COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 11

1. **Coin flipping from bit commitment**

   (a) Alice and Bob use the following protocol:

Alice		**Bob**
$a \in_R \{0,1\}$	$\xrightarrow{\text{Commit to } a \text{ with the bit commitment scheme}}$	
$c := a \oplus b$	$\xleftarrow{b}$	$b \in_R \{0,1\}$
	$\xrightarrow{\text{Open to } a \text{ with the bit commitment scheme}}$	$c := a \oplus b$

   (b) We first consider a cheating Bob.
   If a cheating Bob can make $c = 0$ with probability $p > 1/2$ in the above coin flipping protocol, he can guess a with probability p after Alice commits, by setting a equal to the message he is going to send in the second phase. By ε_h-hiding of bit commitment, $p \le \frac{1}{2} + \varepsilon_h$.
   Similarly, if a cheating Bob can make $c + 0$ with probability $p < 1/2$ in the above coin flipping protocol, he can guess a with probability p after Alice commits, by setting $a = 1 - b$ (the opposite of the message he is going to send in the second phase). By ε_h-hiding of bit commitment, $1 - p \le \frac{1}{2} + \varepsilon_h$.
   Therefore, for a dishonest Bob, $\frac{1}{2} - \varepsilon_h \le \mathbf{Pr}[c = 0] \le \frac{1}{2} + \varepsilon_h$.
   Now let's consider a cheating Alice.
   If a cheating Alice can make $c = 0$ with probability $p > 1/2$ in the above coin flipping protocol, she can run the first phase of the protocol to send a (potentially dishonest) commitment. Then the probability that she can open it to 0 is at least $\mathbf{Pr}[c = 0 \,|\, b = 0]$, and the probability that she can open it to 1 is at least $\mathbf{Pr}[c = 0 \,|\, b = 1]$. By the ε_b-binding of the bit commitment, $\mathbf{Pr}[c = 0 \,|\, b = 0] + \mathbf{Pr}[c = 0 \,|\, b = 1] \le 1 + \varepsilon_b$, which means $2p \le 1 + \varepsilon_b$ since honest Bob chooses b uniformly at random.
   Similarly, if a cheating Alice can make $c = 0$ with probability $p < 1/2$ in the above coin flipping protocol, it means she can make $c = 1$ with probability $1 - p$ in the above coin flipping protocol. Using the same argument, we can show that $2(1 - p) \le 1 + \varepsilon_b$.
   Therefore, for a dishonest Bob, $\frac{1}{2} - \frac{1}{2}\varepsilon_b \le \mathbf{Pr}[c = 0] \le \frac{1}{2} + \frac{1}{2}\varepsilon_b$.
   So the maximum bias of the coin flipping protocol is $\max(\varepsilon_h, \frac{1}{2}\varepsilon_b)$.

2. **Different flavors of oblivious transfer** Below we provide constructions and intuitions on why the constructions are secure. For a formal proof, you need the ideal functionality in the secure function evaluation.

(a) The reduction is straight-forward: the sender sends $(b_0, b_1, 0, ..., 0)$ via 1-out-of-k OT, and the receiver picks $c \in \{0, 1\}$.

(b) Alice and Bob use the following protocol:

$$
\begin{array}{lcl}
\textbf{Alice} & & \textbf{Bob} \\
r_1 \in_R \{0,1\},\ e_1 := b_1 & \xrightarrow{[e_1 \mid r_1]_{\text{1-2-OT}}} & \text{if } c = 1,\ \text{pick } e_1,\ \text{else } r_1 \\
r_2 \in_R \{0,1\},\ e_2 := b_2 \oplus r_1 & \xrightarrow{[e_2 \mid r_2]_{\text{1-2-OT}}} & \text{if } c = 2,\ \text{pick } e_2,\ \text{else } r_2 \\
r_3 \in_R \{0,1\},\ e_3 := b_3 \oplus r_1 \oplus r_2 & \xrightarrow{[e_3 \mid r_3]_{\text{1-2-OT}}} & \text{if } c = 3,\ \text{pick } e_3,\ \text{else } r_3 \\
\vdots & \vdots & \vdots \\
e_k := b_k \oplus r_1 \oplus \cdots \oplus r_{k-1} & \xrightarrow{e_k} & b := e_c \oplus r_1 \oplus \cdots \oplus r_{c-1}
\end{array}
$$

Alice trivially does not learn any information about Bob's choice $c \in \{1, ..., k\}$ because of the guarantee of each 1-out-of-2 OT. If Bob wishes to learn bit b_c, he needs to know all preceding one-time pads $r_1, \ldots, r_{c-1}$ as well as the value e_c. Hence, he cannot choose any of the values $e_1, \ldots, e_{c-1}$, and he has to choose the bit e_c. However, in that case he does not learn e_i for $i < c$, and thus learns no information about b_i for $i < c$, and moreover he does not learn r_c, and thus learns no information about b_i for $i > c$. Hence, even when Bob does not follow the protocol, he learns at most one of the k bits.

(c) Alice and Bob use the following protocol:

$$
\begin{array}{lcl}
\textbf{Alice} & & \textbf{Bob} \\
i \in_R \{0,1\} & & j \in_R \{0,1\} \\
b_i := b,\ b_{1-i} = 0 & \xrightarrow{[b_0 \mid b_1]_{\text{1-2-OT}}} & \text{pick } b_j \\
 & \xrightarrow{i} & \text{if } i = j, \text{ set } b := b_j, \text{ else set } b := \perp
\end{array}
$$

Alice does not learn any information about whether Bob receives the bit or not because Alice does not learn anything during the first phase by the guarantee of 1-out-of-2 OT, and Bob does not send anything to Alice in the second phase. Moreover, Bob receives the bit with probability 1/2 otherwise has no information about it because by the guarantee of 1-out-of-2 OT, Bob can learn only one of b_0, b_1.

(d) Let κ be a security parameter. Alice and Bob use the following protocol:

Alice		**Bob**
$r_1, \ldots, r_\kappa \in_R \{0,1\}$	$\xrightarrow{\forall i : [r_i]_{\text{Rabin-OT}}}$	$\forall\, i$: receive $r'_i \in \{r_i, \perp\}$
$t_0 := \bigoplus_{i \in T_0} r_i$, $t_1 := \bigoplus_{i \in T_1} r_i$	$\xleftarrow{T_0, T_1}$	$T_c := \{\, i \mid r'_i \neq \perp \,\}$ $T_{1-c} := \{\, i \mid r'_i = \perp \,\}$
$e_0 := t_0 \oplus b_0$, $e_1 := t_1 \oplus b_1$	$\xrightarrow{e_0, e_1}$	$t_c := \bigoplus_{i \in T_c} r'_i$, $b_c := e_c \oplus t_c$

Alice does not learn any information about Bob's choice $c \in \{1, \ldots, k\}$ since the sets T_0 and T_1 do not reveal which instances of the underlying Rabin OT were successful. Furthermore, with probability $1 - 2^{-\kappa}$ there is at least one bit r_i the receiver does not learn, and, therefore, at least one of the one-time pads t_0 and t_1 is uniformly random. Therefore, except with probability $2^{-\kappa}$, the receiver learns at most one of the bits b_0 and b_1.