Petros Wallden
Sean Thrasher
Laura Lewis

QCS 2024–25
March 14, 2025

Tutorial 6

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.

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

i. $|\psi_1\rangle = |0\rangle$.
ii. $|\psi_2\rangle = \frac{1}{\sqrt{1+(\sqrt{2}-1)^2}}\left(|0\rangle + \left(\sqrt{2}-1\right)|1\rangle\right)$.

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

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

(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 $\rho_E(\psi_1) = \rho_E(\psi_2)$?

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

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

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

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

Problem 3

Consider the trap-based quantum authentication scheme given in the lectures. Let the key shared between the parties be: The QOTP part $\vec{k} = (k_x^1, k_z^1, k_x^2, k_z^2, k_x^3, k_z^3) = (1, 0, 1, 1, 0, 1)$. The permutation part of the key is given by the permutation $\Pi(1) = 2$, $\Pi(2) = 3$, $\Pi(3) = 1$.

(a) Imagine that Bob receives the state $\rho = |+ - 0\rangle \langle + - 0|$. Check the verification algorithm and confirm that Bob accepts the message with certainty.

(b) Now check that the message $|+\rangle$ was the one that was given to Bob, by computing the Authentication algorithm on this state, with the shared key $\vec{k}$ and checking that it is consistent with the previous question.

(c) Now imagine that Bob receives the state $|0 - 0\rangle \langle 0 - 0|$ (can think of Eve having applied Hadamard at the first qubit after the Authentication). Check the verification algorithm and state with what probability will he accept.