrammatically, as we did in class
2. State and prove Lemma 4.9
3. State and prove Lemma 4.10
4. State and prove Lemma 4.11 (assuming Lemma 4.12) (**4x**)
5. State and prove Lemma 4.12 (**4x**)

References

[1] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. Cryptology ePrint Archive, Paper 2022/884, 2022.

[2] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography, 2022.

[3] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition.* Chapman & Hall/CRC, 2nd edition, 2014.