Quantum Aspects of Cryptography

Midsem Exam

Saturday, March 1, 2025

Important Instructions.

1. Ground rules.
   (a) *Permitted.* As announced, you are allowed to carry one A4 sheet with handwritten notes (you may write on both sides) but nothing beyond that, to explicitly help you with your exam.
   (b) *Forbidden.* In particular, devices such as a tablet, phone etc. must not be used and no interaction with your peers is allowed. Please call me instead, should there be any confusion.
   (c) *Penalty.* You will immediately lose 50% of your points should any violation of these ground rules be observed. The second violation will cause you to lose all points for this exam.
   (d) *Duration.* Please try to finish your exam within an hour and a half. I will do my best to offer as much extra time as logistically possible.
2. Grading/points.
   (a) 5 points for Assignment Exercises (these are taken from your assignments)
   (b) 15 points for 'new' questions (these you have not seen before), distributed as
      i. 8 points for Certified Deletion
      ii. 7 points for Uncloneable Encryption

Note that all questions are *not* mandatory. Please look at these options carefully before starting. Please let me know if you spot a mistake or if something is unclear or feels suspicious. Good luck.

1 Review | Questions from the Assignment

Answer *either* Set A *or* Set B—doing both is redundant.

1.1 Set A

Quantum Review—Bit commitment. Here is semi-formal description of (a variant of) *bit-commitment*, in the classical setting. A bit-commitment protocol involves two parties Alice and Bob and it has two phases: the commit phase and the reveal phase.

In the commit phase, Alice chooses a bit $a \in \{0, 1\}$ and 'commits' to it by producing a string s_a and sending it to Bob. (Think of s_a as locking the answer in a safe and giving the safe—but not the combination—to Bob.)

In the reveal phase, Alice reveals the 'opening' r to the commitment s_a. Using (r, s_a) Bob can recover a (or output $\perp$ if the pair (r, s_a) is invalid). (Think of r as the combination to the safe.)

A bit commitment protocol must satisfy two properties:

1. Binding.
   Suppose both Alice and Bob follow the protocol honestly but Alice becomes malicious in the reveal phase.
   Alice should not be able to produce an opening r that opens to both $a = 0$ and $a = 1$.

2. Hiding.
   Suppose Alice follows the protocol honestly, but Bob is malicious.
   Bob should not be able to learn anything about the bit a from the commitment string s_a before the reveal phase starts.

Exercise 1 (3 points)**.** Suppose Alice and Bob have no bounds on their computational resources. Consider the following two cases:

1. Show that bit-commitment is impossible if both Alice and Bob are classical, i.e. both binding and hiding cannot simultaneously hold. You may argue as follows.
   (a) Suppose the scheme satisfies the binding property. Then for a given s_a, can there be any r that reveals $\neg a$ (instead of a)?
   What can you say about the relation between the set of possible strings sent by Alice when $a = 0$ and $a = 1$, i.e. $\{s_0\}$ and $\{s_1\}$ resp.?
   (b) Using your answer above, can you show that Bob can always learn b from s_b.
2. Show the same when they are both quantum by proceeding as follows.
   (a) Suppose Alice prepares a state $|\phi_b\rangle$ on registers AB and sends register B to Bob. Denote by ρ_b the reduced state on register B.
   (b) What does the hiding property say about the relation between ρ_0 and ρ_1?
   (c) What does Uhlman's theorem say about transforming purifications of a density matrix ρ? How are they related?
   (d) What does this observation say about the binding property of the commitment scheme?

Non-locality

Exercise 2 (2 points; Tsirelson bound)**.** Assume $x, y \in \{0, 1\}$ and $a, b \in \{\pm 1\}$. The CHSH expression is

$$I = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$$

where $\langle A_x B_y \rangle = \sum_{ab} abP(ab|xy)$. Show that according to quantum theory $I \leq 2\sqrt{2}$. This bound is known as the Tsirelson bound.

1.2 Set B

Crypto Review

Exercise 3 (2 points; 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 [2]) 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
$$m_1 \star m_2 = \mathsf{Dec}(\mathsf{Enc}(m_1) * \mathsf{Enc}(m_2)) \tag{2}$$
   where $*$ is an operation acting on the ciphertexts and we suppressed the encryption/decryption keys from Enc and Dec. *For this exercise, ignore* Dec *in 2 and answer the following.*
   (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?

Certified Deletion

Exercise 4 (3 points; 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.~~

2 Certified Deletion

The first question is rather conceptual but long (you may want to save it for the end). The second one simply asks you to complete one step of the proof that we did not cover in class. There are no options in this section.

Homomorphic Encryption. We quickly review homomorphic encryption, which basically allows one to compute on encrypted data. (If you're familiar with it, feel free to skip the box below).

Let Oprtns denote any set of quantum gates[a] that is universal. Informally, we say that a quantum encryption scheme is fully homomorphic, if for every operation $\star \in \mathsf{Oprtns}$ there is an efficient operation $*$ such that (2) holds (we suppressed the encryption/decryption keys in (2)). A bit more formally, a *Quantum Fully Homomorphic Encryption* (QFHE) scheme is specified by $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Eval}, \mathsf{Dec})$ where $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ behave as a public key encryption scheme.[b] Additionally, for every poly sized circuit f that takes $m_1 \dots m_k$ as inputs, there is a function $\tilde{f}$

$$\tilde{f}(\mathsf{Enc}_{\mathsf{pk}}(m_1), \mathsf{Enc}_{\mathsf{pk}}(m_2), \dots \mathsf{Enc}_{\mathsf{pk}}(m_k))$$

that (i) decrypts to $f(m_1 \dots m_k)$ under $\mathsf{Dec}_{\mathsf{sk}}$ and (ii) can be evaluated using only the public key pk efficiently as

$$\mathsf{Eval}_{\mathsf{pk}}(f, \mathsf{Enc}_{\mathsf{pk}}(m_1), \mathsf{Enc}_{\mathsf{pk}}(m_2), \dots \mathsf{Enc}_{\mathsf{pk}}(m_k))$$

where $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$.

[a] (i.e. unitaries acting on at most two qubits)

[b] Secret key fully homomorphic schemes can also be defined but let us stick to public key encryption for now.

A client can use homomorphic encryption to delegate a computation to a server. Of course, the client's message is hidden from the server as long as the underlying cryptographic assumption remains secure. The following question asks you to strengthen this guarantee—it asks you to use certified deletion to come up with a procedure that preserves the QFHE functionality and, after the encrypted answer is received, allows the client to verify that the prover has *information theoretically* deleted the client's information. It would help to remember that our definition of certified deletion only made sense for public key encryptions.

Question 1 (4 points)**.** *Let* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ *be a QFHE scheme as described above; assume* Eval *is unitary. Let* $\mathsf{Del}(\mathsf{ct})$ *and* $\mathsf{Ver}(\mathsf{ct}, \mathsf{cert})$ *denote the deletion and verification procedures for the certified deletion scheme, as discussed in class (where* ct *is the ciphertext and* cert *is the deletion certificate produced by* $\mathsf{Del}(\mathsf{ct})$*). Suppose the client wants to have the server apply a circuit* f *on its one-bit message* b *without revealing* b*. We model the server as follows:*

- *It computes everything correctly (it may perform additional operations that don't affect the computation).*
- *After the server sends its last message to the client, it tries to learn the client's input.*
- *And finally, the server is computationally bounded until it sends its last message—thereafter it becomes computationally unbounded.*

Let $\mathcal{S}$ *denote the set of such servers.*

To protect against such a server, the client uses the following schemes (encryption and decryption keys are implicitly taken to be produced by the key generation algorithm $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$*).*

i Sends a homomorphic encryption of $c = \mathsf{Enc}_{\mathsf{pk}}(b)$ *to the server. The server computes* $\mathsf{Eval}_{\mathsf{pk}}(f, \mathsf{Enc}_{\mathsf{pk}}(b))$ *and returns it to the client.*

ii Samples $(x,\theta) \leftarrow \{0,1\}^\lambda$, sends $\mathsf{ct} := \left(\ H^\theta \left|x\right\rangle_X, \mathsf{Enc}(\theta, b \oplus\ (\oplus_{i:\theta_i=0} x_i)\,)\ \right)$ to the server.
The server performs two steps:
(a) Function evaluation. It computes $\mathsf{Enc}(b)$ using Eval and the ciphertext ct sent by the client; similarly, it computes $\mathsf{Enc}(f(b))$ using Eval and $\mathsf{Enc}(b)$.
(b) Deletion Certificate. It obtains x' by measuring register X in the Hadamard basis.
The server returns $(\mathsf{Enc}(f(b)), x')$ to the server.
The client accepts

Given this, answer the following:

1. *Explain why the first scheme is insecure against servers in $\mathcal{S}$. (0.5 pt)*
2. *Explain what is wrong with the second scheme. (1 pts)*
3. *Give a candidate scheme that you think is correct, i.e. it allows the client to learn $\mathsf{Enc}(f(b))$ and leaks no information about b to any server in $\mathcal{S}$ (given the client accepts the deletion certificate). Your scheme may use multiple rounds of interaction between the client and the server. Give an informal analysis of its security. (2.5 pts)*
   Hint: Does it help if the client returns $\mathsf{Enc}(f(b))$ to the server, after recovering $f(b)$? Also, does it help that Eval is unitary?

The last step in the proof. Let x, x', y, u be n-bit strings. Let $H\left|y\right\rangle$ denote $H^{\otimes n}\left|y\right\rangle$. You may recall from the security analysis of certified deletion, that in the final argument, we asserted something akin to the following (without doing the proof in class):

Proposition 1. *Given a bipartite state on registers AX is of the form*

$$\left|\alpha\right\rangle_{AX} := \left|\phi_{x'}\right\rangle_A \otimes \sum_{y:\Delta(y,x')<\frac{n}{2}} H\left|y\right\rangle_X \tag{3}$$

(where recall $\Delta(a,b) = h(a \oplus b)$ and $h(s)$ is the relative Hamming weight of s), if register X is measured in the standard *basis and the outcome x is XORed into a bit $p = \oplus_i x_i$, the resulting state can be written as*

$$\sigma^{AP} = \mathsf{tr}_X(\left|\alpha\right\rangle\left\langle\alpha\right|_{AX}) \otimes \left(\frac{\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|}{2}\right)_P. \tag{4}$$

We said that Proposition 1 follows from Theorem 1 below.

Theorem 1. *Suppose a bipartite state $\left|\gamma\right\rangle_{AX}$ can be written in the following form*

$$\left|\gamma\right\rangle_{AX} := \sum_{u:h(u)<n/2} \left|\psi_u\right\rangle_A \otimes \left|u\right\rangle_X. \tag{5}$$

Now, if register X is measured in the Hadamard basis *to obtain x which is XORed into a bit $p = \oplus_i x_i$ then the resulting state can be written as*

$$\rho^{AP} = \mathsf{tr}_X(\left|\gamma\right\rangle\left\langle\gamma\right|_{AX}) \otimes \left(\frac{\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|}{2}\right)_P. \tag{6}$$

The question below gives you some hints and asks you to prove Proposition 1.

Question 2 (4 points)**.** *Prove the following intermediate statements to finally obtain a proof of Proposition 1.*

i Prove Proposition 1 for the case where $x' = 0$. (1 pt)

ii Let $\mathsf{CNOT}_{x'}\left|y\right\rangle = \left|y \oplus x'\right\rangle$. Prove that one can write

$$\left|\alpha'\right\rangle_{AX} := (\mathsf{CNOT}_{x'})_X H \left|\alpha\right\rangle_{AX}$$

in the form $\left|\gamma\right\rangle_{AX}$ as in Eq 5 for some choice of $\left|\psi_u\right\rangle$s. (1 pt)

iii Relate the probability amplitude of the following two procedures: (a) obtaining z when $\left|\alpha\right\rangle_{AX}$ is measured in the standard basis and (b) obtaining z when $\left|\alpha'\right\rangle_{AX}$ is measured in the Hadamard basis? (1 pt)

iv Use your answers so far to complete the proof of Proposition 1. (1 pts)

3 Uncloneable Encryption

3.1 3 pointer

Do *any one* of the following questions. You are expected to know the relevant definitions.

Question 3 (3 points)**.** *Prove the following by constructing explicit attacks.*

1. *A classical deterministic encryption scheme cannot be secure for multiple encryptions. (1 pt)*
2. *A classical encryption scheme cannot satisfy uncloneable IND. (1 pt)*
3. *Suppose S satisfies uncloneable IND for messages of 1 bit length. Show that the natural 2 bit extension of S (as discussed in class) cannot satisfy uncloneable IND. (1 pt)*

Question 4 (3 points)**.** *If yes, give a proof. If no, give an explicit construction and show that it violates the statement. In your answers, you may use the fact that the Broadbent Lord '20 scheme (recall it encrypts b as $H^\theta \left|x\right\rangle, b \oplus (\oplus_i x_i)$), satisfies uncloneability.*

1. *Does uncloneability imply semantic security? (1 pt)*
2. *Does uncloneable indistinguishability imply semantic security? (1 pt)*
3. *Does semantic security imply uncloneable indistinguishability? Does semantic security imply uncloneability? (1 pt)*

3.2 4 pointer

This is the last question and there are no options to choose from here.

Question 5 (4 points)**.** *We defined a 'deterministic scheme' in class and proved that there is a general attack. The following asks you to prove some of the steps that went into this result.*

i We used the following statement in that proof: Suppose $\left|\phi_1\right\rangle, \left|\phi_0\right\rangle$ are states on λ qubits. Let $\alpha := \langle\phi_1|\phi_0\rangle$. Prove that

$$\mathbb{E}_{\left|\phi_1\right\rangle \leftarrow \mu_n}\left(|\alpha|^2\right) = \frac{1}{2^\lambda}$$

where μ_n is the uniform spherical measure. (1 pt)

ii What we really wanted to use, was

$$\mathbb{E}_{\left|\phi_1\right\rangle \leftarrow \mu_n}\left(|\alpha|\right) = \mathsf{negl}. \tag{7}$$

Prove this using your answer above and Lévy's lemma (stated below for your reference). You may assume that for $f(\left|\psi\right\rangle) := \left|\langle\psi|\phi_0\rangle\right|^2$, $\kappa = 2$ (as in Lévy's lemma) and it may help to use $\epsilon = \lambda 2^{-\lambda/2}$. (1 pt)

iii Using your results so far, establish the following:

$$\begin{aligned}\mathbb{E}_{\left|\phi_0\right\rangle, \left|\phi_1\right\rangle}\mathsf{TD}(\rho_0^B, \rho_1^B) &\leq \mathbb{E}_{\left|\phi_0\right\rangle, \left|\phi_0^\perp\right\rangle : \langle\phi_0|\phi_0^\perp\rangle = 0}\left[\frac{1}{2}\left\|\mathsf{tr}_C\left[\left|\phi_0\right\rangle\left\langle\phi_0\right| - \left|\phi_0^\perp\right\rangle\left\langle\phi_0^\perp\right|\right]\right\|_1\right] + \mathsf{negl}(\lambda) \\ &\leq \mathbb{E}_{\left|\phi_0\right\rangle, \left|\phi_1\right\rangle : \langle\phi_0|\phi_1\rangle = 0}\mathsf{TD}(\rho_0^B, \rho_1^B) + \mathsf{negl}(\lambda)\end{aligned}$$

where $\left|\phi_0\right\rangle$ and $\left|\phi_1\right\rangle$ are states on registers AB where each register corresponds to $\lambda/2$ qubits, and ρ_0^B and ρ_1^B are the respective reduced states. To establish the first inequality, expand $\left|\phi_1\right\rangle = \alpha\left|\phi_0\right\rangle + \sqrt{1-|\alpha|^2}\left|\phi_0^\perp\right\rangle$ and the triangle inequality, together with 7. (2 pt)

Lemma (Lévy's Lemma)**.** *Let f be a function from unit vectors on n qubits to $\mathbb{R}$ satisfying*

$$|f(\left|\phi\right\rangle) - f(\left|\psi\right\rangle)| \leq \kappa \left\|\left|\phi\right\rangle - \left|\psi\right\rangle\right\|_2$$

for some $\kappa > 0$. Then, there is a universal constant $\delta > 0$ such that for all $\epsilon > 0$,

$$\Pr_{\left|\psi\right\rangle \leftarrow \mu_n}\left[\left|f(\left|\psi\right\rangle) - \mathbb{E}_{\left|\phi\right\rangle - \mu_n}[f(\left|\phi\right\rangle)]\right| \geq \epsilon\right] \leq 3e^{\frac{-\delta\epsilon 2^n}{\kappa^2}}.$$

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.