Quantum Communication Applications: Beyond QKD

Blind Quantum Computing

Anoop Kumar Pandey

IEEE 6th International Conference on Public Key Infrastructure & its Applications– PKIA 2025

03rd September 2025

Bit

Qubit

0/1

$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$

Pauli Operators

Operator (A)	A |0⟩	A |1⟩
I (Identity)	|0⟩	|1⟩
X (Bit Flip)	|1⟩	|0⟩
Y (Bit & Phase Flip)	i|1⟩	-i|0⟩
Z (Phase Flip)	|0⟩	-|1⟩

Matrix Representation

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \text{a} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \text{b} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$\langle\psi| = \begin{pmatrix} a^* & b^* \end{pmatrix}$ (Adjoint or Transpose conjugate)

$$\text{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{X}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\text{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

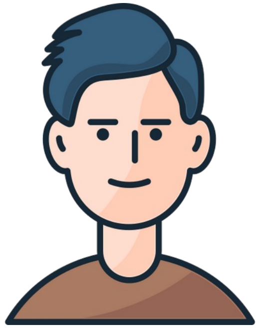
$$\text{X}X^\dagger = \text{XX} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =$$

Important

- $A^\dagger = A$ (Hermitian)
- $A^\dagger A = A\,A^\dagger = I$ (Unitary)
- $A^2 = I$

Blind Quantum Computing

Goal



Intended: $x \to f(x)$

Steps

$x \to x'$ — x' → $x' \to f(x')$

$f(x') \to f(x)$ ← $f(x')$ —

Final: $x \to f(x)$

Note: $x' \not\to x$

Problem Statement

Problem Statement

Client with the ability to person (I, X, Y, Z)

Server with Universal Operator Capabilities

Goal:

1. Hide Input States
2. Hide Quantum Operation

$x \longrightarrow x`$

Masking Input

For Client: Randomly flip the input state as follows:

- Generate a random bit: r (0/1)
  - Must be uniformly random
  - Must be kept secret
- Apply $X^r|0\rangle$
  - $r = 0$, Send $|0\rangle$
  - $r = 1$, Send $|1\rangle$

For Server: Indistinguishable random state

Unmasking Input

$f(x`) \longrightarrow f(x)$

$A^\dagger = A$

$A^\dagger A = A A^\dagger = A^2 = I$

Consider the following

- Client Input: $|\psi\rangle$ and Intended Operation $C\,|\psi\rangle$
- Masked Input: $\sigma\,|\psi\rangle$
- Server Operation: Clifford Operation (unitary) [E.g. H, CNOT]
  - $\sigma' = C\sigma\, C^\dagger$ (transforms one Pauli to another Pauli: σ conjugated by C)
  - $C^\dagger C = C\, C^\dagger = I$
- After Server Operation, State = $C\ \sigma\,|\psi\rangle$
- At Client side: Let's apply a transformation $\sigma' = C\sigma\, C^\dagger$
  - $C\sigma\, C^\dagger C\ \sigma\,|\psi\rangle = C\ \sigma\,\sigma\,|\psi\rangle = C\ \sigma^2\,|\psi\rangle = C\,|\psi\rangle$

$f(x`) \longrightarrow f(x)$

$A^{\dagger} = A$

$A^{\dagger}A = A\,A^{\dagger} = A^2 = I$

Unmasking Input

- Server Operation: Non-Clifford Operation
  - $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
- State after Server Operation: $T\,\sigma\,|\psi\rangle$
- Case 1: σ commutes with T; i.e. $T\,\sigma\,|\psi\rangle = \sigma\,T\,|\psi\rangle$
  - Use $\sigma' = \sigma$ such that
    - $\sigma'\,T\,\sigma\,|\psi\rangle = \sigma\,T\,\sigma\,|\psi\rangle = \sigma\,\sigma\,T\,|\psi\rangle = \sigma^2\,T\,|\psi\rangle = T\,|\psi\rangle$

Unmasking Input

$f(x`) \longrightarrow f(x)$

$A^\dagger = A$

$A^\dagger A = A A^\dagger = A^2 = I$

- Case 2: σ doesn't commute with T (Happens when σ has X or Y)
  - After Server operation, State T σ |ψ⟩
  - Client again applies σ and sends it (σ T σ |ψ⟩) to the server to apply the S gate
    - $S = T^2 = T\,T$
    - $S\sigma T \sigma |\psi\rangle = T\,T\,\sigma T \sigma |\psi\rangle = aT|\psi\rangle$ since $(T\sigma)^2 = aI$. Here a is a scalar
- Problem: If we ask server to apply T after the S, server will know that σ contains X or Y
- Resolution: After every T ask to apply S, but in case of Z, apply S to some random qubit (ancilla)

Masking Operation

$f(x`) \longrightarrow f(x)$

- Server knows the set of operations to be performed
  - $U = U_1 U_2 \dots \dots U_n$
- Client can apply the fixed set of gates like {H, CNOT, T, S} in the same order
  - Apply the undesired states to ancillas

Conclusion

- Server blindness is achieved
  - Input and Operations are masked
  - Desired Operation is obtained through decoding server output
- But
  - It doesn’t guarantee data integrity
  - What if the server is not applying the asked operations

Thank you

anoop@cdac.in
pki@cdac.in

https://ncdt.in

@pkiindia