Midsem | Answers sketched

Sunday, March 2, 2025 12:58 pm

§1 Exercise Questions

I am skipping these since we already had the occasion to discuss Assignment 1,
I already uploaded the hints for Assignment 2
and the remaining questions are either textbook (Katz and Lindell)
or just algebra that can be easily verified.

§2 Certified Deletion

Question 1

(1) Scheme (i) This scheme is trivially insecure because
the server can simply keep a copy of c
and when it becomes unbounded
it can recover the bit b.

(2) Scheme (ii) asserts in point (b) that
the Server obtains a deletion certificate
by measuring X in the Hadamard basis.

However, the scheme fails in general
because to recover $\mathrm{Enc}(b)$
from ct using Eval
(and then does further operations on $\mathrm{Enc}(b)$)
the state in register X can no longer be
guaranteed to be $H^\theta |x\rangle_X$
(in general, it could be arbitrarily entangled with
the remaining registers).
This in turn means that
the scheme is not even correct—it is unclear
how even an honest server could produce
a valid deletion certificate.

(* The last line was supposed to be "The client accepts if the deletion certificate is valid";
sorry about that—hope that was implicit enough)

(3) Here's one candidate scheme (there may be others but they must be properly justified—and may well merit a research paper).

Proceed as in Scheme (ii) until step (a).
After step (a), the client uses its secret key sk to recover $f(b)$ from $\mathrm{Enc}(f(b))$
Since $f(b)$ is classical, the client keeps a copy of this answer and then undoes the decryption step above.

<--- I did not explicitly say this
but f was assumed to be a function
i.e. for each input
there is a fixed output.
This is why $f(b)$ can be copied
it is just a (classical) bit.

Here's the crucial bit, the client now returns $\mathrm{Enc(f(b))}$ to the server.

The server undoes all its step (remember we assumed Eval is unitary)
and returns to the state where it is holding ct
as originally sent by the client.

Now, register X is in the state $H^\theta |x\rangle_X$
and so measuring it in Hadamard
indeed produces a valid deletion certificate.

Security of certified deletion ensures
all information about the message b
is deleted from the view of the server

and so the scheme stays secure
even against servers in S.

Correctness of $f(b)$ follows from the assumption that the server is honest in the "function evaluation" phase.

Question 2

(i) For $x' = 0$, the sum over y in Eq (3) is over y such that $h(y) < \frac{n}{2}$
and thus
$|\alpha\rangle_{AX}$ is exactly in the same form as
the premise of Theorem 1
which immediately gives the asserted result,
with $|\psi_u\rangle = |\phi_{x'}\rangle$ for all u (up to normalisation).

Pen 1
Pen 2
Pen 3
Pen 4

(ii)

$$(\mathrm{CNOT}_{x'})_X \quad H_X |\alpha\rangle_{AX}$$

$$= (\mathrm{CNOT}_{x'})_X \quad H_X \Big(|\phi_{x'}\rangle_A \otimes \sum_{y:\Delta(y,x') < \frac{n}{2}} H|y\rangle_X \Big)$$

$$= |\phi_{x'}\rangle_A \otimes \sum_{y : h(y \oplus x') < \frac{n}{2}} |y \oplus x'\rangle$$

$$= |\phi_{x'}\rangle_A \otimes \sum_{u : h(u) < \frac{n}{2}} |u\rangle$$

and this is in the required form with $|\psi_u\rangle = |\phi_{x'}\rangle \quad \forall u$
(up to normalisation).

(iii)

$$\langle z|_X \quad |\alpha\rangle_{AX} = |\phi_{x'}\rangle_A \otimes \langle z| \sum_{y:\Delta(y,x')<\frac{n}{2}} H_X|y\rangle$$

$$\langle z|_X H_X |\alpha'\rangle_{AX} = |\phi_{x'}\rangle_A \otimes \langle z| \sum_{y:\Delta(y,x')<\frac{n}{2}} H_X \,(\mathrm{NOT}_{x'}\, H_X \quad H_X |y\rangle$$

$$= |\phi_{x'}\rangle_A \otimes \langle z| \sum_{y:\Delta(y,x')<\frac{n}{2}} (Z_{x'} \quad H_X|y\rangle$$

$$= (-1)^{z \cdot x'} |\phi_{x'}\rangle_A \otimes \langle z| \sum_{y:\Delta(y,x')<\frac{n}{2}} H_X|y\rangle$$

These are same upto a global phase.

Thus, the distribution over z in both cases is identical.

(iv) Using (ii) one can apply Theorem 1 & ensure the parity of z (when the X register of $|\alpha'\rangle_{AX}$ is measured in the Hadamard basis) is uniform & independent of register A.

Using (iii) one sees the distribution over z when produced by measuring X of
(a) $|\alpha'\rangle$ in Hadamard &
(b) $|\alpha\rangle$ in standard basis
is identical.

Thus parity of z as produced in (b) is also uniform & independent of A.

This is exactly what Eq (6) says, completing the proof.

§3 Uncloneable Encryption

§3.1 (3 pointers)

Question 3

(1) It suffices to give one deterministic scheme that is secure for encrypting once but not more.

Scheme: One-time pad

Attack: Given encryptions of m_1 and m_2 using the same key k,
i.e. given $\mathrm{ct}_1 = m_1 \oplus k$ and $\mathrm{ct}_2 = m_2 \oplus k$
one can XOR these ciphertexts to obtain $m_1 \oplus m_2$
which clearly leaks information about m_1, m_2
violating any reasonable notion of secrecy of
m_1 and m_2.

(2) Consider the following splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$

$\mathcal{A}$ gets a classical ciphertext ct and
sends ct to both $\mathcal{B}$ and $\mathcal{C}$ (this is possible because ct is classical and can be copied).
$\mathcal{B}$ and $\mathcal{C}$ later receive the secret key
using which they can both learn the message
and thereby simultaneously output which message was encrypted

They win the uncloneable IND game with probability 1.

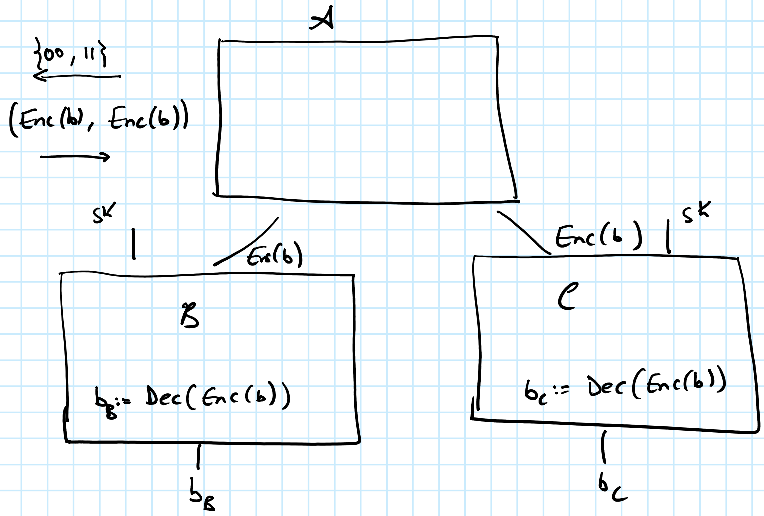
(3) Consider the following splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$

Let Enc, Dec denote encryption & decryption specified by S.

Challenger $\mathcal{A}$

Let Enc, Dec denote encryption & decryption specified by S.

Challenger



Clearly, $b_\mathcal{B} = b_\mathcal{C} = b$, i.e. $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the uncloneable-IND game w.p. 1.

Question 4.

(1) It suffices to consider a game that satisfies unclonability but not semantic security.

Consider the scheme by Broadbent and Lord:
it encrypts a message m as $(H^\theta|x\rangle, m \oplus x)$

It is known that it is not possible for both $\mathcal{B}, \mathcal{C}$ (where $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is a splitting adversary) to output m entirely,
i.e. it satisfies unclonability.

However, it is easy to construct an $\mathcal{A}'$ that breaks symantic security for this scheme.
$\mathcal{A}'$ can simply measure $H^\theta|x\rangle$ in a random basis (between standard and Hadamard, independently for each qubit) to obtain x'.

Clearly, x' will match x around 3/4ths the bits with overwhelming probability.
(1/2 because the basis was correct,
the other 1/2, will still be correct with probability 1/2)

Thus, $m \oplus x \oplus x'$ reveals around 3/4 of the bits of m
which violates semantic security.

For instance, the adversary could know in advance that
m is either all zeros or all ones,
and use the above procedure to determine which
of the two messages was encrypted by the challenger.

(2) Yes.
We show that if semantic security breaks
uncloneable IND also breaks.

Suppose $\mathcal{A}'$ breaks semantic security of the scheme.

Consider the following splitting adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ for the uncloneable IND game.

$\mathcal{A}$ proceeds as follows:

uses $\mathcal{A}'$ to send the message $\{m_0, m_1\}$ to the challanger $\mathcal{C}$ of uncloneable IND
gets ct as a response from $\mathcal{C}$
sends ct to $\mathcal{A}'$ and receives b.

Sends b to both $\mathcal{B}$ and $\mathcal{C}$ who simply output what they receive.

It is easy to see that $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ win with the same advantage against $\mathcal{C}$
as $\mathcal{A}'$ does against the challenger for semantic security.

NB: We did not assume that the scheme satisfying semantic security
produces classical ciphertexts—we did not assume anything can be cloned.

(3)

Semantic security does not imply uncloneable indistinguishability.

It suffices to consider any semantically secure scheme
and demonstrate that it does not satisfy uncloneable indistinguishability.

Take any classical encryption scheme that
satisfies semantic security (against efficient quantum adversaries).

We can now use the same attack as in
Question 3, part 2.

Semantic security does not imply uncloneability

Exactly the same, except that now $\mathcal{B}$ and $\mathcal{C}$
use the secret key to decrypt and
output the entire message.

§3.2 (4 pointer)

See Lecture Notes for Uncloneable Encryption
E.pdf, page 64

I attach the screenshots here for your convenience.

NB: For an arbitrary $|\phi_1\rangle$, given $|\phi_0\rangle$, one can write

$$|\phi_1\rangle = \alpha|\phi_0\rangle + \sqrt{1-|\alpha|^2}\,|\phi_0^\perp\rangle$$

phase absorbed

where $\alpha = \langle\phi_0|\phi_1\rangle$ & $\langle\phi_0|\phi_0^\perp\rangle = 0$.

$\therefore$ By symmetry, we have that

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

$(\because \sum |\alpha_i|^2 = 1 \Rightarrow \mathbb{E} \sum_i |\alpha_i|^2 = 1$
$\Rightarrow \sum_i (\mathbb{E}\, |\alpha_i|^2) = 1$

& by symmetry $\mathbb{E}\,|\alpha_i|^2 = \mathbb{E}\,|\alpha_j|^2 \;\forall\, i,j$

where α_i are the components along $\{|\phi_0^\perp\rangle, |\phi_0\rangle, \dots\}$

arbitrary but fixed vectors s.t.
the set is an orthonormal basis.

—64—

∴ Taking $\epsilon = \lambda 2^{-\frac{\lambda}{2}}$

$K = 2$

$f(|\psi\rangle) = |\langle\psi|\phi_0\rangle|^2$ in Lemma 3.4,

one can write down

$$\Pr_{|\phi_1\rangle \leftarrow \mu_n}\left[\left| |\alpha|^2 - \frac{1}{2^\lambda} \right| \geq \frac{\lambda}{2^{\lambda/2}}\right] \leq \underbrace{3e^{-\frac{\delta\lambda^2}{4}}}_{\text{TODO: check.}}$$

or $\mu_{\frac{\lambda}{2}}$ maybe.

∴ One can therefore derive that

$$\mathbb{E}_{|\phi_1\rangle \leftarrow \mu_n}\left[|\alpha|\right] \leq \underbrace{3\exp\left(-\frac{\delta\lambda^2}{4}\right)}_{\text{\& that } |\alpha|^2 > \frac{1}{2^\lambda}} \cdot \underbrace{1}_{\text{the contribution is still at most } 1} + \underbrace{1}_{\text{the remaining prob is at most } 1} \cdot \underbrace{\frac{\sqrt{\lambda}+1}{2^{\lambda/4}}}$$

$$= \text{negl}(\lambda)$$

given $|\alpha|^2 < \frac{\lambda}{2^{\lambda/2}} + \frac{1}{2^\lambda}$

$\Rightarrow |\alpha| \leq \sqrt{\frac{\lambda}{2^{\lambda/2}} + \frac{1}{2^\lambda}}$

$\leq \sqrt{\frac{\lambda}{2^{\lambda/2}}} + \sqrt{\frac{1}{2^\lambda}}$

NB2 : $\boxed{\mathbb{E}_{|\phi_0\rangle, |\phi_1\rangle} TD(\rho_0^\ell, \rho_1^\ell)}$ where $\rho_b = \text{tr}_C |\phi_b\rangle\langle\phi_b|^{\otimes \ell}$ $b \in \{0,1\}$

$= \mathbb{E}_{|\phi_0\rangle|\phi_1\rangle} \left\| \text{tr}_C\left[|\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1|\right] \right\|_1$ by defn of ρ_b

(expand $|\phi_1\rangle = \alpha|\phi_0\rangle + \sqrt{1-|\alpha|^2}\, |\phi_0^\perp\rangle$ & substitute to get)

$$= \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle\ |\phi_0^\perp\rangle \\ \langle\phi_0|\phi_1\rangle = 0 \\ a}} \left[\frac{1}{2} \left\| \mathrm{tr}_c \left[(1-|a|^2) \left(|\phi_0\rangle\langle\phi_0| - |\phi_0^\perp\rangle\langle\phi_0^\perp| \right) - \sqrt{1-|a|^2} \left(a\,|\phi_0\rangle\langle\phi_0^\perp| + a^*\,|\phi_0^\perp\rangle\langle\phi_0| \right) \right] \right\|_1 \right]$$

(Me TODO check why it is ok to sample $|\phi_0^\perp\rangle \leftarrow \mu_n$ as well.)

$$\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle,\, |\phi_0^\perp\rangle \\ \langle\phi_0|\phi_0^\perp\rangle = 0}} \left[\frac{1}{2} \left\| \mathrm{tr}_c \left[|\phi_0\rangle\langle\phi_0| - |\phi_0^\perp\rangle\langle\phi_0^\perp| \right] \right\|_1 \right] + \underbrace{\mathop{\mathbb{E}}_{a} \left[|a| \right]}_{\leq}$$

(using the triangle inequality & neglecting smaller terms)

$$\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle,\, |\phi_1\rangle \\ \langle\phi_0|\phi_1\rangle = 0}} \left[\frac{1}{2} \left\| \mathrm{tr}_c \left[|\phi_0\rangle\langle\phi_0| - |\phi_1\rangle\langle\phi_1| \right] \right\|_1 \right] + \overbrace{\mathrm{negl}(\lambda)}$$

(variable renamed)

$$\boxed{\leq \mathop{\mathbb{E}}_{\substack{|\phi_0\rangle,\, |\phi_1\rangle \\ \langle\phi_0|\phi_1\rangle = 0}} \mathrm{TD}\left(\rho_0^B, \rho_1^B \right)}$$

This, establishes [*] on page 64
(and proceeding similarly for $\rho_0^c \rho_1^c$)