Quantum one-time pad

- Task of encrypting a qubit.
- We may try to use the classical one-time pad
- Encrypt $|0\rangle$ and $|1\rangle$ just like classical

But what about $|+\rangle$?

$$X|+\rangle = |+\rangle$$

In this case whatever Key Alice and Bob share, the qubit is encrypted to itself. this is certainly not secure.

A quantum encryption scheme should hide information in all possible bases the qubit could be encoded in.

Say, we should be able encrypt a bit encoded in the Hadamard basis.

Not using X, but applying Z, since

$$Z|+\rangle = |-\rangle \quad \text{and} \quad Z|-\rangle = |+\rangle$$

What about other bases?

Same encryption scheme should work for all qubits.

Is it possible? Yes!

Alice $\xrightarrow{e}$ Bob

key K — key K

message ρ — $\rho = U(K)^\dagger e\, U(K)$

$e = U(K)\, \rho\, U(K)^\dagger$

How it works?

To flip in both bases (X and Z), we apply the unitary operator $X^{K_1} Z^{K_2}$, where $K_1, K_2 \in \{0,1\}$ are the two key bits chosen uniformly at random, with the choice of this encryption operation, an arbitrary single qubit is transformed to

$$\rho \to \frac{1}{4} \sum_{K_1, K_2 \in \{0,1\}} X^{K_1} Z^{K_2} \rho Z^{K_2} X^{K_1}$$

Verify this securely encrypts any single-qubit density matrix ρ.

Note: Pauli matrices pairwise anti commute $XZ = -ZX$.

Consider the Pauli matrix X.

$$\therefore \frac{1}{4}(X + XXX + ZXZ + XZXZX) = \frac{1}{4}(X + X - ZZX - XZZXX)$$

$$= \frac{1}{4}(X + X - X - X) = 0$$

(∵ Pauli matrices are Hermitian and square to identity.

Also, $\{X, Z\} = XZ + ZX = 0$).

Conclusion: If we apply either I, X, Z or XZ with equal probability to the Pauli matrix X, then we obtain 0.

Same applies to Y and Z.

$\therefore$ For any $M \in \{X, Y, Z\}$ we have

$$\frac{1}{4} \sum_{k_1, k_2 \in \{0,1\}} X^{k_1} Z^{k_2} M Z^{k_2} X^{k_1} = 0.$$

Any single qubit state can be written as

$$\rho = \frac{1}{2}\left(I + r_x X + r_y Y + r_z Z\right)$$

hence we have

$$\frac{1}{4} \sum_{k_1, k_2 \in \{0,1\}} X^{k_1} Z^{k_2} \rho Z^{k_2} X^{k_1} = \frac{I}{2} \quad \text{(Check!)}$$

This means that this message for anyone who does not know k_1, k_2 the bit and phase flipped state is completely independent of the input ρ, i.e. all information contained in ρ is hidden from the eavesdropper. Eve only sees $\frac{I}{2}$ independent of ρ.

Protocol: The key $k = (k_1, k_2)$ is chosen uniformly at random in $K = \{0,1\}^2$. To encrypt a qubit in state ρ, Alice applies the unitary operation $X^{k_1} Z^{k_2}$ to ρ. To decrypt, Bob applies the inverse operation $(X^{k_1} Z^{k_2})^\dagger = Z^{k_2} X^{k_1}$.

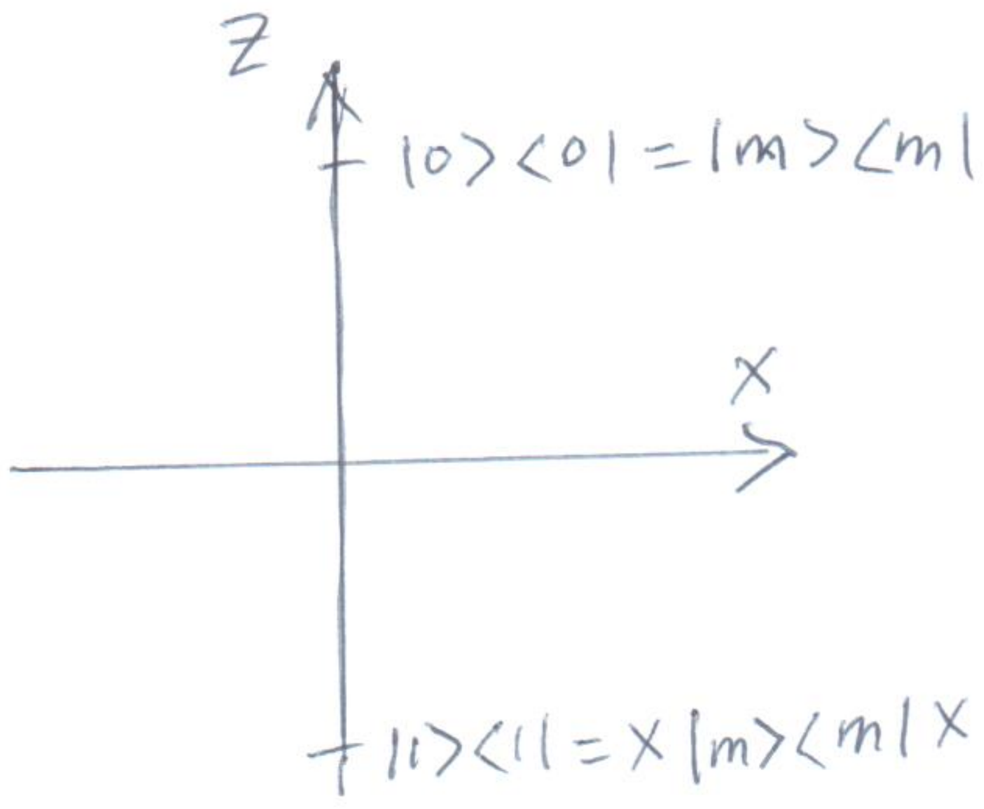
- This is correct.
- This is secure (as the encryption is completely independent of the message).
- Also, to encrypt n qubits, we use $2n$ bits of classical key.

It can be shown that this is optimal for a perfectly secure encryption.

Consider a single bit message $m \in \{0, 1\}$.
We can represent this by a pure quantum state $|m\rangle$
or the density matrix $|m\rangle\langle m|$.

By applying XOR, when $K=1$, m is flipped
when $K=0$, m is unchanged

i.e. when $K=1$, $|m\rangle \mapsto X|m\rangle$ (X = Pauli bit flip matrix)



Encryption implements the transformation

$|m\rangle\langle m| \longmapsto X|m\rangle\langle m|X$

classical one-time pad in the XZ plane of the Block sphere for $m=0$.

If Alice and Bob choose a uniformly random key bit K then the density matrix for the system KM (K contain the key, and M the message) is

$$\rho_{KM} = \frac{1}{2}|0\rangle\langle 0|_K \otimes |m\rangle\langle m|_M + \frac{1}{2}|1\rangle\langle 1|_K \otimes X|m\rangle\langle m|X_M$$

For Eve without any access to the system K containing the key, the density matrix is

$$\rho_M = \frac{1}{2}|m\rangle\langle m|_M + \frac{1}{2}X|m\rangle\langle m|X = \frac{I}{2}.$$

ρ_M does not depend on m. $\forall m$, $\rho_M = \frac{I}{2}$.

No information can be gained from interception.