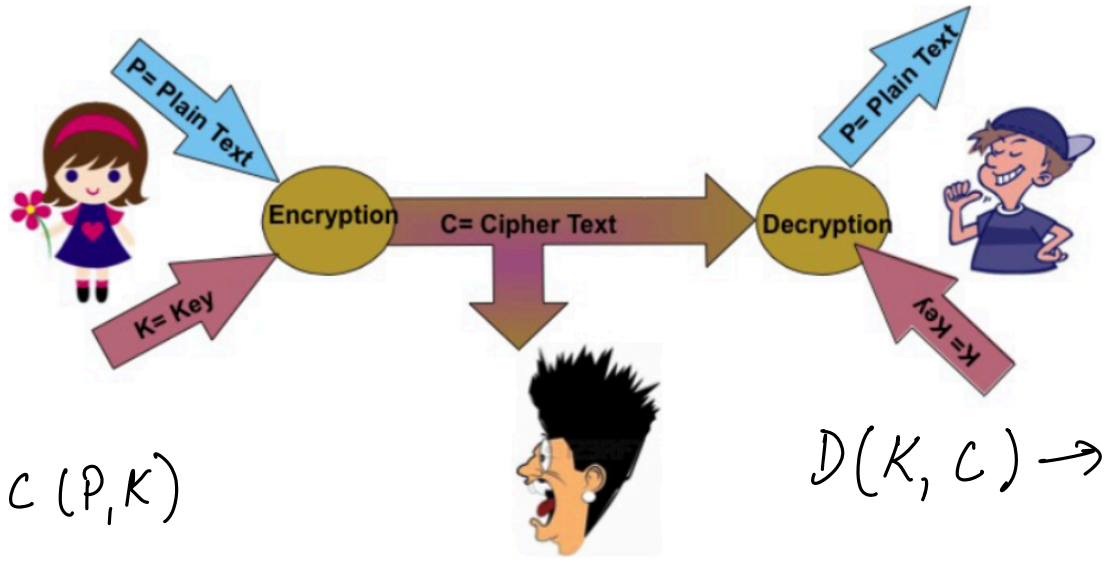
This lecture

- Quantum Characteristics
  - No cloning
  - Measurement
- BB84 Protocol

Perfect Secrecy and QKD

Symmetric Cryptography



$C(P, K)$

$D(K, C) \rightarrow P.$

One Time Pad (Vernam Cipher)

P = 0 1 1 0 1 0 0 1 0 1

K = 1 0 1 1 1 0 1 1 0 0

C = P ⊕ K

1 1 0 1 0 0 1 0 0 1

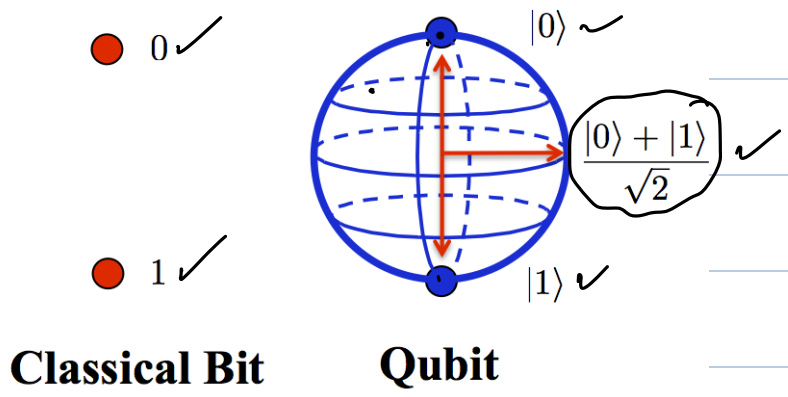
C is impossible to break iff

- K is as long as the message
- K is random
- K is used only once
- K is completely secret.

Quantum Key Distribution distributes Secure Key through Open Channel!!

QKD encoding key on quantum bits!!

Quantum Bit



$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

Measure:

$|0\rangle$ with probability $|\alpha|^2$

$|1\rangle$ with " $|\beta|^2$.

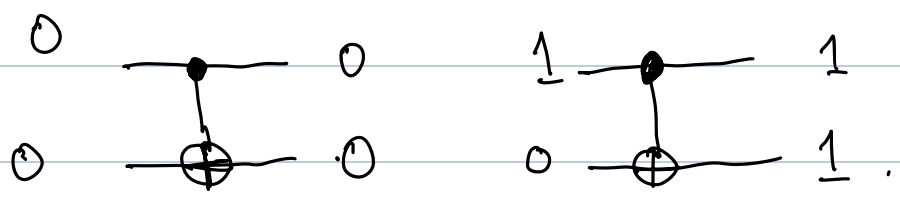
No-Cloning Theorem:

You cannot clone an unknown quantum state

making a copy

keeping original

Clone of an unknown classical state



Clone of an unknown quantum state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

$$|0\rangle|b\rangle|f\rangle \longrightarrow |0\rangle|0\rangle|f_0\rangle.$$

$$|1\rangle|b\rangle|f\rangle \longrightarrow |1\rangle|1\rangle|f_1\rangle.$$

$$(\alpha|0\rangle+\beta|1\rangle)|b\rangle|f\rangle \longrightarrow \alpha|0\rangle|b\rangle|f\rangle + \beta|1\rangle|b\rangle|f\rangle$$

$$\downarrow$$

$$\alpha|0\rangle|0\rangle|f_0\rangle + \beta|1\rangle|1\rangle|f_1\rangle.$$

What would be the clone of $|\psi\rangle$

$$(\alpha|0\rangle+\beta|1\rangle)|b\rangle|f\rangle \longrightarrow (\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle)|f'\rangle.$$

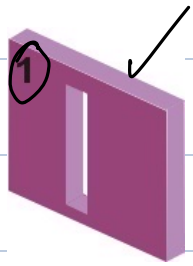
$$\alpha^2|0\rangle|0\rangle|f'\rangle + \beta^2|1\rangle|1\rangle f'$$
$$+\alpha\beta|0\rangle|1\rangle|f'\rangle + \alpha\beta|1\rangle|0\rangle|f'\rangle$$

One cannot make a clone of an unknown quantum state!

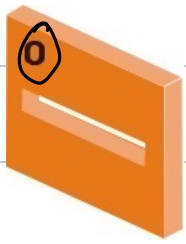
Measuring a quantum state:

Non-orthogonal quantum states

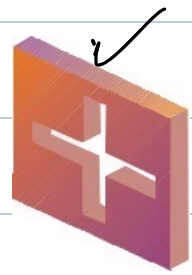
$|\uparrow\rangle \equiv |1\rangle \to 1$



$|\rightarrow\rangle \equiv |0\rangle \to 0$



H-V.

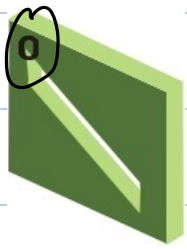


$\{|0\rangle, |1\rangle\}$.

$\langle 1|0\rangle = 0$
$\langle 0|1\rangle = 0$ } orthogonal.

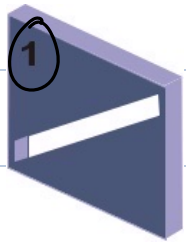
$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

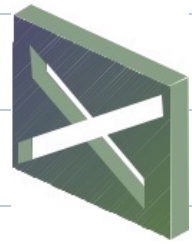
$|0\rangle \equiv 0$.



$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|-\rangle \equiv 1$





$\{|+\rangle, |-\rangle\}$.

orthogonal $\begin{cases} \langle +|-\rangle = \langle 0|0\rangle - \langle 1|1\rangle = 0 \\ \langle -|+\rangle = 0 \end{cases}$

$\langle +|0\rangle = \frac{1}{\sqrt{2}}$

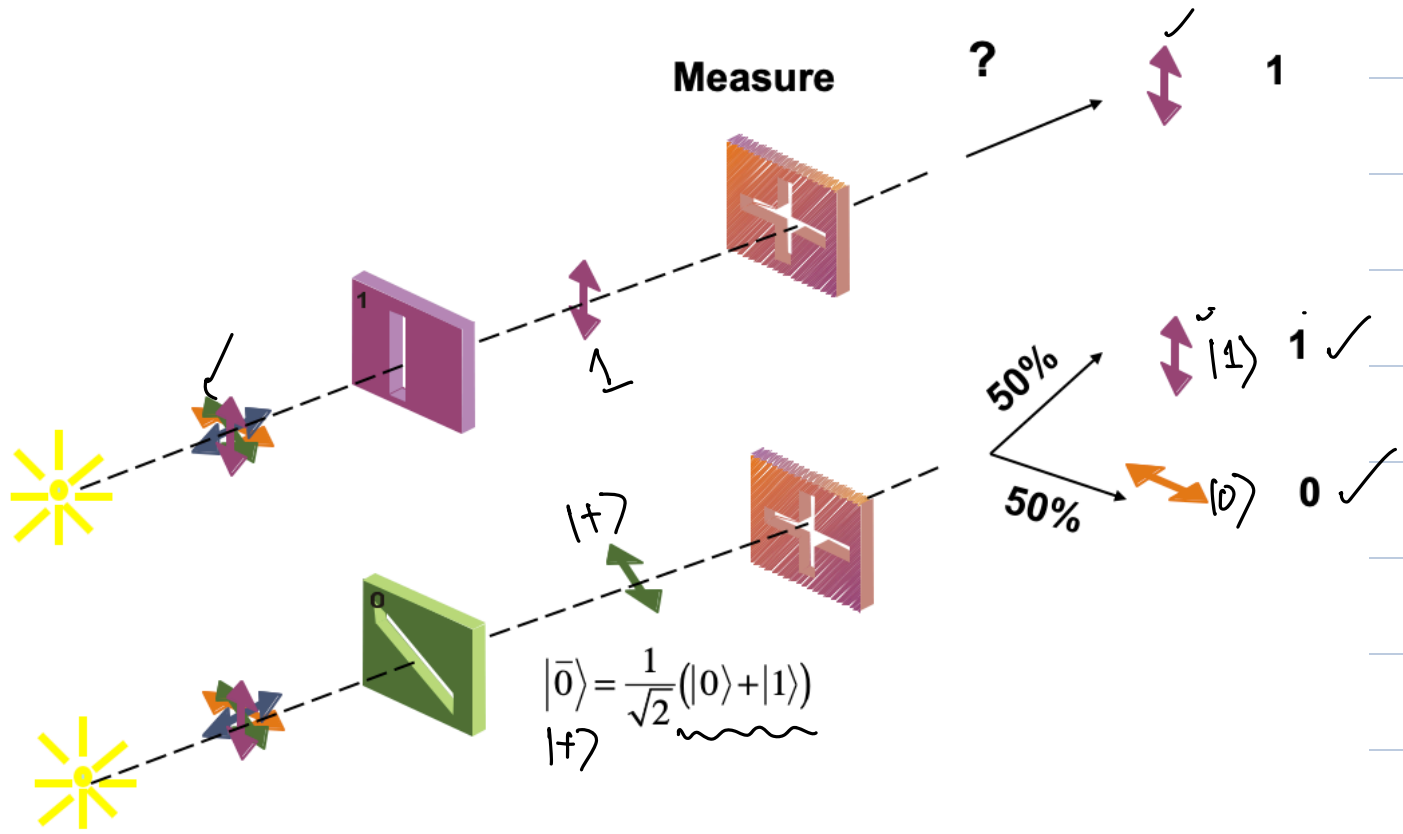
$\langle -|0\rangle = \frac{1}{\sqrt{2}}$

$\langle +|1\rangle = \frac{1}{\sqrt{2}}$

$\langle -|1\rangle = \frac{1}{\sqrt{2}}$

$\left.\begin{matrix} \{|+\rangle, |-\rangle\} \\ \{|0\rangle, |1\rangle\} \end{matrix}\right\}$ non-orthogonal.

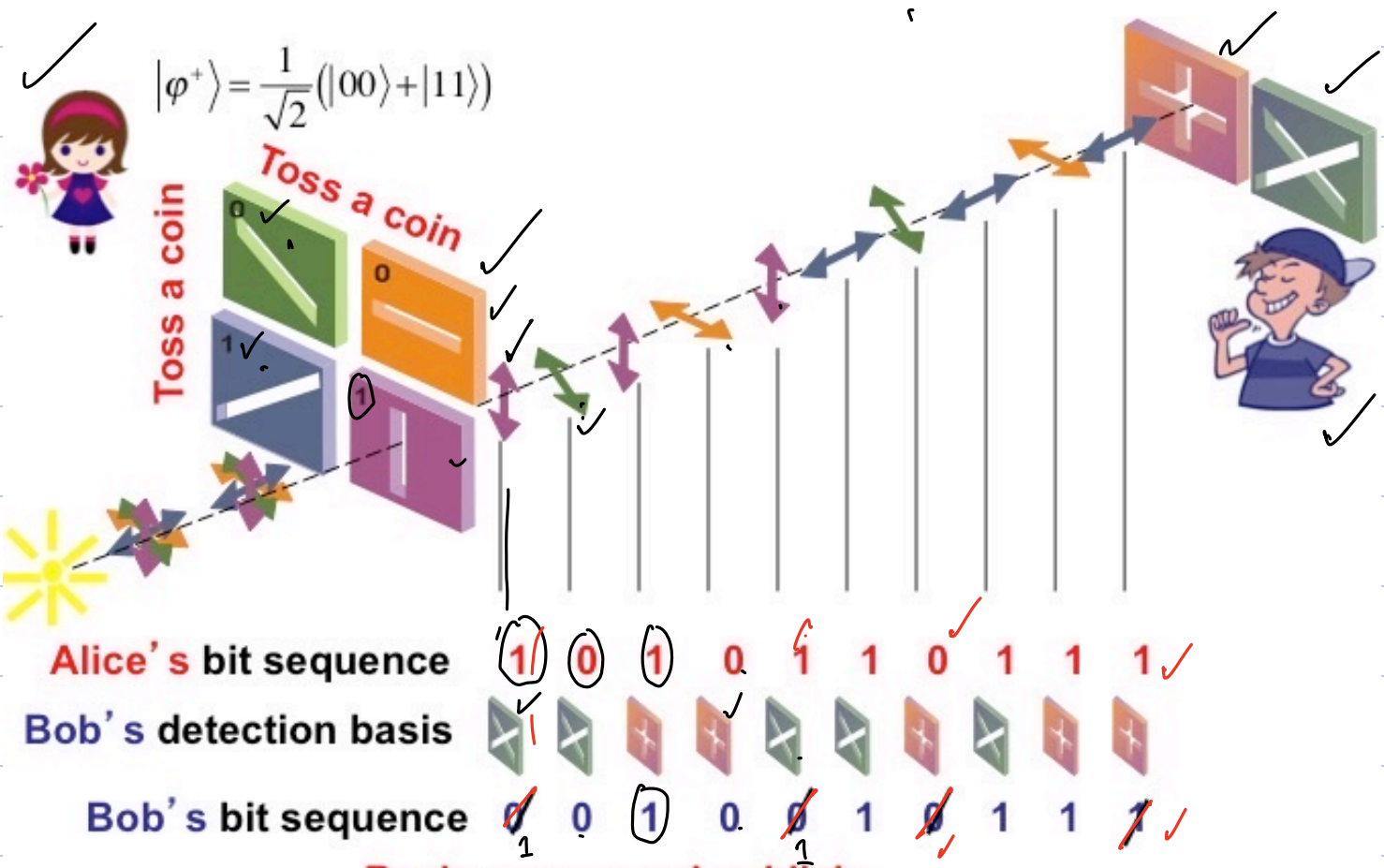
Measurement:



Preparation basis = Measurement basis.
Measured bit values match perfectly with prepared value.

Preparation basis ≠ Measurement basis
Measured bit value is same as prepared one only 50% of the times.

BB84 Protocol



01011

50 % of times basis would match.

After sifting:

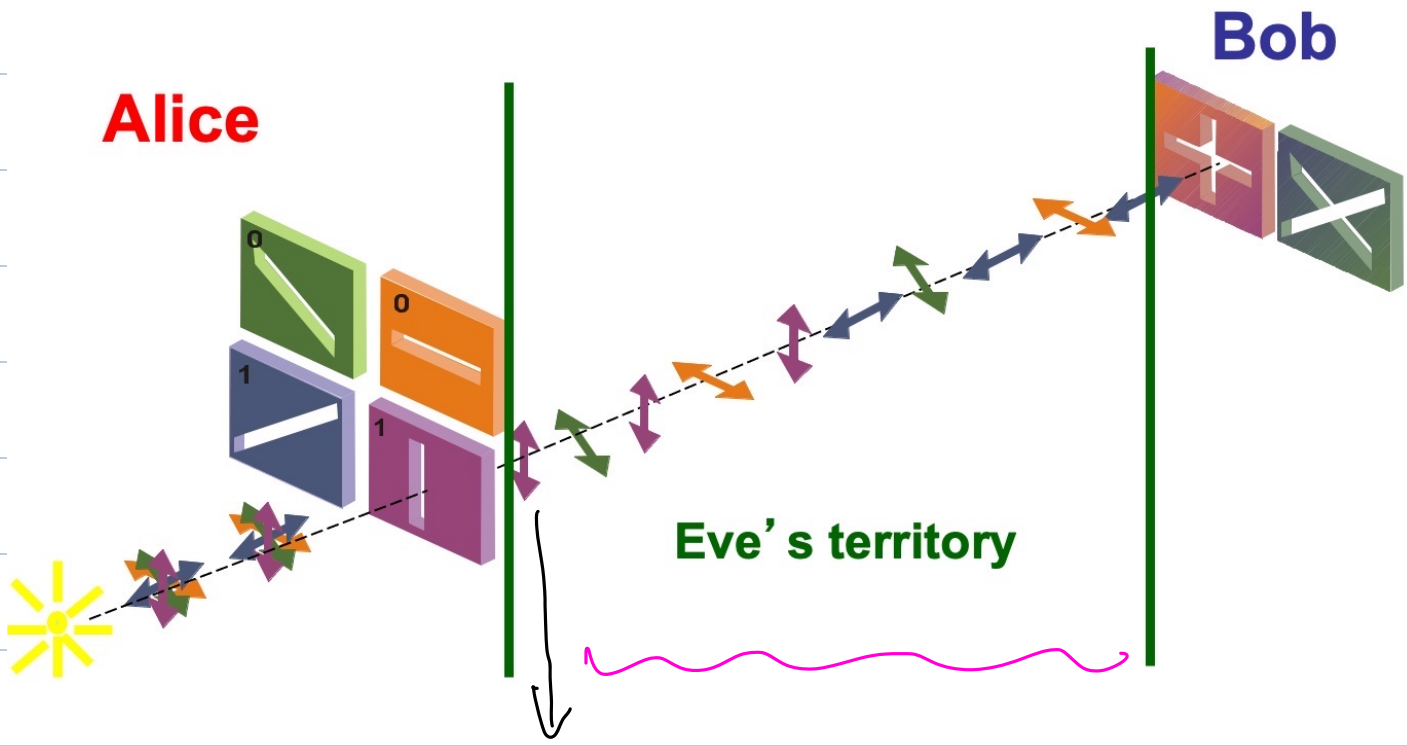
Key: $\frac{1}{2}$ the original length.

The key is distributed using this scheme not the message.

$10^6 \longrightarrow \frac{1}{2} \times 10^6 = 0.5 \times 10^6$.

We have generated a symmetric key b/w Alice & Bob by sending quantum states through open channel.

Is it Secret?



∴ Eve cannot clone an unknown quantum state

What if Eve measures too

Alice	Eve			Bob
	Reference	Result from attack		
	✓ 	"0" ✓	✓	✓ 
	× 	"0" ✓	✓	✓ : 0
		"1"	×	× : 1
				✓ : 0
				× : 1

0

All three basis are same 50 % times.

Error introduced is 25 %.

Eve's information is 50 %.