National Aeronautics and Space Administration

Exploration & SPACE Communications

More than you ever imagined...

Chaotic Quantum Key Distribution

By: Noah Cowper, NASA Goddard Space Flight Center

Mentor: Harry Shaw, NASA Goddard Space Flight Center

Introduction

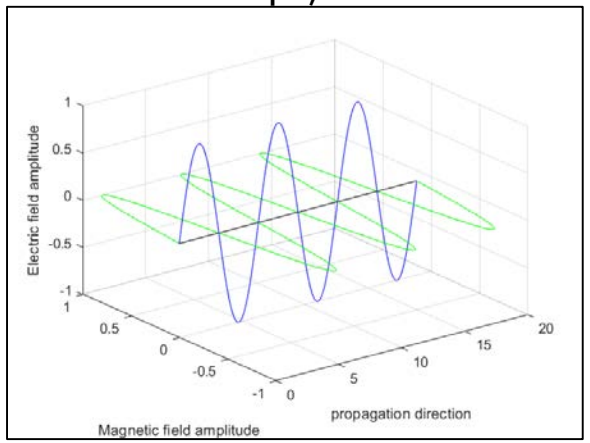
- Quantum Key Distribution (QKD) utilizes the polarization state of photons to establish a secret key between a sender and receiver.

$$\{|0\rangle, |+\rangle\} = 1 \ \ and \ \{|1\rangle, |-\rangle\} = 0$$

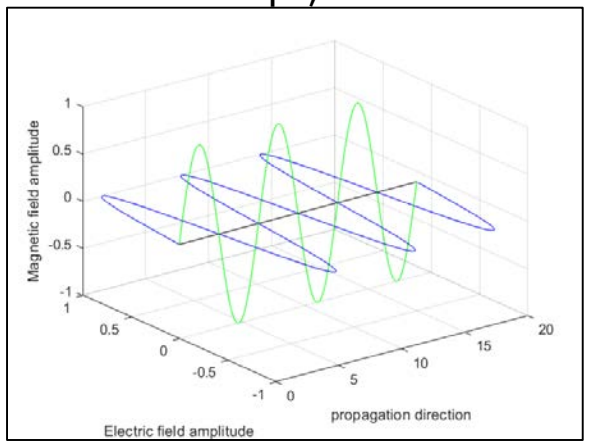
- Measurement in the wrong basis causes a collapse into a random state, since states in one basis can be written as a superposition of the corresponding states in the other basis.

$$|+\rangle \ = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$|0\rangle$

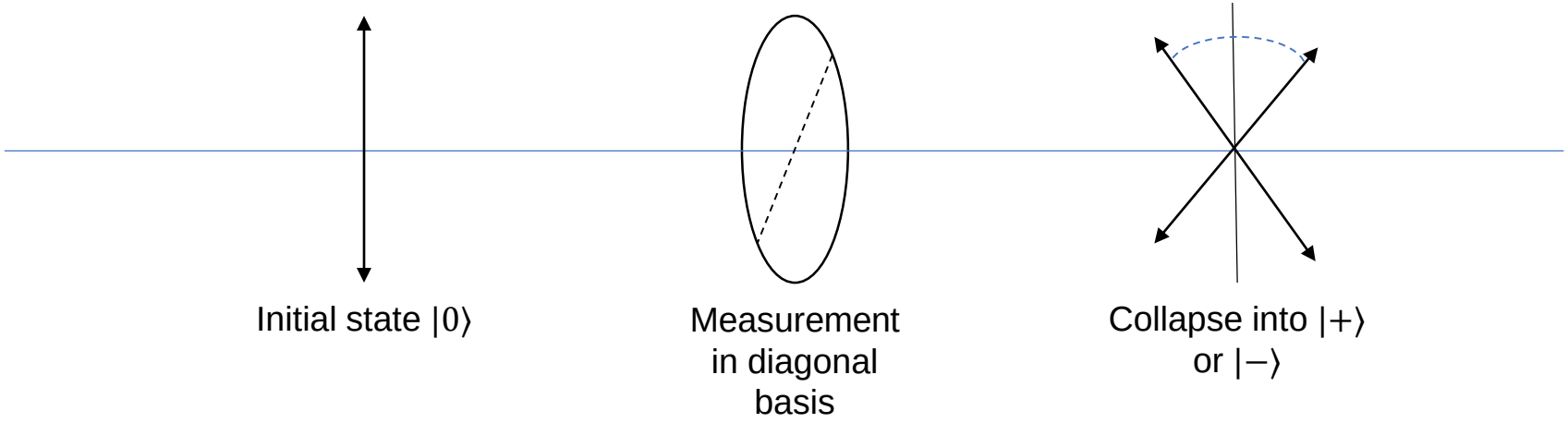


$|1\rangle$



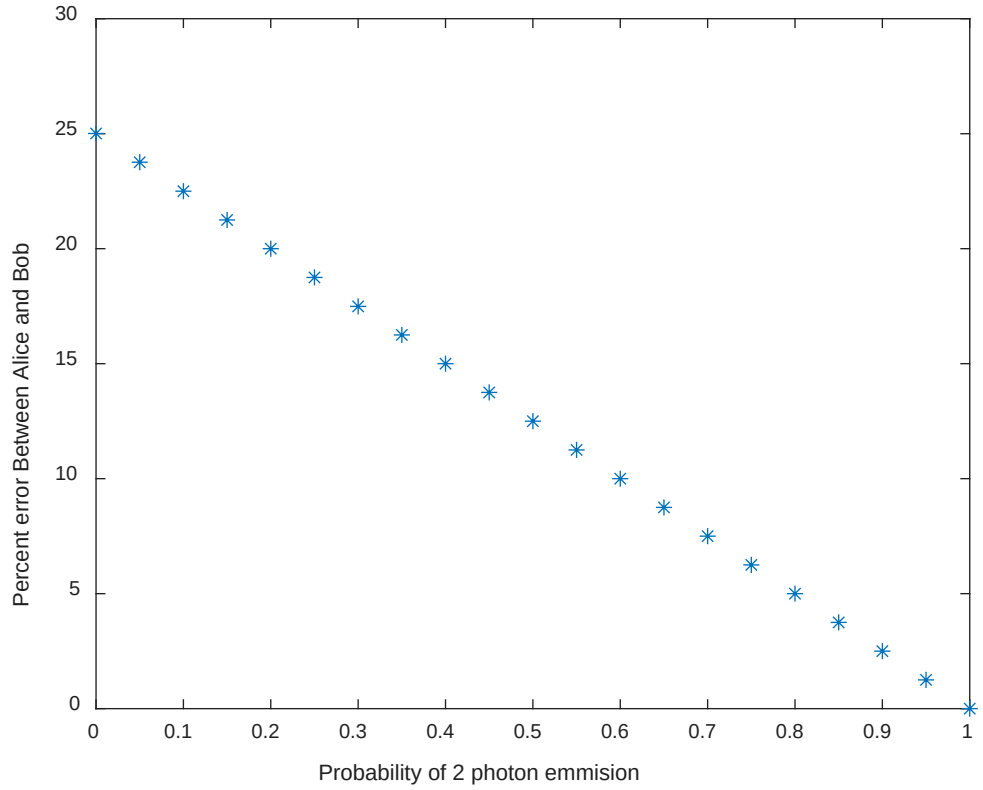
Eavesdropper

Measurement of the photons can only be done in 1 basis, and measurement of a photon in the wrong basis destroys the information encoded on it.



Quantum Key Distribution (QKD) Problems

- Theoretically QKD is a secure form of communication, but proofs of security rely on single photon emissions.
- Due to the nonideality of experimental setups single photon sources can only be probabilistic.
- Multiphoton emissions allow eavesdropper to be undetected in their measurement of the channel.

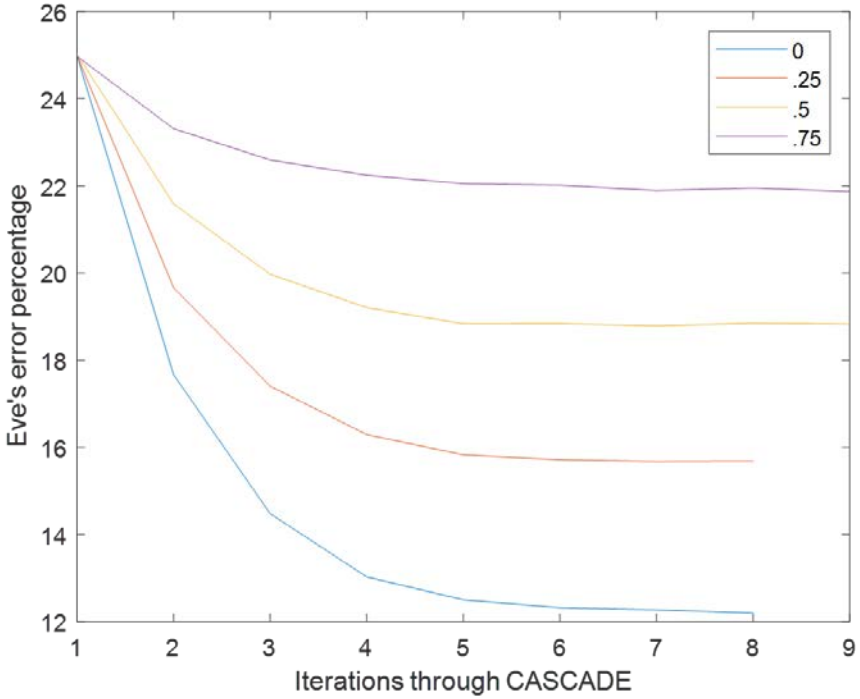


Mayers, D.; Unconditional Security in Quantum Cryptography. J. of the ACM **2001**,48, 351–406.

Information Accessible to Eavesdropper

- Eavesdropper can know up to 75% of the key information just from key establishment.
- Lower bound in eavesdropper error percentage of 12.5%.
- Gains information by selecting correct polarization basis (50% of the key).
- Obtains another 25% by guessing bit value.
- Last 12.5% is obtained by listening to key reconciliation.

Eve’s error percentage as the probability of double photon emission goes up.

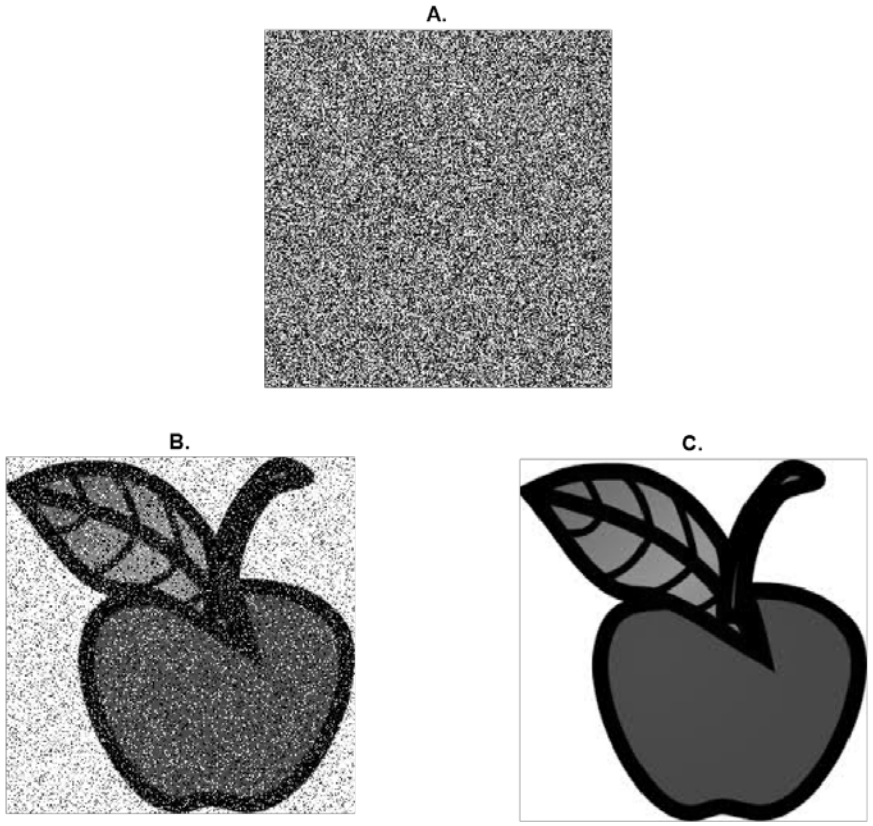


Encryption Using Classic QKD

Message	0	1	0	0	1	0
Encryption key	1	1	0	1	0	1
Transmitted message	0	1	1	0	0	0
Decryption key	1	1	0	1	0	1
Received Message	0	1	0	0	1	0

Bennett,C.H.;Brassard,G.; Public Key Distribution and Coin Tossing. Int. Conf. on Computers, systems and Signal Processing **1984**, 1, 175–179.

Simulation of Comm. Using Classic QKD

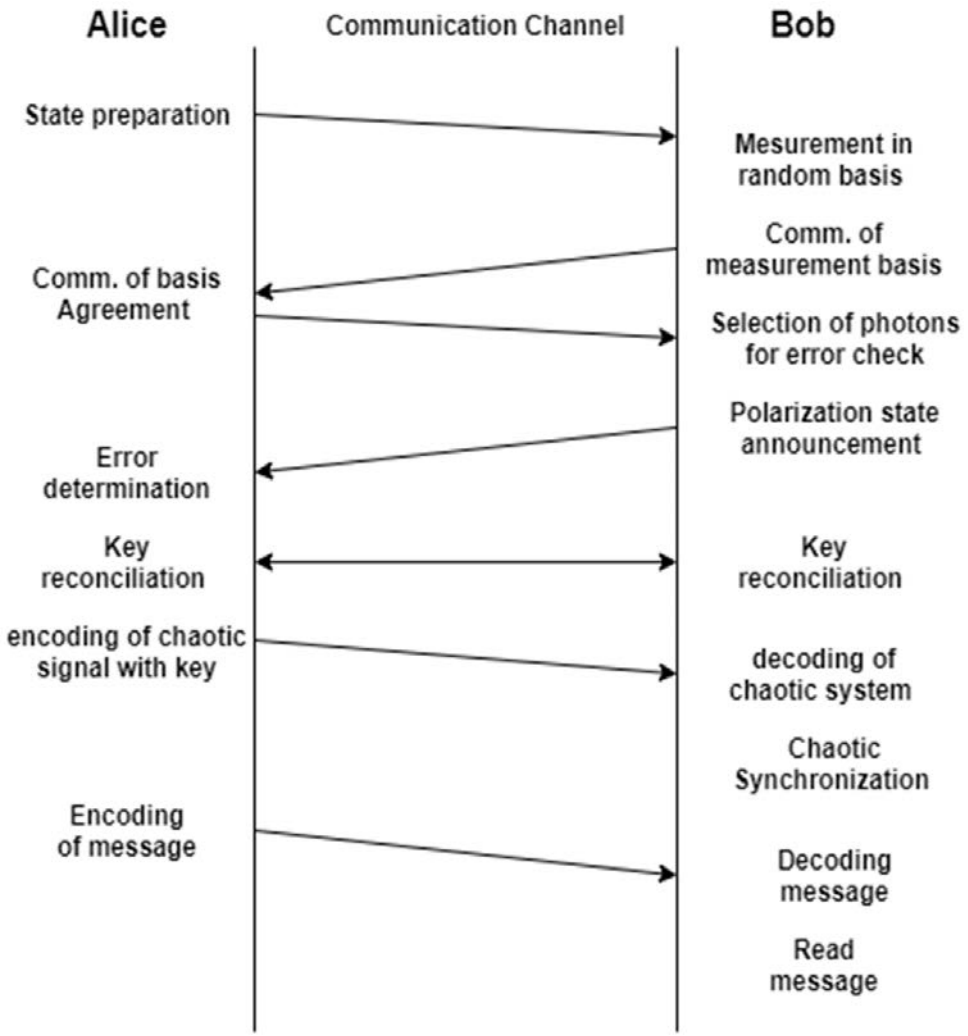


A: message in channel, B: message read by Eve, C: mess read by Bob

http://clipart-library.com/clipart/320465.htm

Proposed Protocol

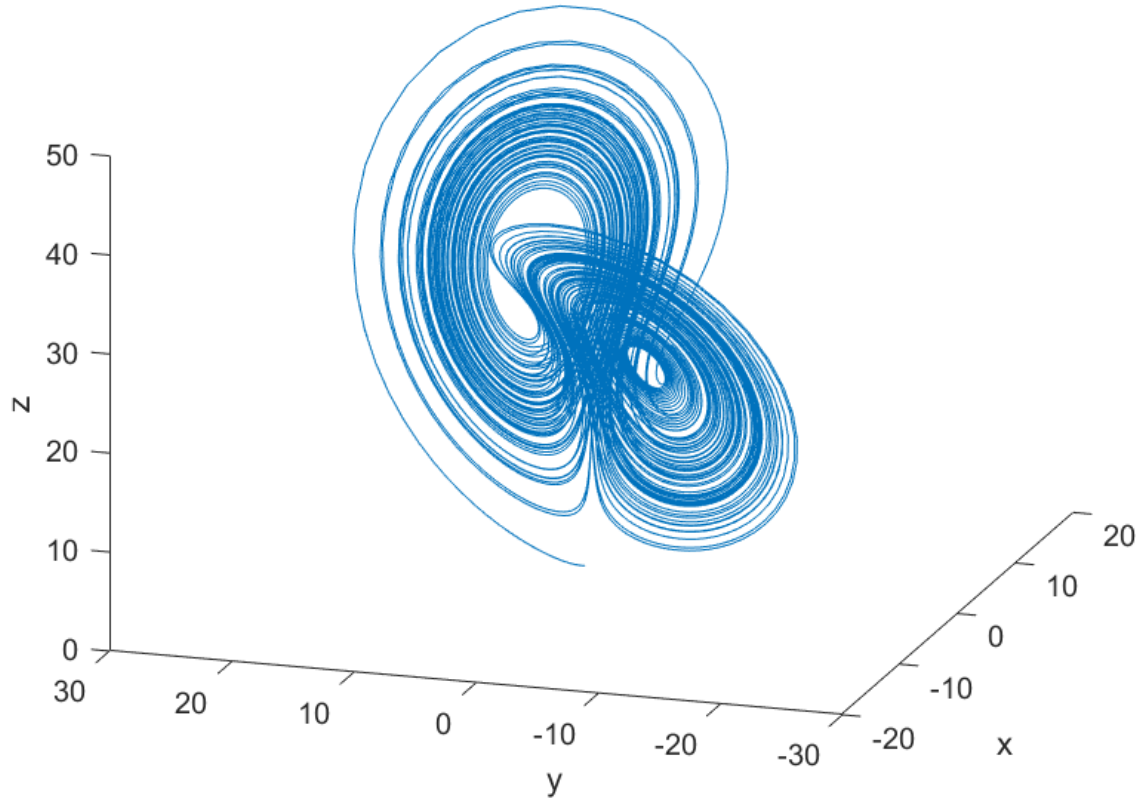
- Alice prepares a set of photons in a known polarization basis and state .
- Bob measures in a random basis and records the states obtained.
- Bob communicates classically to Alice what basis each photon was measured in.
- Alice tells Bob which photons were measured in the correct basis, and these become raw key between the two.
- Bob then selects a small portion of these and sends them to Alice for an error estimation.
- The two then correct the errors between their raw keys.
- Alice then uses her key to encode the generated chaotic solution and transmits it to Bob.
- Bob then uses his key to decode the message and then takes the solution and uses is to drive a corresponding chaotic system to reconstruct the set of solutions.
- Alice uses her other two solutions to encrypt the intended message and sends it to Bob.
- Bob uses his reconstructed solutions to decrypt and read the message.



Lorenz System

Solution to the Lorenz system

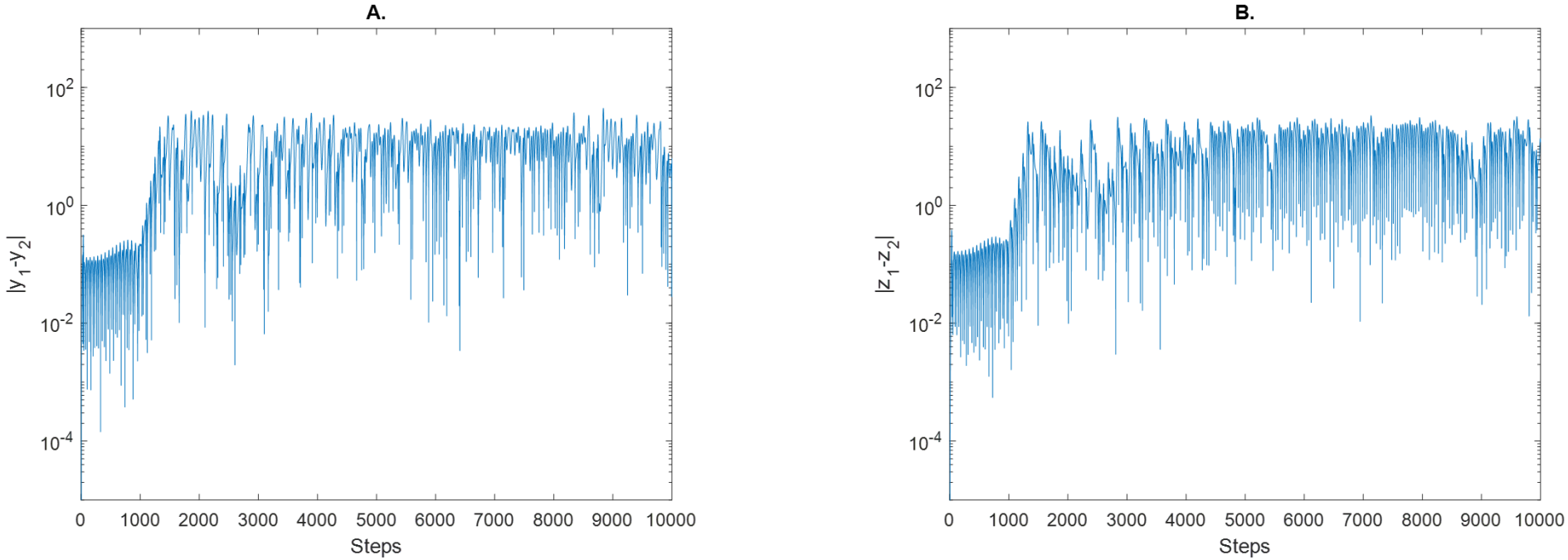
$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = \rho x - y - xz$$
$$\dot{z} = xy - \beta z$$



Lorenz, E.N.; Deterministic Nonperiodic. J ATMOS SCI **1963**, 20, 130–141

Chaotic Synchronization

Difference In y and z values of chaotic systems with an initial condition difference of 10e-5.



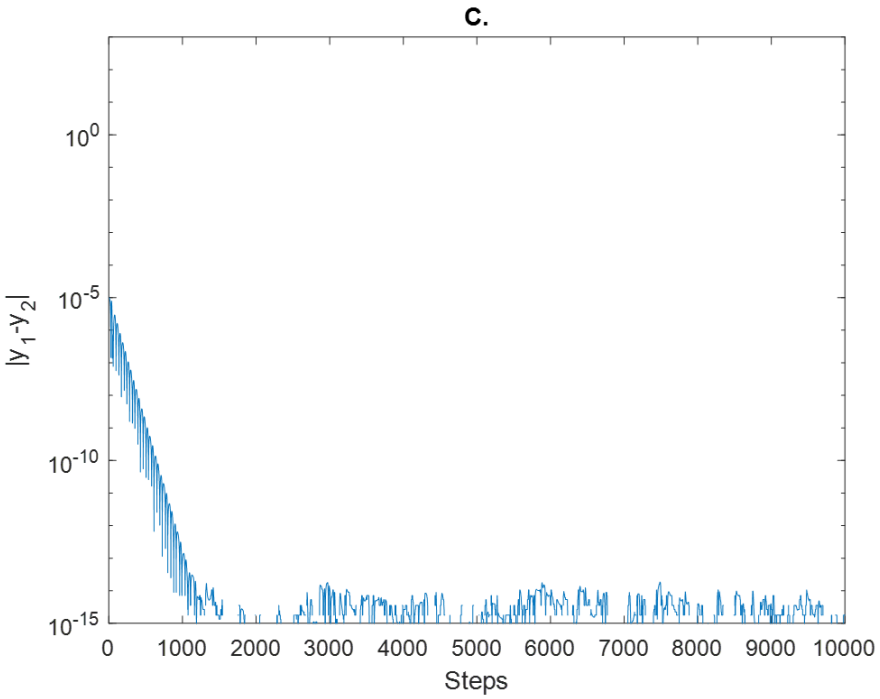
Lorenz equations

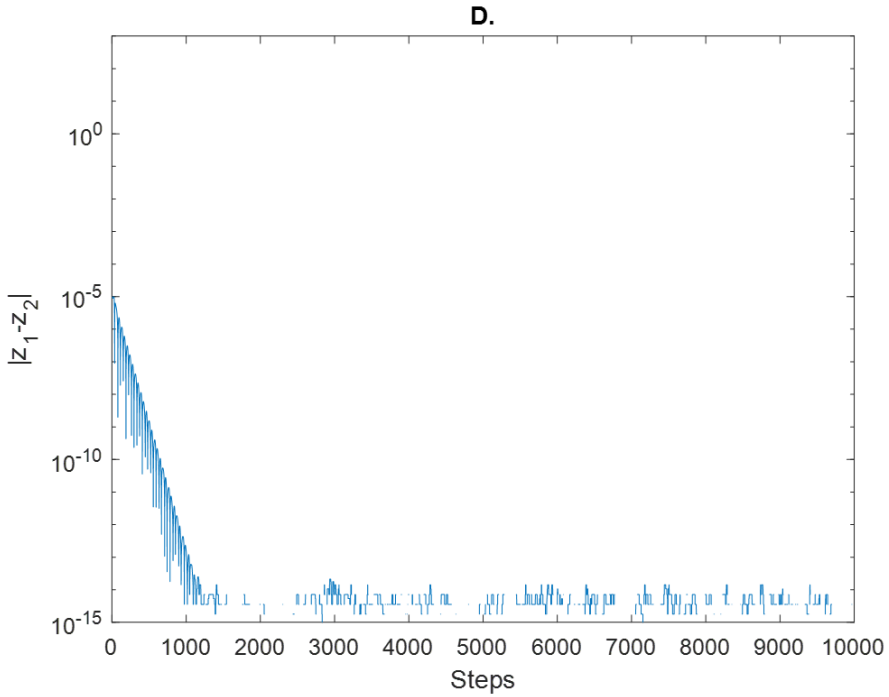
$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = \rho x - y - xz$$
$$\dot{z} = xy - \beta z$$

Lorenz, E.N.; Deterministic Nonperiodic. J ATMOS SCI **1963**, 20, 130–141.

Chaotic Synchronization

Difference of y and z values during Chaotic Synchronization





Drive System

$$\dot{x_d} = \sigma(y_d - x_d)$$
$$\dot{y_d} = \rho x_d - y_d - x_d z_d$$
$$\dot{z_d} = x_d y_d - \beta z_d$$

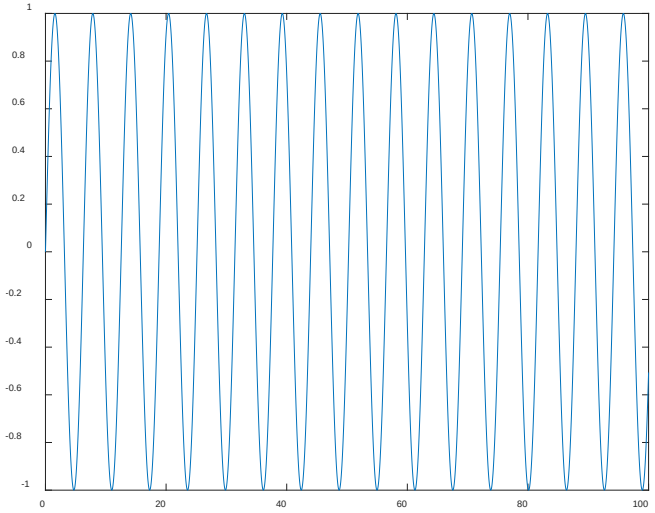
Response System

$$\dot{y_r} = \rho x_d - y_r - x_d z_r$$
$$\dot{z_r} = x_d y_r - \beta z_r$$

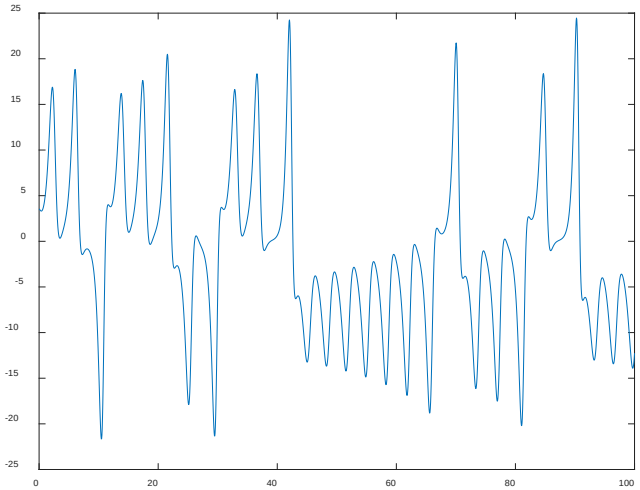
Pecora, L.M.; Carroll, T.L.; Synchronization in Chaotic Systems. PHYS. REV. LETT. **1990**, 64, 821–824.

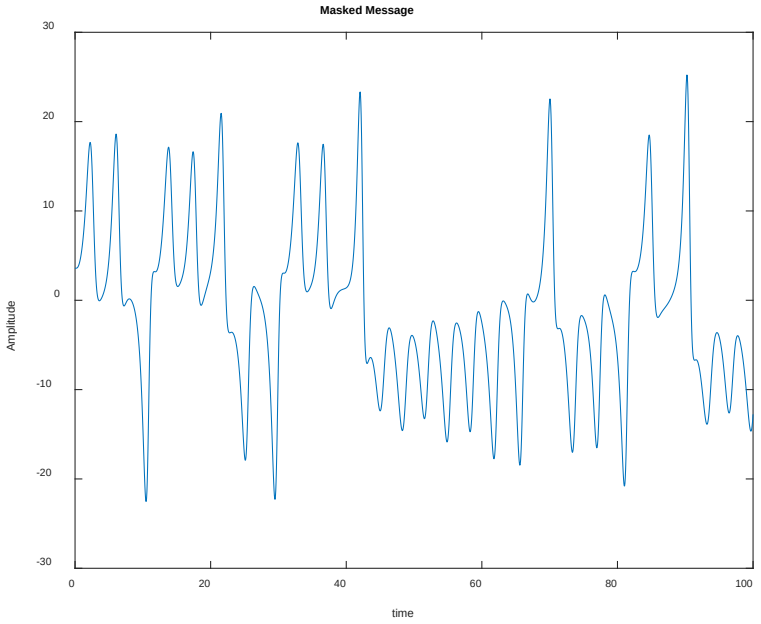
Encryption Using Chaotic QKD

Message

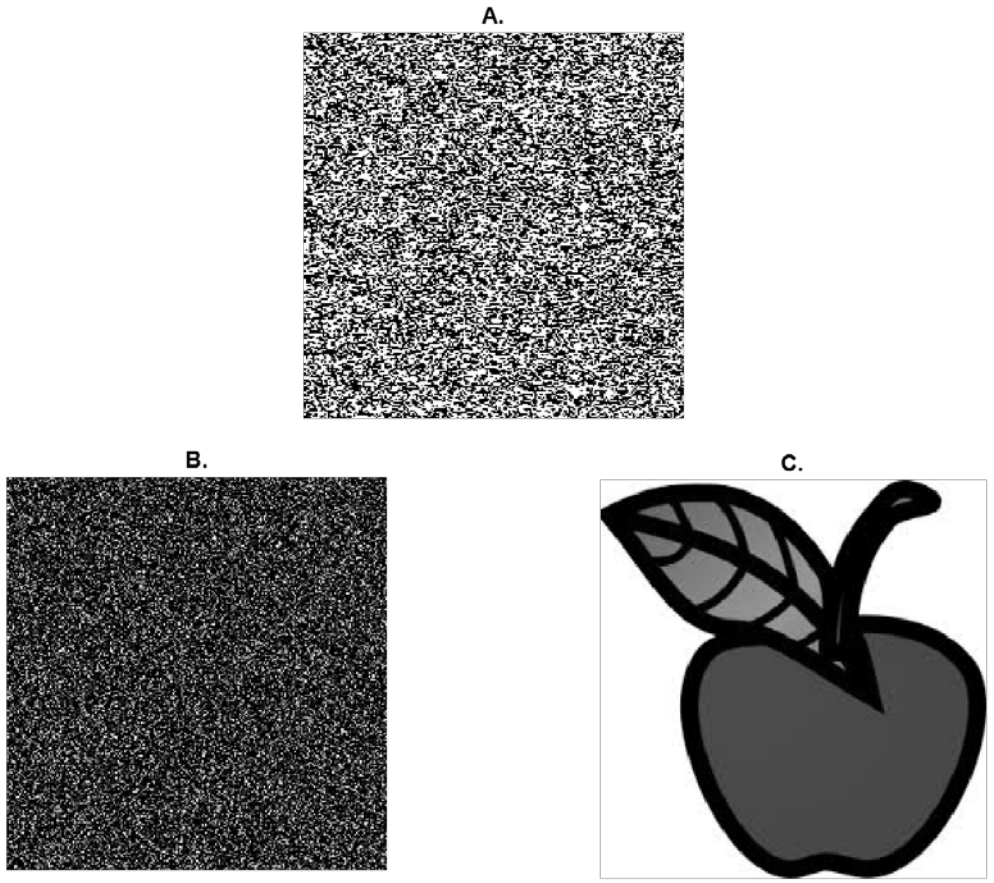


Chaotic Mask





Simulation of Comm. Using Chaotic QKD



A: message in channel, B: message read by Eve, C: mess read by Bob

Eve has the same amount of information as in classic QKD.

http://clipart-library.com/clipart/320465.htm

Advantages Over Previous Schemes

- BB84 protocol is vulnerable to number splitting attacks since single photons are probabilistic.
- Other chaotic QKD protocols encrypt parameters and initial conditions and send them over the quantum channel. The information required to obtain these 6 numbers is much less than obtaining one whole solution to the chaotic system.
- The proposed protocol allows the eavesdropper to gain their maximum amount of information about the key while still providing a secure form of communication.

Conclusions / Future Work

- Eavesdropper in a QKD protocol can gain at maximum 87.5% of the secret key.
- Chaotic QKD requires eavesdropper to have more knowledge of the key than they have access to.
- Chaotic QKD bypasses the problem of double photon emission since the knowledge of the key has to be so high.
- Chaotic QKD securely transmits information between two parties.

- The proposed protocol has been modeled but will requires lab implementation in order to verify its ability to securely transmit information. This will require a verification on the maximum information accessible to the eavesdropper and the ability of a distant party to reconstruct a chaotic solution from a received message.

Acknowledgements

I would like to extend my gratitude for helping with this project to.

- Dr. Harry Shaw
- Dr. Haleh Safavi
- Dr. Shantanu Gupta
- Dr. Mark Wan
- Jimmy Acevedo
- Dr. David Thayer

Acronyms Used:

- QKD: Quantum Key Distribution

Questions?