Collaborators : None

Sources : Lecture Notes

Q3) Quantum Money Attacks

Among the 3 qubits, initialize the first 2 qubits to $|0\rangle$ & let the 3rd-qubit be qubit from original banknote to be counterfeited.

Let 3rd qubit, i.e, original banknote be $|\phi\rangle = a|0\rangle + b|1\rangle$ where $a^2+b^2=1$ → ①

As $|000\rangle \to \left[\frac{\sqrt{3}}{2}|000\rangle + \frac{1}{\sqrt{12}}|110\rangle + \frac{1}{\sqrt{12}}|101\rangle + \frac{1}{\sqrt{12}}|011\rangle\right]$

$|001\rangle \to \left[\frac{\sqrt{3}}{2}|111\rangle + \frac{1}{\sqrt{12}}|001\rangle + \frac{1}{\sqrt{12}}|010\rangle + \frac{1}{\sqrt{12}}|100\rangle\right]$

Let J.S. after the process be $|\psi\rangle$. Then, it transforms $(|00\rangle \otimes |\phi\rangle)$ to $|\psi\rangle$.

$\Rightarrow |00\phi\rangle \rightsquigarrow |\psi\rangle$

$\to [a|000\rangle + b|001\rangle] \rightsquigarrow |\psi\rangle$

$$\Rightarrow |\psi\rangle = a\left[\frac{\sqrt{3}}{2}|000\rangle + \frac{1}{\sqrt{12}}|110\rangle + \frac{1}{\sqrt{12}}|101\rangle + \frac{1}{\sqrt{12}}|011\rangle\right] + b\left[\frac{\sqrt{3}}{2}|111\rangle + \frac{1}{\sqrt{12}}|001\rangle + \frac{1}{\sqrt{12}}|010\rangle + \frac{1}{\sqrt{12}}|100\rangle\right]$$

$$|\psi\rangle = \left(\sqrt{\frac{5a^2+b^2}{6}}\right)|0\rangle \otimes \left[\frac{\frac{\sqrt{3}a}{2}|00\rangle + \frac{a}{\sqrt{12}}|11\rangle + \frac{b}{\sqrt{12}}|01\rangle + \frac{b}{\sqrt{12}}|10\rangle}{\left(\sqrt{\frac{5a^2+b^2}{6}}\right)}\right] +$$

$$\left(\sqrt{\frac{a^2+5b^2}{6}}\right)|1\rangle \otimes \left[\frac{\frac{a}{\sqrt{12}}|10\rangle + \frac{a}{\sqrt{12}}|01\rangle + \frac{\sqrt{3}b}{2}|11\rangle + \frac{b}{\sqrt{12}}|00\rangle}{\left(\sqrt{\frac{5b^2+a^2}{6}}\right)}\right]$$

After discarding 1st-qubit, the remaining qubits can be in state $\left[\frac{\frac{\sqrt{3}a}{2}|00\rangle + \frac{a}{\sqrt{12}}|11\rangle + \frac{b}{\sqrt{12}}|01\rangle + \frac{b}{\sqrt{12}}|10\rangle}{\left(\sqrt{\frac{5a^2+b^2}{6}}\right)}\right]$ with probability $\left(\frac{5a^2+b^2}{6}\right)$;

or state $\left[\frac{\frac{a}{\sqrt{12}}|10\rangle + \frac{a}{\sqrt{12}}|01\rangle + \frac{\sqrt{3}b}{2}|11\rangle + \frac{b}{\sqrt{12}}|00\rangle}{\left(\sqrt{\frac{5b^2+a^2}{6}}\right)}\right]$ with probability $\left(\frac{a^2+5b^2}{6}\right)$.

~~For the bank to~~ Let these states be $|P_1\rangle$ & $|P_2\rangle$.

For the bank to accept these qubits both, they have be $(|\phi\rangle \otimes |\phi\rangle)$ when measured in the basis corresponding to $|\phi\rangle$.

$\Rightarrow$ Probability [Measurement of 2-qubits $= |\phi\rangle \otimes |\phi\rangle$] =

Probability [2-qubits state $= |P_1\rangle$] $\times$ Probability [Measurement of $|P_1\rangle = |\phi\rangle \otimes |\phi\rangle$]

+ Probability [2-qubits state $= |P_2\rangle$] $\times$ Probability [Measurement of $|P_2\rangle = |\phi\rangle \otimes |\phi\rangle$]

$$= \left(\frac{5a^2+b^2}{6}\right) \times \left[\left\| \langle P_1 | (|\phi\rangle \otimes |\phi\rangle) \rangle \right\|^2\right] + \left(\frac{a^2+5b^2}{6}\right) \times \left[\left\| \langle P_2 | (|\phi\rangle \otimes |\phi\rangle) \rangle \right\|^2\right]$$

As $|\phi\rangle \otimes |\phi\rangle = (a|0\rangle \otimes b|1\rangle) \otimes (a|0\rangle + b|1\rangle) = (a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle)$

$$\Rightarrow Pr[\text{Success}] = \left(\frac{5a^2+b^2}{6}\right) \times \left[\frac{\frac{\sqrt{3}a^3}{2} + \frac{ab^2}{\sqrt{12}} + \frac{ab^2}{\sqrt{12}} + \frac{ab^2}{\sqrt{12}}}{\left(\sqrt{\frac{5a^2+b^2}{6}}\right)}\right]^2 +$$

$$\left(\frac{a^2+5b^2}{6}\right) \times \left[\frac{\frac{a^2b}{\sqrt{12}} + \frac{a^2b}{\sqrt{12}} + \frac{\sqrt{3}b^3}{2} + \frac{a^2b}{\sqrt{12}}}{\left(\sqrt{\frac{a^2+5b^2}{6}}\right)}\right]^2$$

$$= \left[\frac{\sqrt{3}}{2} a \left(a^2+b^2\right)\right]^2 + \left[\frac{\sqrt{3}}{2} b \left(a^2+b^2\right)\right]^2 = \frac{3}{4} \left(a^2+b^2\right)^3$$

As $(a^2+b^2) = 1 \Rightarrow$ $\boxed{Pr[\text{Success}] = \frac{3}{4}}$