CHSH Inequality

$X, Z, V, W \rightarrow$ are observables

$\pm 1 \rightarrow$ eigenvalues

$$C = \langle X_1 W_2 \rangle - \langle X_1 V_2 \rangle + \langle Z_1 W_2 \rangle + \langle Z_1 V_2 \rangle = \pm 2$$

correlation

$$\langle C \rangle = 2\sqrt{2} \leftarrow \text{for Bell State}$$

$$\langle X_1 W_2 \rangle = \langle \Psi^+ | X_1 W_2 | \Psi^+ \rangle = \mathrm{Tr}(X_1 W_2 \, |\Psi^+ \rangle\langle \Psi^+|)$$

$$\mathrm{Tr}(A \otimes B \, |\Psi^+ \rangle\langle \Psi^+|) = P(\text{output same bits}) - P(\text{output} \neq \text{bits})$$

→ The inequality must be violated to have a pair of entangled qubits ($|\langle C \rangle| \leq 2$)

→ Maximally violated → $\langle C \rangle = 2\sqrt{2}$ = Bell state

E91 protocol

→ Each part has a set of 3 basis (2 in common)

→ A entangled pair is prepared (one qubit for each)

→ then they measure its qubit in one of the its 3 basis randomly (Θ_i^A, Θ_i^B)

→ 2/9 times their basis match ($\Theta_i^A = \Theta_i^B$)

→ They announce their basis

→ if $\Theta_i^A = \Theta_i^B \Rightarrow$ key bit value match

→ else ($\Theta_i^A \neq \Theta_i^B$) → check using CHSH (Bob $= \{X, Z\}$
Alice $= \{V, W\}$)

→ if $\Theta_i^A = \Theta_i^B$ or $\langle C \rangle = 2\sqrt{2}$, then they are maximally entangled, therefore free from Eve

→ Keep cases which $\langle C \rangle = 2\sqrt{2}$ and $\theta_i^A = \theta_i^B$ to form the key
→ 7/9 % of the initial qubits are thrown away in the process

→ has an advantage for using entanglement than the BB84 protocol, but it may be a little bit unefficient in some cases

BB84 protocol (entanglement version BBM92)

→ Alice prepares a entangled pair (one qubit for herself and the other to Bob)
→ they select one of their 2 basis randomly (θ_i^A, θ_i^B)
→ if $\theta_i^A = \theta_i^A$ they keep the bit in the key

→ As the qubits are being used through the quantum channel without being measured, Eve can't get the values, and if she tries to attack it will disturb the system

→ BB84 is equivalent to BBM92

Advantage of the entanglement version

→ in the standard version, Eve can intercept the qubits, measure them, and when the basis are revealed, it can have the information about the key with 50% of certainty

→ We need to keep in mind the pessimistic approach

- which all the disturbance in the system is due to Eve's attack

-> Eve can do whatever she wants to

-> So in the entangled version, there's more prob. that the pairs are a couple and don't have nothing between them

Error correction

Alice -> $0 \oplus 1 = 1$

Bob -> $0 \oplus 1 = 1$ $\qquad 1 \oplus 1 = 0$

bits paired to each other ↗ addition mod 2 (XOR)

Alice 00 10 11 01 -> parity 0 $(n(0) = n(1))$

Bob 01 10 11 01 -> parity 1 $(n(0) \neq n(1))$

$$\boxed{\begin{array}{cccc} 00 & 10 & 11 & 01 \\ 0 & 1 & 0 & 1 \\ \multicolumn{4}{c}{1 \oplus 1 = 0} \end{array}}$$

Alice

$$\boxed{\begin{array}{cccc} 01 & 10 & 11 & 01 \\ 1 & 1 & 0 & 1 \\ \multicolumn{4}{c}{0 \oplus 1 = 1} \end{array}}$$

Bob

-> If Bob and Alice parity are different, so there's 1 error

→ We could add another bit for parity

1 (original)   1 (parity)

$1 \oplus 1 = 0$

if one of them flips, we can find the error:
$1 \oplus 0 \rightarrow 1$
$1 \oplus 1 \rightarrow 1$

$0 \oplus 0$ if both of them flip, so we can't find

Cascade Protocol (Error correction)

→ inefficient
→ shuffle the bits, then divide the bit string into blocks, compute the parity of each block, and then announce these bits
→ if some blocks don't match the parity, so it's needed to make another round with smaller blocks
→ when we permute, the errors are distributed
→ can only detect 1 error
→ large QBER → you need smaller blocks
→ it fails if QBER > 25%

→ Error correction is always classically done

Privacy Amplification

→ to eliminate Eve's information
→ After Error Correction
→ Some information is leaked to Eve during EC

→ They randomly permute their qubits and pair them up, do the addition mod 2 and keep the resulting value
→ Note: Alice and Bob know which pair to join
→ In this process they don't reveal any further info.
→ When the ⊕ is done, we are reducing the Eve's info, since she has at least 50% of the key, and now she has less than before, since she knows which bits to pair up, but may not know the actual values of them
→ We can run this many times (rounds) to reduce, even more, Eve's info.
→ 50% of the key is discarded, since we just keep the ⊕ result

Post Processing

→ EC and PA
→ at the end the key is secret
→ A & B have the same key

Key generation rate

→ $\frac{n^\circ \text{ of qubits used as key}}{\text{total of sent qubits}}$

→ $R = R_{sift}[1 - \underbrace{H(\delta)}_{EC} - \underbrace{H(\delta)}_{PA}]$ $\delta = QBER$

sifted key

→ $R > 1$ → otherwise, too many qubits has been lost

Attacks

→ Imagine that there's a quantum communication system based on photons, so when Alice wants to send some info to Bob, she encodes it in photons and send them through a noisy channel.

→ Eve wants to intercept this data, so she, as an external agent, has no limits, so for that she can replace the noisy channel in the middle of the connec. to a perfect one. Then she can keep a photon when the package has more than 1, and when Alice announces its basis, Eve can do the measurements.

→ That's why the entanglement is important