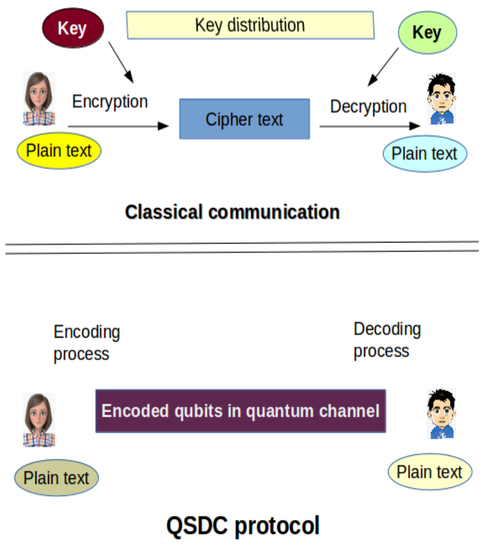
Quantum Secure Direct Communication with Mutual Authentication using a Single Basis

Nayana Das [1], Goutam Paul [2], Ritajit Majumdar [3]

[1]dasnayana92@gmail.com, [2]goutam.k.paul@gmail.com,[3]majumdar.ritajit@gmail.com

INDIAN STATISTICAL INSTITUTE

Introduction to QSDC



- In classical cryptography, sending a secret message always requires a key.
- Quantum Secure Direct Communication (**QSDC**) can transmit secret messages over a quantum channel directly without any key.
- Predefined encoding and decoding rules.

QSDC using a Single Basis

- Alice's and Bob's k-bit identities Id_A and Id_B.
- Θ be a predefined set of angles with cardinality N.
- $\Theta = \{x^\circ : x \text{ is an integer and } 1 \leq x \leq 360\}$.
- For each $\theta \in \Theta$, the unitary matrix U_θ is defined as

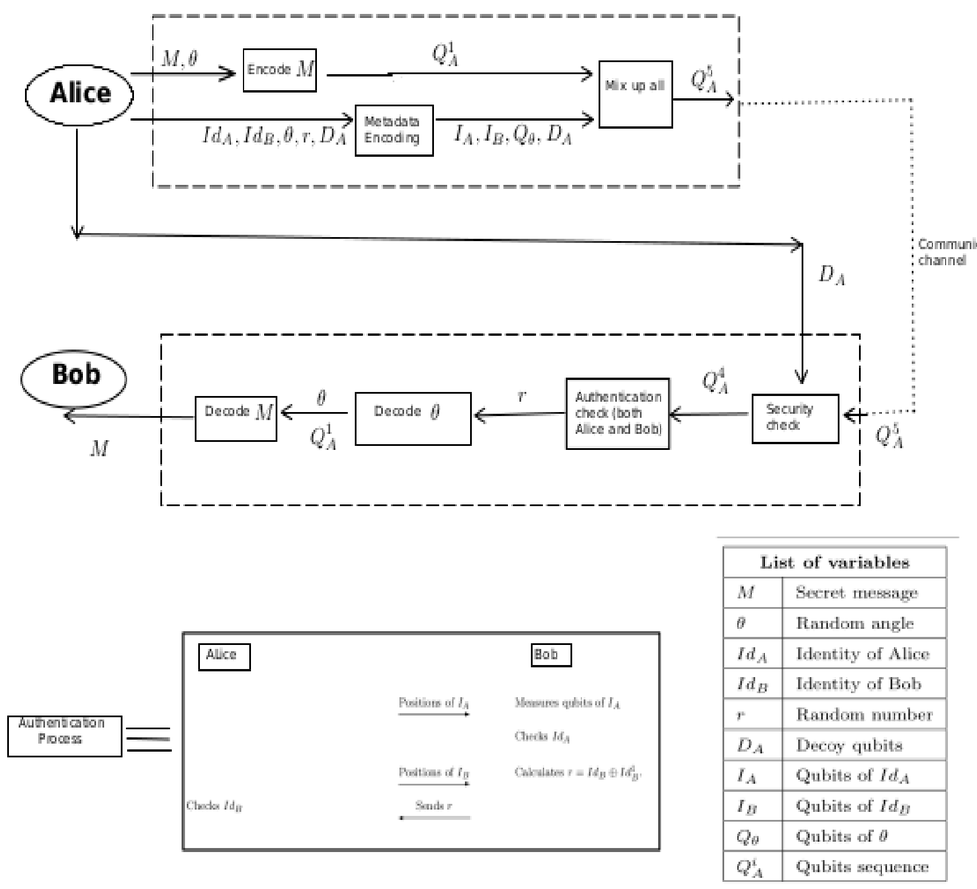
$$U_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

- Then $U_\theta |0\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle$, and $U_\theta |1\rangle = -\sin\theta |0\rangle + \cos\theta |1\rangle$.

The Protocol

- Alice's secret message M. She Encodes M as $0 \rightarrow U_\theta |0\rangle$, $1 \rightarrow U_\theta |1\rangle$ and Prepares sequence Q_A^1.
- Prepares qubit sequences I_A, I_B, Q_θ corresponding to Id_A, Id_B and θ.
- Inserts I_A, I_B, Q_θ in Q_A^1 and sends Bob.
- Alice and Bob authenticate each other using I_A and I_B.
- Bob gets the value of θ from Q_θ.
- He decodes the message M by measuring the qubits of Q_A^1 in $\{U_\theta |0\rangle , U_\theta |1\rangle\}$.

Block diagram of the Protocol



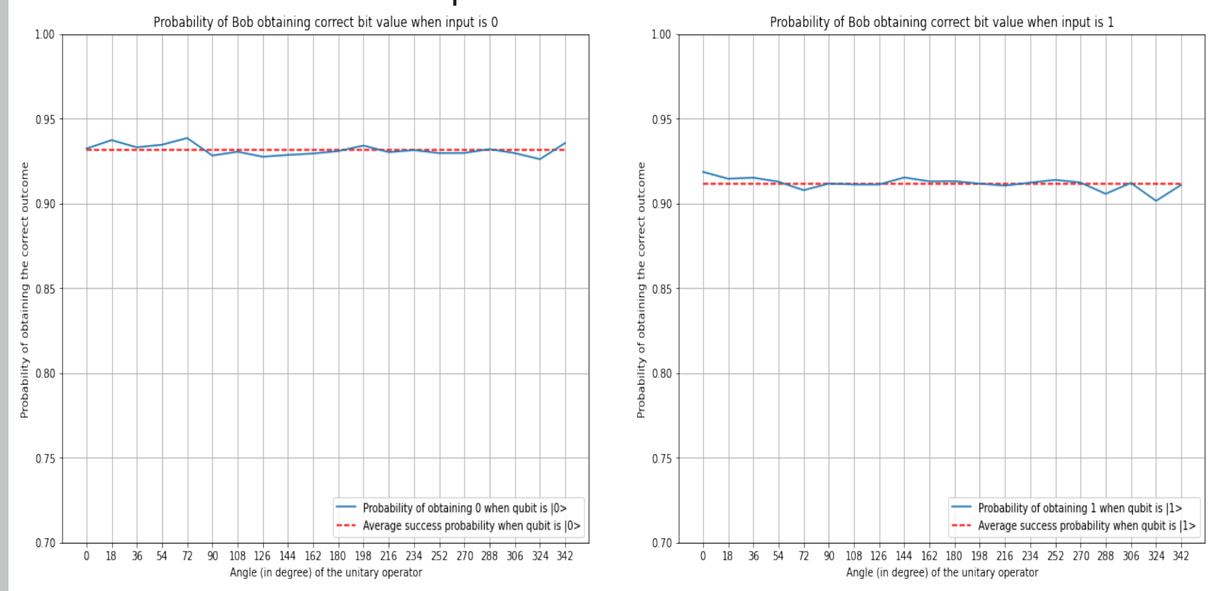
List of variables	
M	Secret message
θ	Random angle
Id_A	Identity of Alice
Id_B	Identity of Bob
r	Random number
D_A	Decoy qubits
I_A	Qubits of Id_A
I_B	Qubits of Id_B
Q_θ	Qubits of θ
Q_A^i	Qubits sequence

Simulation of the protocol in IBM quantum device

- We have executed this protocol in the IBMQ Armonk Device.
- The effect of noise is equivalent to a bit-flip error.
- The effect of noise does not depend on the choice of basis.
- We model an ideal quantum channel as a series of identity gates.
- In a realistic scenario, the channel no longer behaves as identity.
- A minimal overhead of a 3-qubit repetition code is sufficient to protect this protocol against noise.

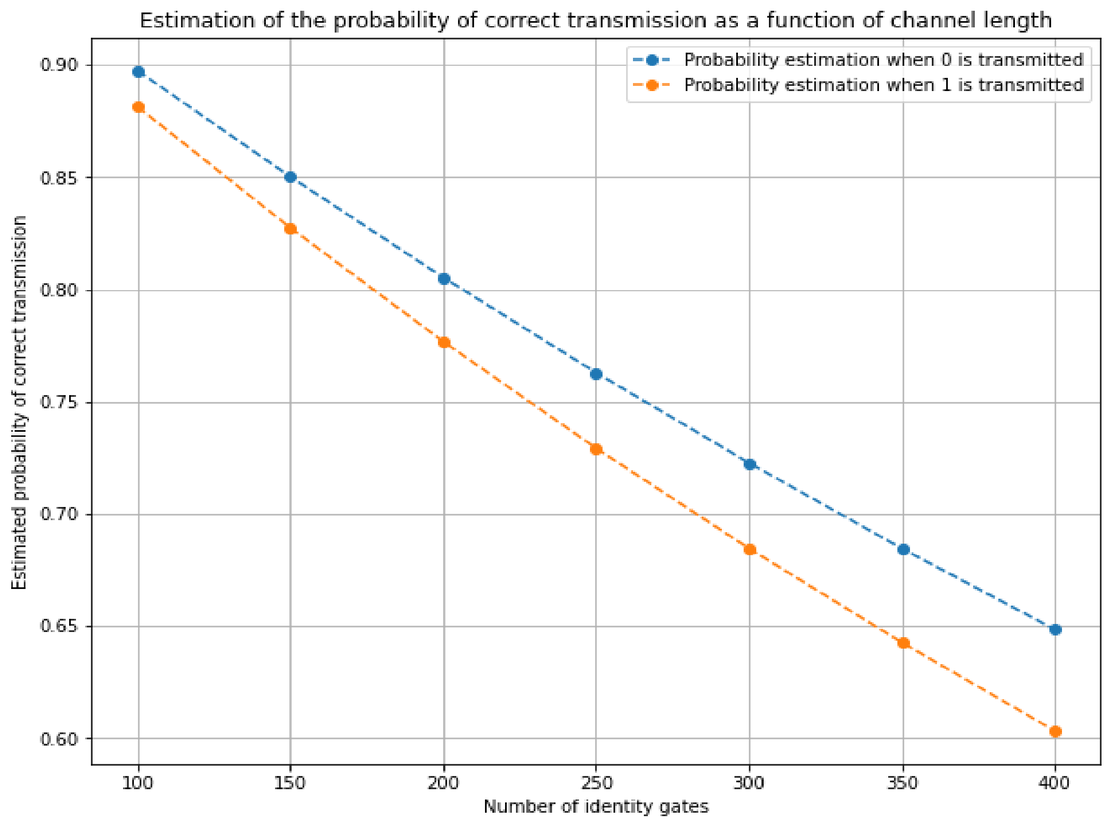
Results of simulation in IBM Quantum Device

Action of noise in real quantum device



Performance when Alice sends 0. Performance when Alice sends 1.

Effect of the length of the channel



Estimated functions for success probability for varying channel length.

Conclusion

- This is a one-step one-way quantum communication protocol.
- It does not use entanglement as a resource.
- Secure against all the familiar attack strategies.
- Our protocol is quite robust to error.
- A simple distance 3 repetition code is sufficient for reliable communication in the presence of noise.

References

Das, N., Paul, G., & Majumdar, R., arXiv:2101.03577, (2021).