IISER KOLKATA

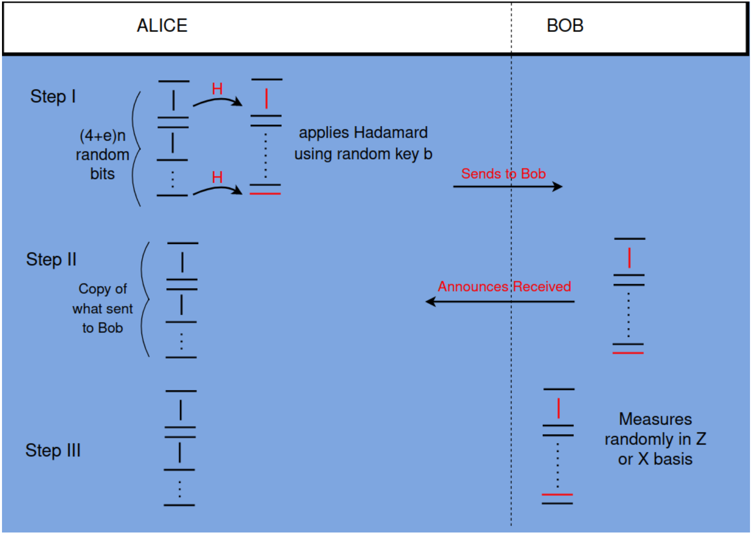
Security Proof of BB84 Protocol

Abhishek Mishra(17MS100)
Supervisor: Prof. Guruprasad Kar, PAMU, ISI Kolkata

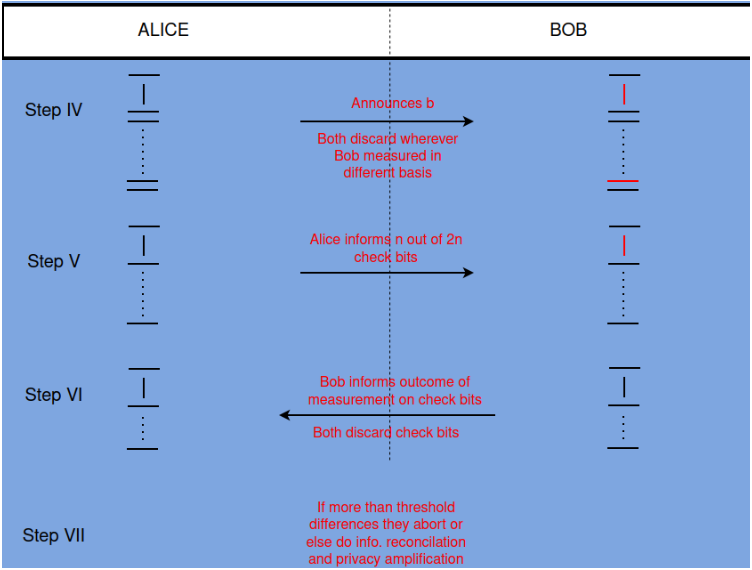
Indian Institute of Science Education and Research, Kolkata
Physics Department
am17ms100@iiserkol.ac.in

December 13, 2021

BB84 Protocol



BB84 Protocol Contd.



Aim of the Project

- To prove the security of BB84 Protocol. Elaborate on the arguments provided by Shor and Preskill by providing justification and formulas and proof.
- To establish the fact that the BB84 rate is equal to the CSS rate by exploring the hidden CSS model.
- To establish connection between Cryptography and Error Correction.

Background Study

- We need theory of Quantum Channel/Noise ,its operator representation and system- Env model.
- Discuss about theory of error correction.
- To introduce Stabilizer formalism and its advantages.
- To discuss CSS codes.
- To prove the security of BB84 protocol by providing equivalence between protocols and proving security of each.

Quantum Noise

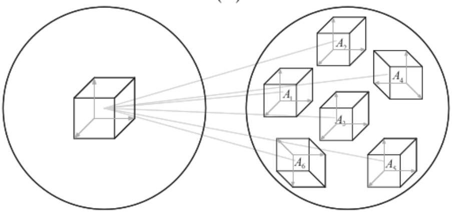
Figure: Left:Closed dynamics : Right: Open Dynamics

- Any Quantum Channel is open to environment , hence can be modelled as first adjoining it to an ancilla or env. of at max d^2 d=dim. of principal system and then doing an unitary evolution and then discarding the ancilla.
- $\xi(\rho) = Tr_{Env.}[U(\rho \otimes |e_0\rangle \langle e_0|)U^{\dagger}]$: ρ is init. state of system and $|e_0\rangle$ is init. state of env.

IISER KOLKATA

Freedom in Operator Representation

- We can represent the above dynamics using just operators acting on principal system called the operator sum representation.
- $\xi(\rho) = \sum_k \langle e_k| U\rho \otimes |e_0\rangle \langle e_0| U^\dagger |e_k\rangle = \sum_k E_k \rho E_k^\dagger$
- $E_k = \langle e_k| U |e_0\rangle$ are the operation elements and $|e_k\rangle$ are the basis of Environment with $\sum_k E_k E_k^\dagger = 1$
- Suppose $E_1, ..., E_m$ and $F_1, ..., F_n$ are operation elements giving rise to quantum operations ξ and $\mathcal{F}$, respectively. Then ξ = $\mathcal{F}$ iff there exist complex numbers u_{ij} such that $E_i = \sum_j u_{ij} F_j$, and u is an m by m unitary matrix.



- We must always be able to distinguish orthogonal states i.e $\langle\bar{0}| E^\dagger F |\bar{1}\rangle = 0$ (i)
- If diff. errors give diff. error syndrome, then it is sufficient for error correction. i.e $\langle\bar{\alpha}| E^\dagger F |\bar{\alpha}\rangle = 0$ (ii)
- It is necessary that recovered state is proprtional to original state i.e $\langle\bar{0}| E^\dagger E |\bar{0}\rangle = \langle\bar{1}| E^\dagger E |\bar{1}\rangle$ (iii)
- So we need a codespace for which we can find a basis of errors fulfilling the above conditions. The general condition for set of errors is then $\langle\psi| E^\dagger E |\psi\rangle = C(E)$

Stabilizer Codes

- The generalized Pauli group is defined as $G_n = \pm\{\mathbb{I}, \mathbb{X}, \mathbb{Y}, \mathbb{Z}\}^n$, $\mathbb{Y} = i\sigma_y$
- Codespace $\mathcal{H}_s$ is the eigenspace stabilized by an abelian subgroup of G_n called the stabilizer S.
- unitary evolution of codespace is described as unitary evolution of Stabilizer.
- Generator of stabilizer is also called check operators because the measurement outcomes dictate the error that has ocurred and hence the recovery to be performed if the error is catachable.
- Error is catchable or the error cond. are that for any $E_a, E_b \in \xi$
  - $E_a^\dagger E_b \in S$
  - $\exists M \in S : \{M, E_a^\dagger E_b\} = 0$

IISER KOLKATA

Equivalence of Stabilizer Code

- Two stabilizer codes are equivalent if they differ only by permutation of parties(qubits).
- Two Stabilizer codes are equivalent if they differ by any single qubit unitary transformation or by diff. choice of basis of individual hilbert space.
- This then implies that we can also work with codepsace which is eigen space with +1 eigen value for some check operators and -1 for other.

CSS Code

- CSS code belongs to class of QECC borne out of classical linear codes.
- Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subset C_1$.and $C1$ and $C_2^{\perp}$ both correct t errors. We will define an $[n, k_1 - k_2]$ quantum code CSS(C_1, C_2) capable of correcting errors on t qubits, the CSS code $|x + C_2\rangle = \frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle$
- After a bit flip error described by bit string e and phase flip error described by z, the state is $\frac{1}{\sqrt{|C_2}} \sum_y -1^{(x+y).z} |x + y + e\rangle$, error can be caught by introducing ancilla to catch syndrome.

CSS Error Correction and Stabilizer way

- To catch bit error, $\frac{1}{\sqrt{|C_2}} \sum_y -1^{(x+y).z} |x+y+e\rangle |H_1 e\rangle$
- , for phase error, $\frac{1}{\sqrt{|C_2}} \sum_y -1^{(x+y).z} |x+y\rangle \xrightarrow{H} \frac{1}{\sqrt{|C_2}} \sum_f \sum_y -1^{(x+y).(z+f)} |z\rangle \rightarrow N \sum_f \sum_y -1^{(x+y).(z+f=z')} |z'+f\rangle \rightarrow N \sum_{f \in C_2^{\perp}} -1^{(x).(z')} |z'+f\rangle$
- CSS Codes decouple phase and bit flip errors.
- For stabilizer way of descibing CSS code, we replace check matrix for C_1 by H_Z and $C_2^{\dagger}$ by H_X as $\begin{pmatrix} \mathrm{H}_Z & | & 0 \\ 0 & | & \mathrm{H}_X \end{pmatrix}$
- Now, the commutation of H_Z and H_X implies $H_X H_Z^T = 0 = H_Z H_X^T$ which implies CSS cond. $C_2 = C_X^{\dagger} \subset C_1 = C_Z$

CSS equivalent codes and Dual of CSS

- We define CSS_{xz} similar to css code as $v \in C_1 \rightarrow \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} -1^{z.w} |x + v + w\rangle$, x,z are n bit strings describing bit and phase flips.
- Since, there is only unitary evolution by $U \in G_n$ of the code or stabilizer, corresponding to x,z errors, this is another equivalent stabilizer code.
- Dual of css code is another css borne out of $C_1^{\perp} \subset C_2^{\perp}$.
- CSS goes to $CSS^{\perp}$ by Hadamard transformation H^n and hence the stabilizer is transformed by just exchange of X and Z and hence now bit flip will be recovered by parity matrix of $C_2^{\perp}$ and phase flip by parity matrix of C_1.

Error Correction And Entanglement Distillation

- It can be shown that for the QKD, we need correlation beyond possible classically hence entanglement and entanglement is key component in privacy amplification and information reconciliation.
- Alice prepares n copies of Bell pairs and sends it to Bob through channel prone to noise or eavesdropping and hence the entanglement is lost.
- We recover some amount of entanglement through error correction (CSS specifically).
- $\phi^{+n} = \sum_{i \in C^{2n}} |i_A\rangle |i_B\rangle$, $i \perp j = 0$. We choose CSS_{xz} vectors as orthogonal basis, i.e $\phi^{+n} = \sum_{x,z,i} |CSS_{xz}(i_A)\rangle |CSS_{xz}(i_B)\rangle$, where x,z are correctable bit and phase flip errors.
- $\langle CSS_{xz}(i) | CSS_{x'z'}(j)\rangle = \delta_{xx'}\delta_{zz'}\delta_{ij}$
- In case of no noise, the above representation holds and when Alice measures here pair , the outcome she gets correlates with Bob and corresponding to the outcome the resultant states of both alice and Bob would be in CSS_{xz} for some x,z

- Now, suppose there is error in Bob's particles and error can be any error correctable by used CSS code, then the n bell pairs gets distorted to $\sum_{xzi} |CSS_{xz}(i_A)\,|CSS_{x'z'}(i_B)\rangle\rangle : x - x' = e_1, z - z' = e_2$, e_1 and e_2 are bit and phase flip errors.
- Now, when Alice and Bob measures, they won't get same results but differ by error syndromes, so, Bob can correct the error and now states of both would be in CSS_{xz}, where x,z are corressponding to outcome of Alice then go back to original CSS by corresponding unitary and then use decoding of css to get back ϕ^{+m}

The Proof

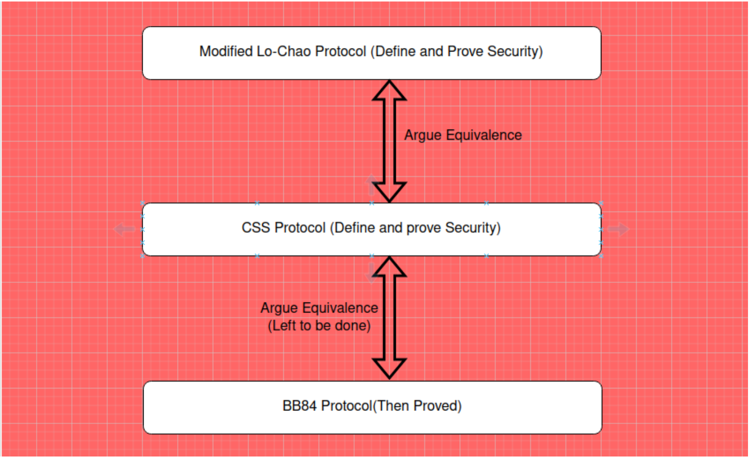


Figure: Equivalence relations

Mod. Lo Chao Protocol

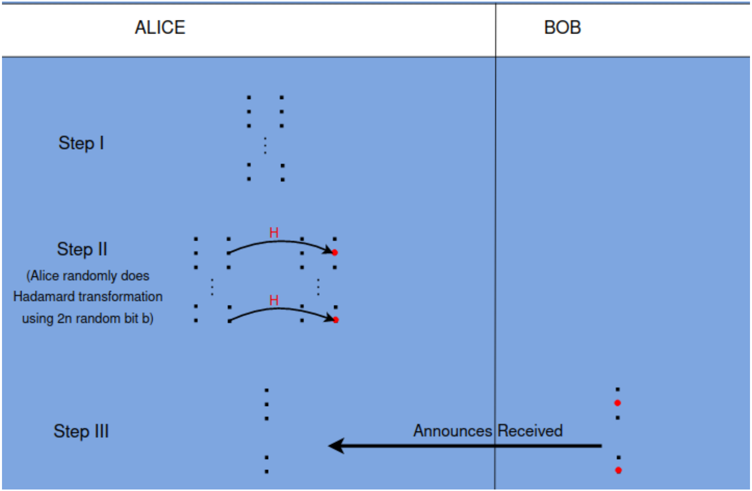
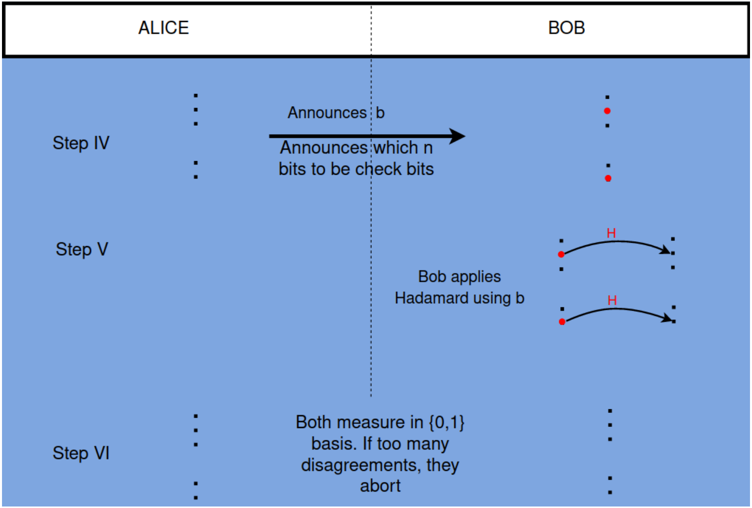


Figure: . . is bell pair

Mod. Lo Chao Protocol Contd.



Mod. Lo Chao Protocol Contd.

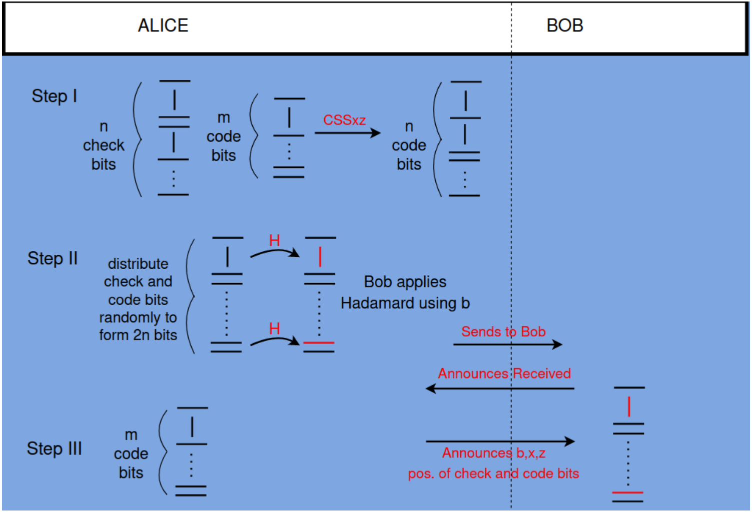
	ALICE		BOB
Step VII	⋮ ⋮	Both measure check operators of css code on code bits, disagreements give error syndrome and then Bob corrects error and they go back to original css and then both apply css decoding	⋮ ⋮

- The definition of security that we use and prove is that the probability that any eavesdropper say Eve can have more than exponentially small mutual information with the shared key is exponentially small if the protocol succeeds.
- The idea is that since check bits are randomly chosen the error rate found there will give a good estimate of error in code bits or in probability language, the probability that the error in code bits will be ϵ more than in check bits is exponentially small in ϵ.
- Alice and Bob measure in $\{0, 1\}$ basis to get error rate.
  $|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-| = |01\rangle\langle 01| + |10\rangle\langle 10|$
  $|\phi^-\rangle\langle\phi^-| + |\psi^-\rangle\langle\psi^-| = |+-\rangle\langle +-| + |-+\rangle\langle -+|$
- We see that error rate in bell basis is same as in local basis(0,1 when b=0 or +,- when b=1) and since hadamard was use to symmetrize the channel , phase and bit flip error rate are equal.

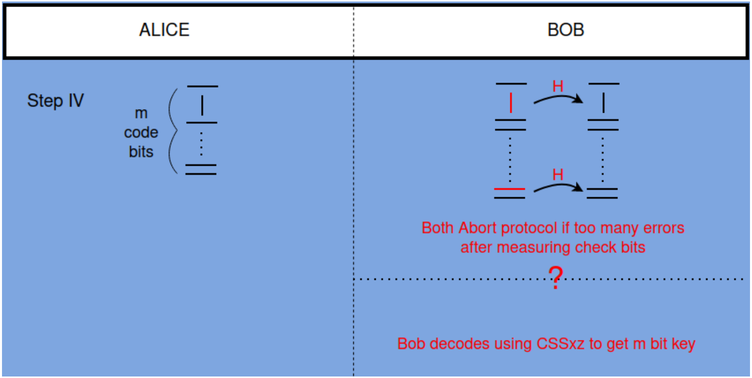
Security of Mod. Lo Chao Contd...

- Now, The fidelity of code bits after error correction with ϕ^{+m} is lower bounded by the probability of t or less errors.
- We invoke a result by Lo and Chao that if this fidelity is $1-2^{-s}$, then the mutual info. of EVE with shared key is atmost $2^{-c}+2^{O(2s)}$, c=$-s+log_2(2m+s+1/log_e2)$.
- Hence if the error on check bits is less than a threshold, the probobality that there is more than t errors on code bits is exponentially small and hence the fidelity is exponentially close to 1 and hence the mutual information is exponentially small as to be proved.

CSS Protocol



CSS Protocol Contd.



Future Goals

- Will provide equivalence between CSS protocol and BB84 protocol.
- Will explore connection between cryptography and Error correction in more details.
- Am also exploring about device independent Cryptography and Random key generator as side project.

IISER KOLKATA

References

- An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation (arXiv:0904.2557) by Daniel Gottesman
- Simple Proof of Security of the BB84 Quantum Key Distribution Protocol (arXiv:quant-ph/0003004)

Thanks!

Department of Physical Sciences

IISER KOLKATA