Let $r_{kA}, r_{kB} \in \{0,1\}^N$ be the raw key for Alice & Bob respectively.

Let $B_i^A \; \forall i = 1,2 \ldots k$ be a single block such that :

$$r_{kA} = B_1^A \cdot B_2^A \cdot \ldots \cdot B_k^A$$

& similarly $r_{kB} = B_1^B \cdot B_2^B \cdot \ldots \cdot B_k^B$

Then, a subset t_i of size m_i is chosen for each block b_i and measurements, indexed by subsets, are exchanged over authenticated classical channel to determine noise present in each block, Q_i.

Then, each of the k keys are distilled seperately & the size of s_i (key after distilling block i) depends on Q_i.

Case 1: Non blockwise Scheme :

Here entire key is treated as a single system from which a random sample of m is chosen

Then Q is estimated. (Q is Fidelity measure)

Then, remaining bits are ran through an Error Corr. process

Then, a test by running the hash f_c over corrected Alice & Bob key

Then, privacy amplification is run, outputting a secret key of length $l \leq n$, where $\eta = N - m$.

Case 2: Blockwise Scheme:

Let B_i be the i^{th} block.

Now, a random subset t_i of size m_i for each B_i is chosen.

So, similarly, Q_i is estimated for each block i.

Then, error correction, a correctness test (Hash) & privacy amplification is performed on each block.

How to measure Q?

Q → Fidelity, which is a measure b/w two states.

For ex: if X is a random variable & we define $Y = 2X$. Then fidelity will be very high ($= 1$).

whereas if X & Y were independent $Q = 0$.

So, F in our case is the "closeness" b/w the transmitted photons state & received photon state. Ideally, they should be same i.e F=1. But, due to presence of noise, received photons are depolarised. So, to simulate this, we need a model for depolarizing channel.

So, for a single Qbit system; a depolarizing channel can be modelled as:

$$N(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

where $\{X, Y, Z\}$ → Pauli Matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ; \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

ρ → density Matrix of input state

So, $\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $\rho_{45} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$; $\rho_{90} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$$\rho_{135} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

So, Now let $\sigma = N(\rho)$ i.e the density Matrix of the received photon.

So, we can calculate Q as:

$$Q = \left[tr\left(\sqrt{\sqrt{\rho}\,\sigma\,\sqrt{\rho}} \right) \right]^2$$

— ∝ ——— ∝ ——— ∝ ———

Error Correction:

① Hamming Code: Parity check

② CRC: Cyclic Redundancy Codes.

— ∝ ——— ∝ ——— ∝ ———

Hashing:

<see the link added in Links file>