Petros Wallden
Mina Doosti
Marine Demarty

Tutorial 6: Solutions

Problem 1

Consider the encryption defined using the secret key $k = a$ as follows. If the input state is $\rho_\psi = |\psi\rangle\langle\psi|$, then

$$\begin{aligned}\mathrm{Enc}_a(\rho_\psi) &= H^a \rho_\psi H^a \\ \mathrm{Dec}_a(\rho_\psi) &= H^a \rho_\psi H^a.\end{aligned}$$

(a) Check the encryption scheme satisfies correctness.

Solution. For correctness we need to check that $\mathrm{Dec}_k(\mathrm{Enc}_k(\rho_\psi)) = \rho_\psi$ for any input state ρ_ψ. In our case we have that

$$\mathrm{Dec}_a(\mathrm{Enc}_a(\rho_\psi)) = H^a(H^a \rho_\psi H^a)H^a = (H^2)^a \rho_\psi (H^2)^a = I\rho_\psi I = \rho_\psi.$$

(b) Which are the possible encryptions for the following two quantum states.

i. $|\psi_1\rangle = |0\rangle$.
Solution. The input state is $\rho_{\psi_1} = |0\rangle\langle 0|$. If $a = 0$ then $\mathrm{Enc}_a(\rho_{\psi_1}) = H^0 \rho_{\psi_1} H^0 = |0\rangle\langle 0|$. If $a = 1$ then $\mathrm{Enc}_a(\rho_{\psi_1}) = H^1 \rho_{\psi_1} H^1 = H\,|0\rangle\langle 0|\,H = |+\rangle\langle +|$.

ii. $|\psi_2\rangle = \frac{1}{\sqrt{1+(\sqrt{2}-1)^2}}\left(|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\right)$.
Solution. The input state is

$$\rho_{\psi_2} = \frac{1}{1+(\sqrt{2}-1)^2}\Big(|0\rangle + \Big(\sqrt{2}-1\Big)|1\rangle\Big)\Big(\langle 0| + \Big(\sqrt{2}-1\Big)\langle 1|\Big).$$

If $a = 0$ then $\mathrm{Enc}_a(\rho_{\psi_1}) = H^0 \rho_{\psi_2} H^0 = \rho_{\psi_2}$. For $a = 1$, first notice that $|\psi_2\rangle$ remains invariant when applying H. That is, $H\,|\psi_2\rangle = |\psi_2\rangle$. Thus, if $a = 1$ then $\mathrm{Enc}_a(\rho_{\psi_1}) = H^1 \rho_{\psi_1} H^1 = H\,|\psi_2\rangle\langle\psi_2|\,H = |\psi_2\rangle\,\langle\psi_2| = \rho_{\psi_2}$.

(c) What are the average ciphertexts $\rho_E(\psi_1)$ and $\rho_E(\psi_2)$?

Solution. The average ciphertexts can be written using part (b) as

$$\begin{aligned}\rho_E(\psi_1) &= \frac{1}{2}\sum_{a\in\{0,1\}} H^a \rho_{\psi_1} H^a = \frac{1}{2}(|0\rangle\langle 0| + |+\rangle\langle +|), \\ \rho_E(\psi_2) &= \frac{1}{2}\sum_{a\in\{0,1\}} H^a \rho_{\psi_2} H^a = \frac{1}{2}(\rho_{\psi_2} + \rho_{\psi_2}) = \rho_{\psi_2} = |\psi_2\rangle\langle\psi_2|\,.\end{aligned}$$

(d) Compute the fidelity of $\rho_E(\psi_1)$ and $\rho_E(\psi_2)$.

Solution. Because $\rho_E(\psi_2) = |\psi_2\rangle\langle\psi_2|$ is a pure state, we can use the simplified expression for fidelity in the case one of the states is pure.

$$
\begin{aligned}
& F(\rho_E(\psi_2), \rho_E(\psi_1)) \\
&= \langle\psi_2| \rho_E(\psi_1) |\psi_2\rangle = \frac{1}{2} \langle\psi_2| (|0\rangle\langle 0| + |+\rangle\langle +|) |\psi_2\rangle \\
&= \frac{1}{2+2\left(\sqrt{2}-1\right)^2}\Big(\langle 0| + \left(\sqrt{2}-1\right)\langle 1|\Big)\Big(|0\rangle\langle 0| + |+\rangle\langle +|\Big)\Big(|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\Big) \\
&= \frac{1}{4+4\left(\sqrt{2}-1\right)^2}\Big(\langle 0| + \left(\sqrt{2}-1\right)\langle 1|\Big)\Big(3|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\Big)\Big(|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\Big) \\
&= \frac{1}{4+4\left(\sqrt{2}-1\right)^2}\Big(3\langle 0| + \langle 1| + \left(\sqrt{2}-1\right)\langle 0| + \left(\sqrt{2}-1\right)\langle 1|\Big)\Big(|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\Big) \\
&= \frac{1}{4+4\left(\sqrt{2}-1\right)^2}\Big(3 + \left(\sqrt{2}-1\right) + \left(\sqrt{2}-1\right) + \left(\sqrt{2}-1\right)^2\Big) \\
&= \frac{1}{4+4\left(\sqrt{2}-1\right)^2}\cdot 4 = \frac{1}{4-2\sqrt{2}} \approx 0.854.
\end{aligned}
$$

(e) Using the bounds between fidelity and trace distance, argue whether the encryption is secure. In other words, do there exist any $|\psi_1\rangle \neq |\psi_2\rangle$ such that $\rho_E(\psi_1) = \rho_E(\psi_2)$?

Solution. Using the general inequalities relating fidelity and trace distance

$$1 - \sqrt{F(\rho,\sigma)} \le D(\rho,\sigma) \le \sqrt{1 - F(\rho,\sigma)},$$

we get in our case

$$0 < 0.076 \approx 1 - \frac{1}{\sqrt{4-2\sqrt{2}}} \le D(\rho_E(\psi_2), \rho_E(\psi_1)).$$

Therefore, the encryption is not information-theoretically secure, as we have two distinct input states for which the trace distance between their averaged quantum ciphertexts is strictly greater than 0. In particular, the above inequalities mean that someone can distinguish between the two cases with at least 0.076 advantage over a random guess.

Problem 2

Consider the Regev public-key cryptosystem with the parameters $q = 17$ and $n = 4$. The private key is defined as $s = (0, 13, 9, 11)$ and the public key is defined by $m = 4$ LWE samples

$$
\begin{gathered}
(a_1 = (14, 15, 5, 2), b_1 = 8), \\
(a_2 = (13, 14, 14, 6), b_2 = 16), \\
(a_3 = (6, 10, 13, 1), b_3 = 3), \\
(a_4 = (9, 5, 9, 6), b_4 = 9).
\end{gathered}
$$

(a) What is the encryption (a, c) for the message $\mu = 1$ if we pick the set $S = \{2, 4\}$?

Solution. To encrypt the message μ, we first compute

$$
\begin{aligned}
a &= \sum_{i\in S} a_i = a_2 + a_4 = (13, 14, 14, 6) + (9, 5, 9, 6) = (22, 19, 23, 12), \\
b &= \sum_{i\in S} b_i = b_2 + b_4 = 16 + 9 = 25.
\end{aligned}
$$

Now we take a and b modulo q and we get $a = (5, 2, 6, 12)$ and $b = 8$. Finally,

$$c = b + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor = 8 + 1 \cdot 8 = 16.$$

Therefore, the ciphertext is $\mathrm{Enc}(\mu) = (a, c) = ((5, 2, 6, 12), 16)$.

(b) Decrypt (a, c) to verify the correctness of the cryptosystem.

Solution. To decrypt $\mathrm{Enc}(\mu) = (a, c)$ using the secret key s we first compute

$$\langle a, s \rangle = 5 \cdot 0 + 2 \cdot 13 + 6 \cdot 9 + 12 \cdot 11 = 212.$$

Next, we compute

$$\begin{aligned} \langle a, s \rangle - c &\equiv 212 - 16 \pmod{q} \\ &\equiv 196 \pmod{q} \\ &\equiv 196 \pmod{17} \\ &\equiv 9 \pmod{17}. \end{aligned}$$

Finally, we observe that this quantity is closer to $\left\lfloor \frac{q}{2} \right\rfloor = 8$ than to 0, and so we conclude that $\mu = 1$.