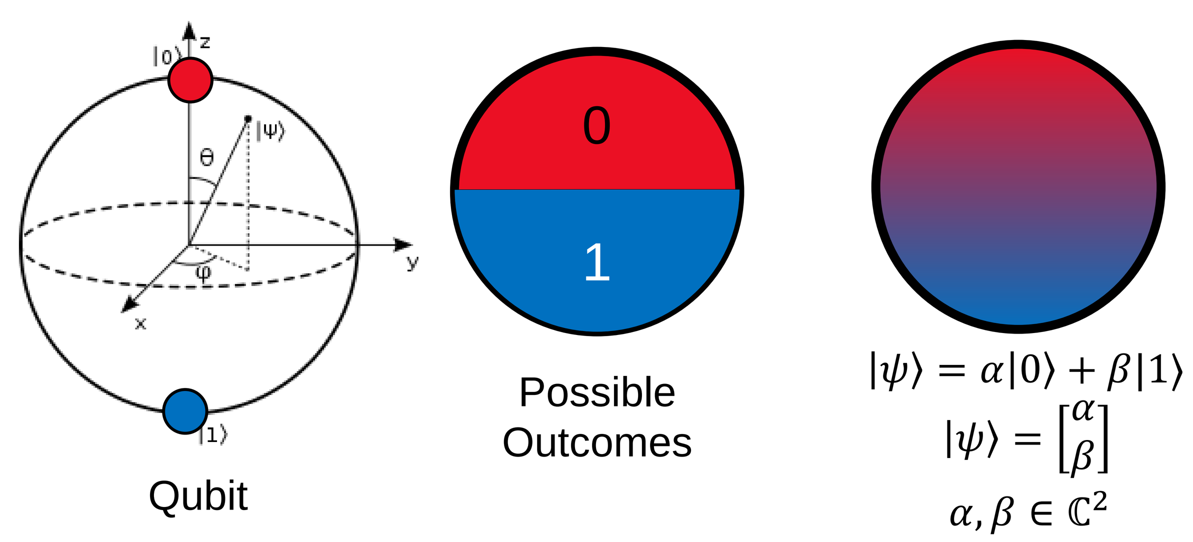
Modeling Adversarial Channels for Quantum Communication

Ashley Hart, RISE at Rutgers Scholar, University of Central Florida
Dr. Anand Sarwate, Rutgers University

RUTGERS THE STATE UNIVERSITY OF NEW JERSEY

1 INTRODUCTION & GOALS

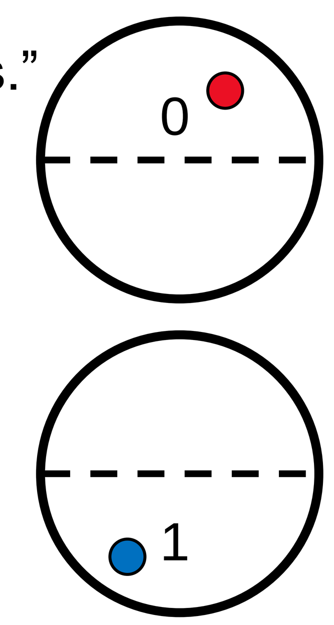
- **Problem:** Modern day communications face the problem of shrinking efficiency gains. [4]
- **Potential Solution:** Quantum computing, only if *reliable* quantum communication can be developed.
- **What is a qubit?** A super position of "basis states."



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$

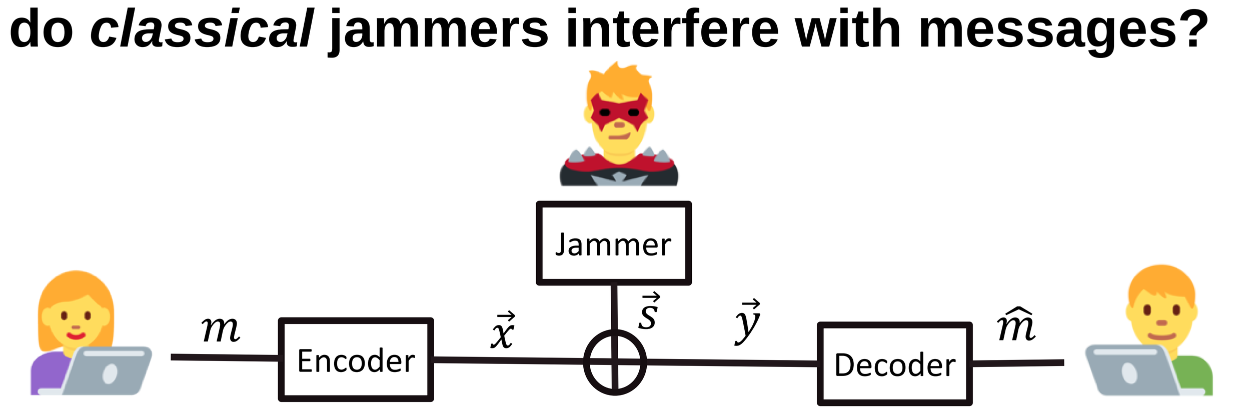
$\alpha, \beta \in \mathbb{C}^2$



- **Approach:** Modeling and comparing classical and quantum communication on arbitrarily varying channels (AVC).
- **Objective:** Exploring how quantum communication can occur in the presence of an adversary, or jammer on an AVC.
- **Research Question:** What abilities do adversaries possess on classical and quantum arbitrarily varying channels and how can we model them?

2 MODELING INTERFERENCE

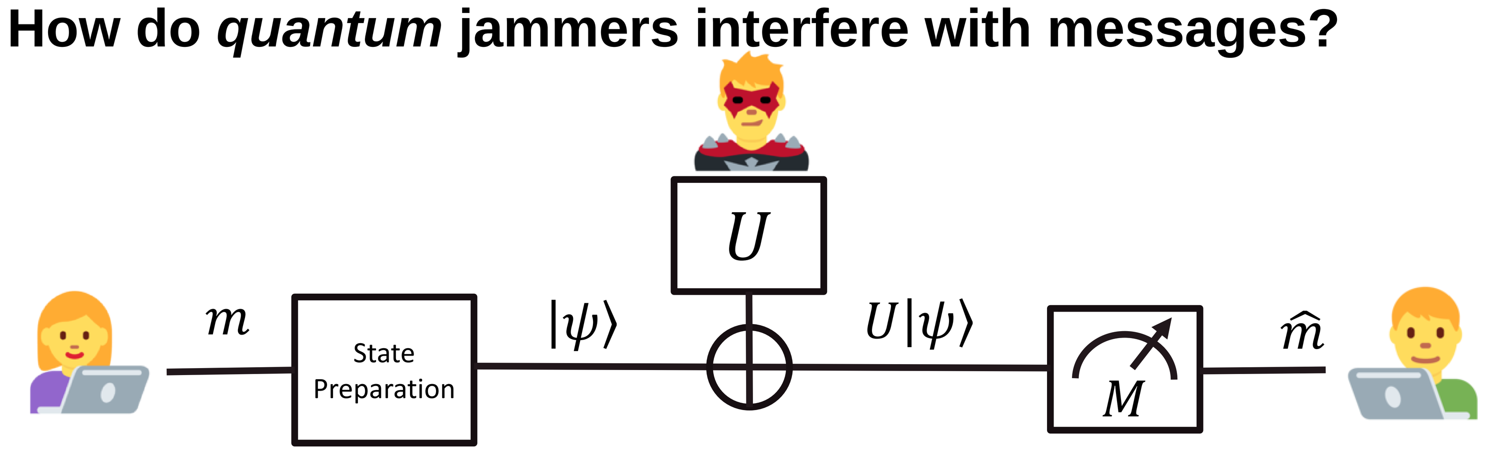
- **How do *classical* jammers interfere with messages?**



$$s^T = [\,0\;0\;1\;0\,]$$

$$m = 4 \longrightarrow \vec{x}^T = [\,0\;1\;0\;0\,] \longrightarrow \oplus \longrightarrow y^T = [\,0\;1\;1\;0\,] \longrightarrow \hat{m} = 6$$

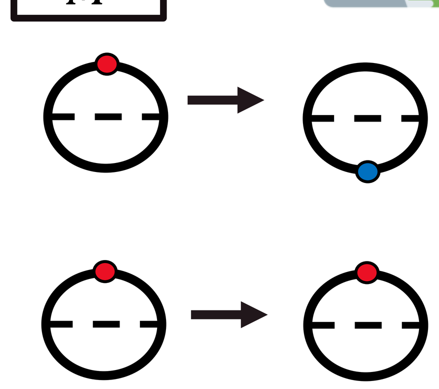
- **How do *quantum* jammers interfere with messages?**



Let $|\psi\rangle$ be our quantum state and $U = \{\sigma_X, I\}$ be the set of operations our jammer can use.

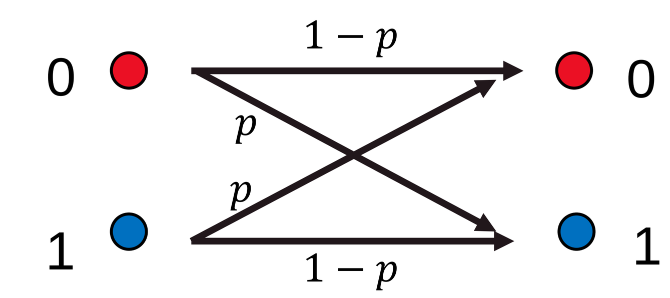
$$\sigma_X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$$I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

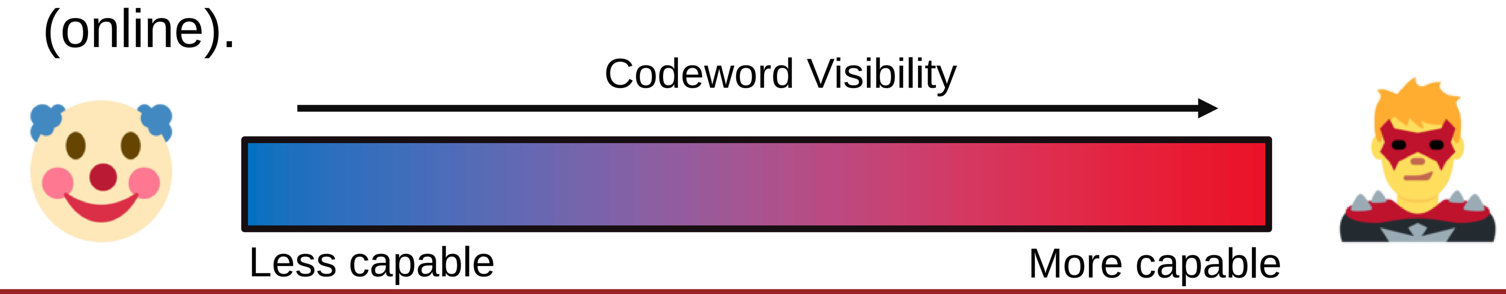


3 LEVELS OF INTERFERENCE

- Jammers that can see more of the codeword data will be able to damage our communication by altering our messages beyond repair.
- **The Shannon Model:** This model captures average-case interference. The jammer cannot see the data and errors occur *randomly* with some probability p.



- **The Hamming Model:** This model captures worst-case interference where the jammer can see the codewords and tailor his interference. At most pn bits can be flipped where p is the probability of a bit flip and n is the number of bits.
- **Intermediate Models (AVCs):** These capture both the Shannon and Hamming models and models that exist between them.
  - The jammer may see a noisy version of the codeword (myopic) or they may view the codeword bits in a sequence (online).



4 FUNDAMENTAL DIFFERENCES

- **Why do we care?** Fundamental rules of quantum mechanics changes how jammers can view our codewords.

- **Quantum State Evolution:** All operations on our quantum state must be *unitary evolutions* U, or *measurements.*
- **Quantum State Collapse:** When a state is measured, it will *collapse* to one of the basis states of the qubit. Therefore, although qubits can represent a lot of data, only a small amount can be extracted.
- **Entanglement:** Describes qubits in a state that cannot be broken into independent parts. Entangled qubits can be transmitted over quantum AVCs.
- **The No-cloning Theorem:** No unitary operator U exists that will take $|\psi\rangle \otimes |\omega\rangle$ to $|\psi\rangle \otimes |\psi\rangle$. In other words, *there is no universal method for copying one qubit state onto another.*
- **Note:** Separable qubit states may be represented by the *tensor product* (denoted by $\otimes$), of the qubits in the system.

5 THE JAMMER'S NEW RULEBOOK

- **What does the jammer want to do?**
  - To view the codeword at least partially
  - To eavesdrop on the channel
  - To manipulate the data without the sender or receiver's knowledge
- **Significance of quantum state collapse:** The adversary cannot evaluate the qubits without collapsing them. This will alarm the receiver that a third-party manipulated the message.
- **Significance of the no-cloning theorem:** Prevents our adversary from copying the codeword data. Raises questions on if the adversary can even see the codeword at all.
- **Significance of entanglement:** Usable as a resource, allowing sender and receiver to know when the entangled qubit has been measured.
- **What models for quantum communication do we have?**
  - The jammer randomly flips qubits
  - The jammer predetermines which qubits to flip. (May be viewed as a special case to the random qubit flip model.)
- **Conclusion:** We cannot simply import classical intermediate models into a quantum setting. Jammers are limited in what they can do which bodes well for reliable quantum communication.

6 FUTURE WORK

The QR code below will take you to a repository where you can follow work on this project. Our next steps include:

- Examining the quantum AVC model proposed by Ahlswede, et al. [1] for leads on intermediate quantum adversaries.
- Exploring quantum analogues to myopic and online adversaries. [2] [3]
- Studying how entanglement can be used as a resource for quantum communication. [5]

7 ACKNOWLEDGEMENTS

- Dr. Anand Sarwate (Rutgers ECE)
- Dr. Emina Soljanin (Rutgers ECE)
- Dr. Evelyn Erenrich (Rutgers RISE)
- Jessica Johnson (Rutgers RISE)
- National Science Foundation: Award CCF- 1909468
- UCF Ronald E. McNair Scholars Program
- RISE at Rutgers 2021 Cohort and Staff
- Image Credit: Emojipedia

8 REFERENCES

[1] Ahlswede, R., and Blinovsky, V. Classical capacity of classical-quantum arbitrarily varying channels. IEEE Transactions on Information Theory 53, 2 (2007), 526–533.
[2] Budkuley, A., Dey, B. K., Jaggi, S., Langberg, M., Sarwate, A. D., Wang, C., and Zhang,Y. Codes for adversaries: Between worst-case and average-case jamming. Manuscript in preparation2021.
[3] Soljanin, E. Quantum information processing: An essential primer. IEEE Journal on Selected Areas in Information Theory 1, 2 (2020), 351–366.
[4]Theis, T. N., and Wong, H.-S. P. The end of Moore's law: A new beginning for information technology. Computing in Science & Engineering 19, 2 (2017), 41–50
[5] Wilde, M. M. Quantum information theory. Cambridge University Press, 2013.