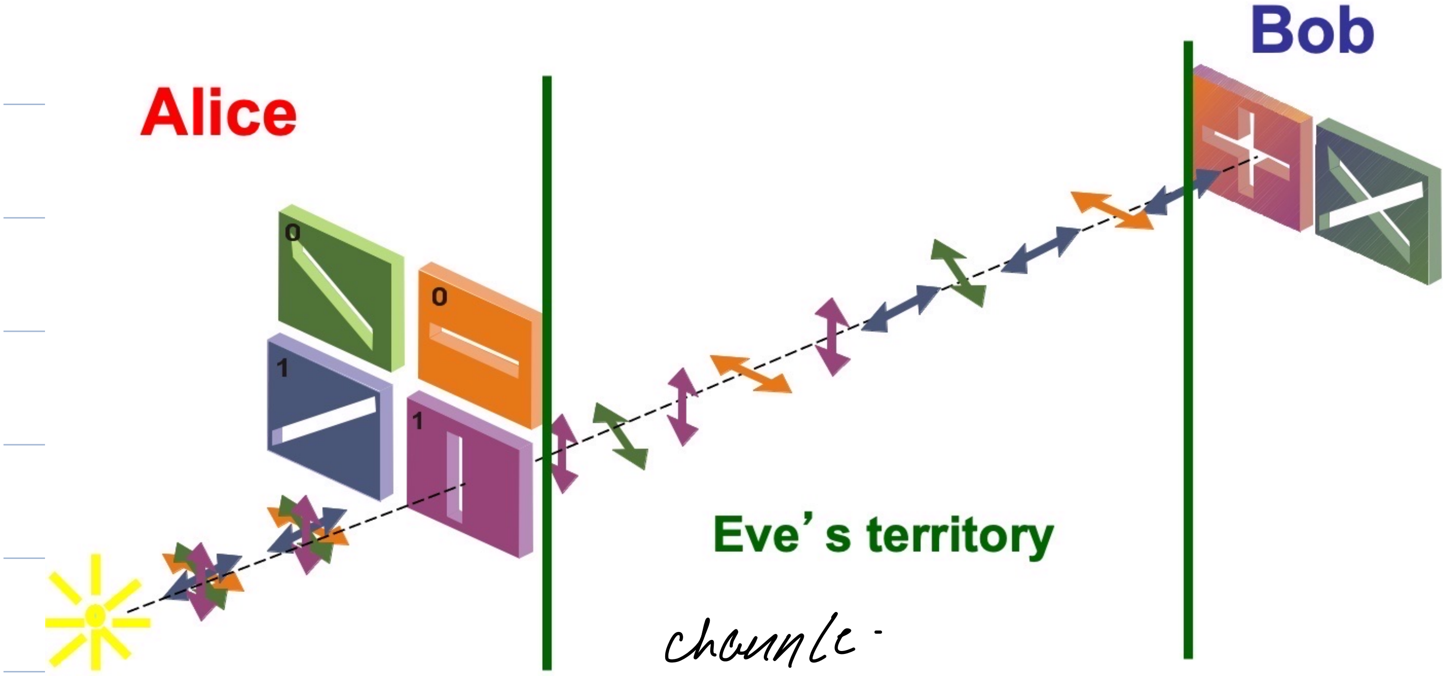
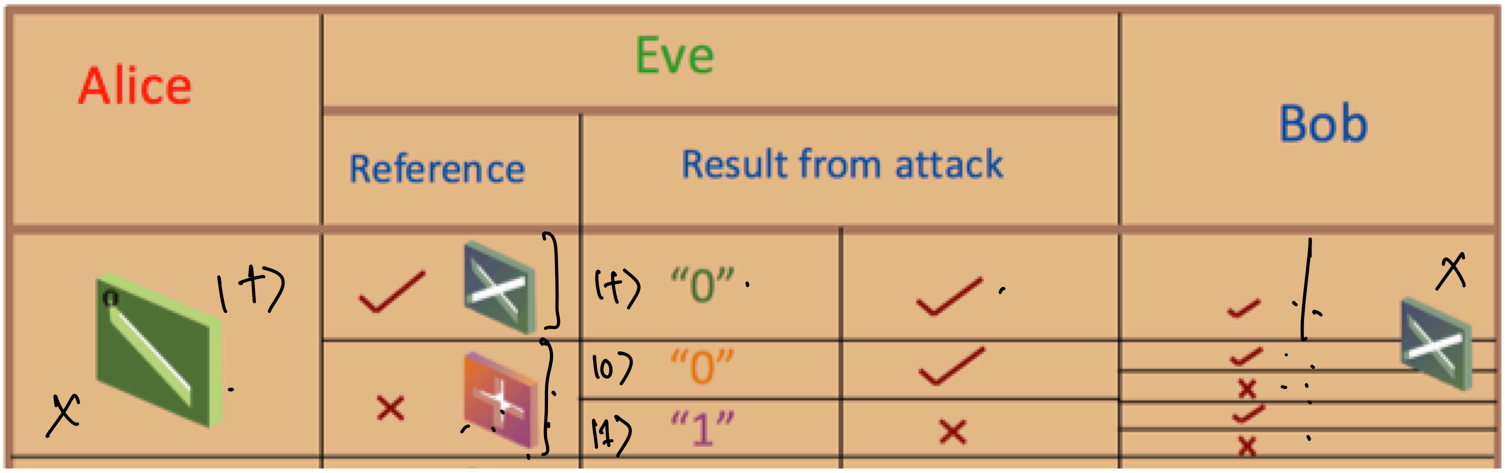
This Lecture:

- QKD with Noise
- Error Correction and Privacy Amplification
- Six State Protocol
- Two State Protocol



channle·

Intercept- Resend Attack·



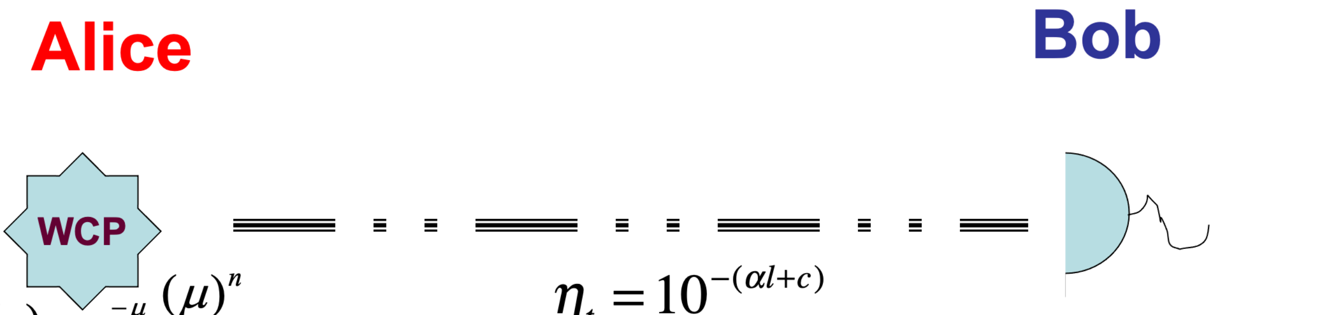
Alice	Eve			Bob
	Reference	Result from attack		
$|+\rangle$ x	✓	$|+\rangle$ "0"·	✓·	✓ x
	✕	$|0\rangle$ "0"	✓	✓ ✗
		$|1\rangle$ "1"	✕	✓ ✗

Eve's information : 50%.

Error introduced : 25%.

-· Individual Attack:

Eve at an advantage



$$P(n) = e^{-\mu}\frac{(\mu)^n}{n!}$$

$P(0)$

$$\eta_t = 10^{-(\alpha l + c)}$$

$\eta_D < 1$.

-

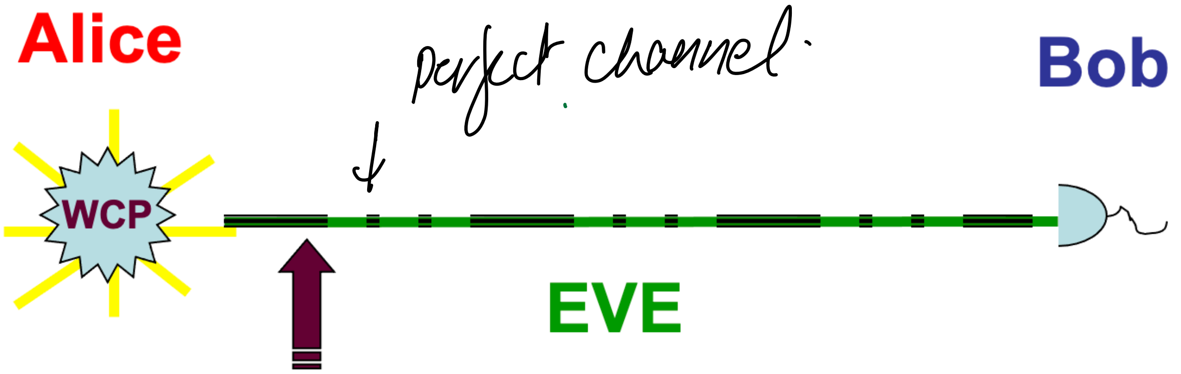
α absorption coefficient

l fibre length

c constant loss in optical components

- Eve is only restricted by laws of physics.
- Passimistically all errors are caused by Eve.

Photon number splitting attack:



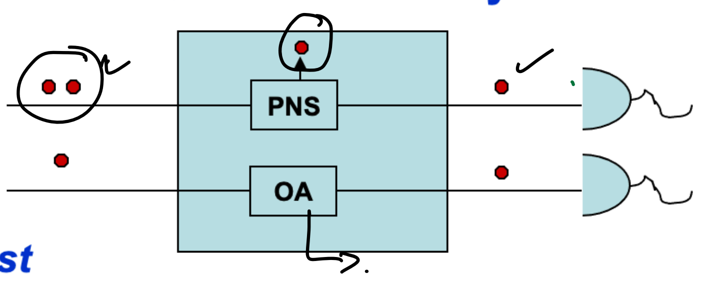
QND *PN Measurement + Splitting ; Polarization undisturbed*

Quantum Memory

$\Delta = P_M/P_{exp}$

1-Δ

Blocks the rest



Disturbance=0 Basis known

Disturbance=D Basis unknown

Error Estimation

- Select check bits. (half of the total number).
- Announce the bit values for that.
- Calculate the error rate (QBER)
- Error Correction + Privacy amplification.

Information Reconciliattion

Error Correction.

- pair up their bits.

44th / 100th.

Announce the result.

Alice: $0 \oplus 1 = 1$.

Bob $0 \oplus 1 = 1$.

$1 \oplus 1 = 0$.

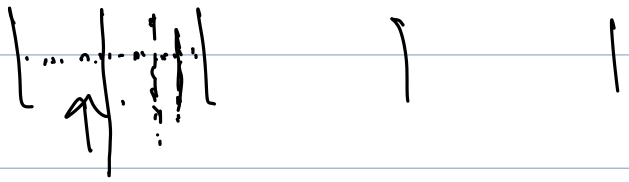
with error

if match no error or two.

Compute parity bit: for whole block by Alice + Bob.

$1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0$ $\underline{1}$.

Parity Check:



large QBER ⇒ small block size.

Small QBER ⇒ large block size.

- After error correction.
  - Key bits exactly match.
  - Information of Eve increases.

Privacy Amplification:

- Randomly permute the bits.
- Pair up the bits.

1 44. 10^6.

$\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2} \sim 10^5$

Alice $1 \oplus 0 = 1$ ✓

Bob $1 \oplus 0 = 1$

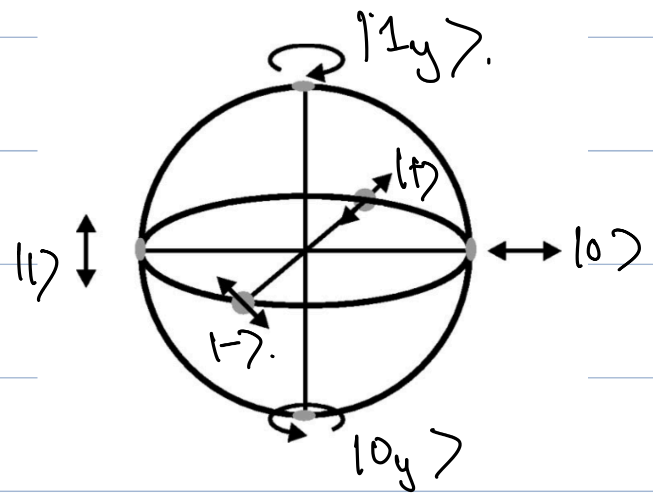
QBER = δ

They donot announce the result but keep the parity bit as key.

$$R = \frac{1}{2}\times\frac{1}{2}\left[1 - \underset{\uparrow EC.}{H(\delta)} - \underset{\rightarrow PA}{H(\delta)}\right].$$

$\delta = 11\%$.

Six State Protocol



3 basis

|0⟩ |1⟩.

|+⟩ |-⟩

|0y⟩ |1y⟩

BB84 — Four-state protocol. In six-state protocol.

-. Alice prepares one of the six states randomly.

-. Sends the qubit to Bob.

-. Bob selects the basis randomly.

Correct basis $\frac{1}{3}$ times.

-. Announce the basis.

-. Keep the ones where basis are same.

-. Key length is reduced to $\frac{1}{3}$.

-. Alice Bob.

0 + + ✓ 0 — — — + 0 $\frac{1}{3}$.

✗ 0 ✓

G. 1 ✗

-0

1

0 1 0 1 0 1 0 1

Eve information 33 %.

Error introduced 33 %.

Two State Protocol

$\lvert 0\rangle$, $\lvert +\rangle = \frac{1}{\sqrt{2}}\left[\lvert 0\rangle + \lvert 1\rangle\right]$.

Z-basis   X-basis.

	Z ✓		X ✓	
$\lvert 0\rangle$	$\lvert 0\rangle$	$Pr = 1$	$\lvert +\rangle$	$Pr = \frac{1}{2}$
	$\lvert 1\rangle$	$Pr = 0$	$\lvert -\rangle$	$Pr = \frac{1}{2}$
$\lvert +\rangle$	$\lvert 0\rangle$	$Pr = \frac{1}{2}$ ✓	$\lvert +\rangle$	$Pr = 1$
	$\lvert 1\rangle$	$Pr = \frac{1}{2}$	$\lvert -\rangle$	$Pr = 0$

Alice

$$\left.\begin{array}{l} \lvert 1\rangle \longrightarrow \lvert +\rangle \\ \lvert -\rangle \longrightarrow \lvert 0\rangle \end{array}\right].$$

$$\left.\begin{array}{l} \lvert 0\rangle \\ \lvert +\rangle \end{array}\right] \text{ inconclusive.}$$

Unambigous state Discrimation: (POVM).

The state is discriminated without error at the cost of some inconclusive results.