Quantum Aspects of Cryptography

Assignment 4—Certified Deletion
(topics from Lecture 4, 6, 7 and 8)

Instructions. Same as those in previous assignments.

1. If your name is *Alice* and you're submitting answers to *Assignment 4*, use `Alice4.pdf` as your filename when submitting.
2. Submit your assignment using this OneDrive link for Assignment 4.

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

Warm-up. Let us start with understanding a simple fact about public key encryption.

Exercise 1 (Public key encryption)**.** In class, we did not formally consider public key encryption. Let us remedy that.

i Look up, understand and write down the formal definition of public key encryption from [2] (Definition 11.1).

ii Semi-formally, argue that IND and IND-CPA (as defined in Exercise 3 of Assignment 3) are equivalent for public key encryptions

iii Can one construct a public key encryption scheme that is secure against unbounded adversaries? If so, give a construction. If not, give a proof.

Generality of the definition. Before we proceed, let us recall the definition of certified deletion.

Exercise 2 (Conceptual—definition of certified deletion)**.** Answer the following.

i *Formal Definition.* Write down the formal statement that we asserted corresponded to certified deletion in class (see Theorem 3.1 in Ref. [1]). Also explain the role $\mathcal{Z}$ plays in this definition.

ii *Intuition.* Explain why this definition captures the notion of certified deletion.

iii *Key leakage based definition.* Consider the following variant of the definition: the adversary does not become unbounded after producing a deletion certificate—instead, if the deletion certificate is valid, the adversary is given the secret key.

(a) Formalise this notion of security (try doing it yourself and if needed, look at Definition A.1, page 65 in Ref. [1])

(b) Can you show, semi-formally, that the notion of security we considered in class (i.e. in i above) is more general than the notion of security you just formalised? Did your response to Exercise 1 have anything to do with your proof?

Most general? The question above suggests that our definition is quite general. In the following, we try to understand whether there is any sense in which it could be generalised further.

Exercise 3 (Conceptual—definition of certified deletion, again)**.** In class we considered certified deletion in the context of public key encryptions. Instead, suppose Alice uses an information theoretically secure encryption scheme, e.g. a one-time pad, to encrypt her message.

i Does certified deletion make sense in this case? Why or why not?

ii Can you think of any notion of certified deletion that might make sense in this setting—where the encryption is already information theoretically secure? Hint: Exercise 2, *Key leakage based definition.*

Fill in the gaps. In class, we couldn't complete all the steps. The following ask you to fill in some of these gaps. Let us start with the following which we used to prove the XOR lemma.

Exercise 4 (Claim to prove the XOR lemma)**.** Prove Claim 2.3 from Ref. [1], i.e. for any $u \in \{0,1\}^n$ such that $\notin \{0^n, 1^n\}$, it holds that

$$\sum_{x:p(x)=0} (-1)^{u\cdot x} = \sum_{x:p(x)=1} (-1)^{u\cdot x} = 0.$$

Ref. [1] also give the proof so if you like, you can understand and write their proof in your own words.

In class, a question was raised about whether indistinguishability between ciphertexts for x and x' is the same as that between 0 and x.

Exercise 5 (A basic question about indistinguishability)**.** Consider the following two notions of security

i Indistinguishability among encryptions of x, x' for all x, x',

ii Indistinguishability among encryptions of $x, 0$ for all x.

Now,

- formalise these notions into ciphertext indistinguishability security games, and
- show that these two notions are equivalent.

In class, we argued that the theorem statement we proved corresponds to certified deletion but we stopped short of replacing $\mathcal{Z}$ with an encryption scheme to obtain an encryption scheme with certified deletion. Let us tie this loose end.

Exercise 6 (Compile any public key encryption scheme into one with certified deletion)**.** The following asks you to essentially compile any public-key encryption scheme, into one with certified deletion, using the theorem we proved in class (Theorem 3.1 [1]) .

i You know how certified deletion is formalised using $\mathcal{Z}$. You know the definition of public key encryption from Exercise 1. Now, try to formalise the notion of a public key encryption scheme with certified deletion. Compare your attempt with Definition 4.7 of [1].

ii Assume you have a public key encryption scheme given by $\mathcal{S} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Give a candidate encryption scheme $\mathcal{S}' := (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}', \mathsf{Del}, \mathsf{Ver})$ that uses $\mathcal{S}$ such that (i) it continues to be a public key encryption scheme, and (ii) also satisfies certified deletion, i.e. it satisfies Definition 4.7 of Ref. [1].

iii Semi-formally argue that your candidate scheme does indeed satisfy Definition 4.7 of Ref. [1].

Hint: You will have to use Theorem 3.1 in Ref. [1]—at least mortals among us would.

You are almost through, one last (real) question. In class, we skipped the step where we used the semantic security of $\mathcal{Z}$ to argue that Hyb_2' and Hyb_2 both result in outcome $\Pi_{x',\theta}$ with negligible probability. This last question asks you to complete this proof.

Exercise 7 (Using the semantic security of $\mathcal{Z}$)**.** Answer the following.

i From the premise of Theorem 3.1 in Ref. [1], write down what is meant by 'Semantic security of $\mathcal{Z}$ wrt to the first input, against $\mathcal{A}$'. Write it in terms of a game between a challenger and an adversary $\mathcal{A}$, with the challenger on the, say, right and the adversary on the left.

ii Write down Hyb_2 and Hyb_2' as we defined them in class.

iii Write down the definition of $\Pi_{x',\theta}$.

iv Prove Claim 3.4 in Ref. [1], i.e. for any $b \in \{0,1\}$, it holds that $\Pr[\Pi_{x',\theta}, \mathsf{Hyb}_2(b)] = \mathsf{negl}$, assuming (i) $\Pr[\Pi_{x',\theta}, \mathsf{Hyb}_2'(b)] = \mathsf{negl}$ and (ii) $\mathcal{Z}$ is semantically secure against $\mathcal{A}$ wrt to the first input (as you defined in i above).

Notes from class. This is not a real question—it essentially asks you to polish up and submit your class notes mostly spanning Lectures 7 and 8.

Exercise 8. Write down the formal proof of Theorem 3.1 in [1]—at least to the extent we discussed it in class. Give clear explanations for all the steps.

References

[1] James Bartusek and Dakshita Khurana. Cryptography with certified deletion, 2023.

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