Petros Wallden
Mina Doosti
Marine Demarty

Tutorial 6

QCS 2023–24
March 8, 2024

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

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

(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

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

(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.