Physical Security : Quantum

M2 Cybesecurity

Notations and basic operations
We recall that :

- $|+\rangle$ denotes the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle$, the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
- The Hadamard gate is the unitary operation that maps $|0\rangle$ to $|+\rangle$, and $|1\rangle$ to $|-\rangle$.

Exercise 1:
Consider four qubits in the state $|\varphi\rangle = \frac{1}{\sqrt{3}}(|1010\rangle + |1101\rangle - |0101\rangle)$.

1. What is the state $|\varphi_1\rangle$ obtained by applying a Hadamard gate to the first qubit of the system?
2. Given a system in the state $|\varphi_1\rangle$, what happens when we measure the last qubit in the standard basis (with $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$)? (Probability of each possible classical output and quantum four qubit state obtained.)
3. Let $|\varphi_2\rangle$ be the state of the system when the classical outcome of the previous measurement is 0, what happens if we measure the first qubit of the system in state $|\varphi_2\rangle$ in the diagonal basis (with $\{|+\rangle\langle +|, |-\rangle\langle -|\}$)?

Exercise 2:
We consider the following 2-player quantum game:

- (1) Alice prepares a qubit uniformly at random in one of the states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and sends it to Bob.
- (2) Bob chooses uniformly at random the standard ($\{|0\rangle, |1\rangle\}$) or the diagonal ($\{|+\rangle, |-\rangle\}$) basis. He announces his choice to Alice.
- (3) If the state sent by Alice is one of the states of the basis chosen by Bob, then Alice declares that Bob wins the game.

- (4) Otherwise, Alice announces the state she sent. Then Bob verifies Alice's announcement by measuring the qubit in the basis which contains the state announced by Alice. If his outcome corresponds to Alice's announcement, Bob declares that Alice wins the game. Otherwise, he detects a cheating and abort the game.

Example 1: Alice sends $|1\rangle$; Bob chooses the $\{|0\rangle, |1\rangle\}$-basis, he wins the game.
Example 2: Alice sends $|0\rangle$; Bob chooses the $\{|+\rangle, |-\rangle\}$-basis; Alice announces $|0\rangle$; Bob measures the qubit in the $\{|0\rangle, |1\rangle\}$-basis, he obtains 0 and Alice wins the game.

1. What is the probability for Bob to win the game if both players are honest (respect the protocol)?

2. Same question for Alice.

3. Notice that Bob cannot improve his winning probability by cheating during step (4). Can he improve his winning probability by cheating during step (2)? (Hint use the density matrices describing the two quantum states he wants to distinguish)

4. If Alice is cheating:

   4.1. Assume that Alice does step (1) honestly and starts cheating at step (2). What is her maximal probability of winning? What is the probability that her cheating is detected?

   4.2. Assume that Alice prepares the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one qubit to Bob. Explain how using a Hadamard gate on her qubit she can win with probability 1 with no risk of being detected.

Quantum information

P1: Pure quit state: normed vector in Hilbert space

One qubit state: $|\psi_1>=\alpha|0>+\beta|1>,\ |0>=\begin{pmatrix}1\\0\end{pmatrix},\ |1>=\begin{pmatrix}0\\1\end{pmatrix},\ |\alpha|^2+|\beta|^2=1$

In general:

$$|\psi>=\sum_{i\in\{0,1\}^n}\alpha_i|i> \qquad\qquad |||\psi>||=\sqrt{<\psi|\psi>}=\sqrt{\sum_{i\in\{0,1\}^n}\alpha_i^*\alpha_i}=1$$

P2: Composed systems: tensor product

$$|\psi>=|\psi_1>\otimes|\psi_2>$$

$|0_1 1_2>=|0>_1\otimes|1>_2$

Entangled: not a product, ex: $\frac{1}{\sqrt{2}}(\alpha|00>+\beta|11>)$

P3: Measurement : Probabilistic and irreversible

Measuring with $\{P_0,\ P_1\}$ such that $P_0+P_1=I$ and $P_iP_j=\delta_{i,j}P_i$

with probability $||P_i|\psi>||^2$ classical outcome i state after measure $\frac{P_i|\psi>}{||P_i|\psi>||}$

Example:

$|\psi>=\alpha|0>_1|\phi>+\beta|1>_1|\phi'>$ Measured with $\begin{matrix}P_0=|0><0|_1 & \text{projector over} & |0>\\ P_1=|1><1|_1 & \text{projector over} & |1>\end{matrix}$

with probability $p=|\alpha|^2\ c=0$ state after measure $|0>|\phi>$

with probability $p=|\beta|^2\ c=1$ state after measure $|1>|\phi'>$

P4:Unitary Evolution

$$U:|\psi>\mapsto U|\psi> \text{ with } U^\dagger U=I$$

Contact: **mehdi.mhalla@univ-grenoble-alpes.fr**

Mixed states

probabilistic distribution of states $\rho = \sum_i p_i |\psi_i >< \psi_i|$

General measurement

$\{M_i\}, \sum M_i M_i^\dagger = I$ $p_i = Tr(\rho M_i)$ state after measure $\frac{1}{p_i} M_i \rho M_i^\dagger$

Trace out

$$|a >< a'|_1 \otimes |b >< b'|_2 \otimes |c >< c'|_3 = |a >_1 |b >_2 |c >_3 < a'|_1 < b'|_2 < c'|_3$$
$$Tr_2 |a >_1 |b >_2 |c >_3 < a'|_1 < b'|_2 < c'|_3 = < b'|b > |a >_1 |c >_3 < a'|_1 < c'|_3$$

Purification

$|\psi >= \sum_i \sqrt{p_i} |i > |\psi_i >$

Fidelity

$F(\rho, |\psi >< \psi|) = \sqrt{< \psi|\rho|\psi >}$

Entropy

$S(\rho) = -Tr(\rho \log_2(\rho))$