Quantum Cryptography

Secret Key Distribution

Tashfeen, Ahmad

Computer Science, University of Oklahoma

Exit Exam Presentation, Fall 2021

Overview

1. Introduction: we'll introduce and motivate some key ideas.
2. Quantum Mechanics: we'll present needed theorems and theory.
3. Bennett-Brassard 1984 Protocol: definition and example.
4. Real Working System: we'll see how this was done in the real world.
5. Conclusion & References

Introduction: Computational Security

Computational Security

Security due to computational intractability, i. e., security of the system is by the computational bottle neck of the time.

Introduction: Computational Security

Computational Security

Security due to computational intractability, i. e., security of the system is by the computational bottle neck of the time.

Rivest–Shamir–Adleman (RSA) relies on the prime factorisation,

$$pq \stackrel{?}{=} N \quad p, q \in P$$

Introduction: Computational Security

Computational Security

Security due to computational intractability, i. e., security of the system is by the computational bottle neck of the time.

Rivest–Shamir–Adleman (RSA) relies on the prime factorisation,

$$pq \stackrel{?}{=} N \quad p, q \in P$$

Diffie–Hellman key exchange relies on the discrete log,

$$\log_b a \mod m$$

Introduction: Computational Security

Computational Security

Security due to computational intractability, i. e., security of the system is by the computational bottle neck of the time.

Rivest–Shamir–Adleman (RSA) relies on the prime factorisation,

$$pq \stackrel{?}{=} N \quad p, q \in P$$

Diffie–Hellman key exchange relies on the discrete log,

$$\log_b a \mod m$$

Vigenère cipher was broken after three centuries of no solutions [4].

Introduction: Computational Security

Computational Security

Security due to computational intractability, i. e., security of the system is by the computational bottle neck of the time.

Rivest–Shamir–Adleman (RSA) relies on the prime factorisation,

$$pq \stackrel{?}{=} N \quad p, q \in P$$

Diffie–Hellman key exchange relies on the discrete log,

$$\log_b a \mod m$$

Vigenère cipher was broken after three centuries of no solutions [4].

Could there be a system that is *provably secure* and independent of the current *computational resources*?

Introduction: Information Theoretic Security

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$e(m) \equiv m + k \mod 2$ Alice

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$e(m) \equiv m + k \mod 2 \qquad \text{Alice}$$

$$d(e(m)) \equiv e(m) + k \mod 2 \qquad \text{Bob}$$

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$
\begin{aligned}
e(m) &\equiv m + k \mod 2 && \text{Alice} \\
d(e(m)) &\equiv e(m) + k \mod 2 && \text{Bob} \\
&\equiv m + k + k \mod 2
\end{aligned}
$$

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$
\begin{aligned}
e(m) &\equiv m + k \mod 2 && \text{Alice} \\
d(e(m)) &\equiv e(m) + k \mod 2 && \text{Bob} \\
&\equiv m + k + k \mod 2 \\
&\equiv m + 2k \mod 2
\end{aligned}
$$

Introduction: Information Theoretic Security

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$\begin{aligned} e(m) &\equiv m + k \mod 2 && \text{Alice} \\ d(e(m)) &\equiv e(m) + k \mod 2 && \text{Bob} \\ &\equiv m + k + k \mod 2 \\ &\equiv m + 2k \mod 2 \\ &\equiv m \mod 2 \end{aligned}$$

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$
\begin{aligned}
e(m) &\equiv m + k \mod 2 && \text{Alice} \\
d(e(m)) &\equiv e(m) + k \mod 2 && \text{Bob} \\
&\equiv m + k + k \mod 2 \\
&\equiv m + 2k \mod 2 \\
&\equiv m \mod 2
\end{aligned}
$$

Key space is infinite!

Information Theoretic Security

Security independent of computational resources, i. e., cipher text provides no information about the plaintext.

Vernam cipher found in 1920s (a.k.a. one-time pad), proved to be information theoretically secure by Shannon in 1949 [2].

$$\begin{aligned} e(m) &\equiv m + k \mod 2 && \text{Alice} \\ d(e(m)) &\equiv e(m) + k \mod 2 && \text{Bob} \\ &\equiv m + k + k \mod 2 \\ &\equiv m + 2k \mod 2 \\ &\equiv m \mod 2 \end{aligned}$$

Key space is infinite!

$$e(m) + k : \texttt{ATTACKATDAWN} \quad \& \quad e(m) + k' : \texttt{ATTACKATNOON}$$

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message No information about the m is known other than its length $\lg(m)$.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message No information about the m is known other than its length $\lg(m)$.

Random Key k must be truly random.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message No information about the m is known other than its length $\lg(m)$.

Random Key k must be truly random.

Unique Key k must never be reused.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message No information about the m is known other than its length $\lg(m)$.

Random Key k must be truly random.

Unique Key k must never be reused.

Key length k must be as long as the message $\lg(k) = \lg(m)$.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message No information about the m is known other than its length $\lg(m)$.

Random Key k must be truly random.

Unique Key k must never be reused.

Key length k must be as long as the message $\lg(k) = \lg(m)$.

Eve must not have any information of k.

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

- **Message** No information about the m is known other than its length $\lg(m)$.
- **Random Key** k must be truly random.
- **Unique Key** k must never be reused.
- **Key length** k must be as long as the message $\lg(k) = \lg(m)$.
- **Eve** must not have any information of k.
- **Trivial?** Even though these requirements may seem trivial...

Introduction: One time pad

For the information theoretic security, we need the message m and key k to full some requirements.

Message: No information about the m is known other than its length $\lg(m)$.

Random Key: k must be truly random.

Unique Key: k must never be reused.

Key length: k must be as long as the message $\lg(k) = \lg(m)$.

Eve: must not have any information of k.

Trivial?: Even though these requirements may seem trivial...

No!: Generating such a k in real life is hard. How do Alice and Bob generate such a k at two different place? Remember, we are now talking about info. theoretically secure.

Introduction: Key Machine

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Ideal $\forall k, P(k) = 2^{-|k|}$.

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Ideal $\forall k, P(k) = 2^{-|k|}$.

Relaxed Close to uniform randomness and n bits don't tell anything about $(n+1)^{th}$ bit.

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Ideal $\forall k, P(k) = 2^{-|k|}$.

Relaxed Close to uniform randomness and n bits don't tell anything about $(n+1)^{th}$ bit.

Ideal Eve can't meddle with the machine.

Introduction: Key Machine

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Ideal $\forall k, P(k) = 2^{-|k|}$.

Relaxed Close to uniform randomness and n bits don't tell anything about $(n+1)^{th}$ bit.

Ideal Eve can't meddle with the machine.

Relaxed Eve may meddle with the machine, but we should be able to tell!

Introduction: Key Machine

- Ideal: gen. k', k s. t. $k = k'$.
- Relaxed: $P(k' \neq k) \leq \varepsilon$.
- Ideal: $\forall k, P(k) = 2^{-|k|}$.
- Relaxed: Close to uniform randomness and n bits don't tell anything about $(n+1)^{th}$ bit.
- Ideal: Eve can't meddle with the machine.
- Relaxed: Eve may meddle with the machine, but we should be able to tell!

Figure: xkcd.com/1240/

Ideal gen. k', k s. t. $k = k'$.

Relaxed $P(k' \neq k) \leq \varepsilon$.

Ideal $\forall k, P(k) = 2^{-|k|}$.

Relaxed Close to uniform randomness and n bits don't tell anything about $(n+1)^{th}$ bit.

Ideal Eve can't meddle with the machine.

Relaxed Eve may meddle with the machine, but we should be able to tell!

Figure: xkcd.com/1240/

Quantum Mechanics!

Quantum Mechanics: Desirable Properties

Quantum Mechanics: Desirable Properties

Inherent randomness Qunta have an inherent randomness with respect to their states and being able to measure those states, i. e., observation may cause the state to change (meddling detection)!

Quantum Mechanics: Desirable Properties

Inherent randomness Qunta have an inherent randomness with respect to their states and being able to measure those states, i. e., observation may cause the state to change (meddling detection)!

No-Cloning theorem Unlike classical states, quantum states can not always be cloned. E. g., you can make a copy of a document but that does not copy the polarisation states of all the ink-photons from the original to the new document.

Quantum Mechanics: Classical Bits vs. Quantum Bits

Quantum Mechanics: Classical Bits vs. Quantum Bits

- We know a classical bit can be in one of the two states, let ψ be the state of the bit then,

$$\psi \in \{0, 1\}, \quad P(\psi = 1) = P(\psi = 2) = \frac{1}{2}$$

- We know a classical bit can be in one of the two states, let ψ be the state of the bit then,

$$\psi \in \{0, 1\}, \quad P(\psi = 1) = P(\psi = 2) = \frac{1}{2}$$

- Quantum Bit (qubit) $|\psi\rangle$,

$$\begin{aligned} |\psi\rangle &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} & \alpha, \beta \in \mathbb{C} \\ &= \begin{pmatrix} \alpha \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \beta \end{pmatrix} \\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \alpha |0\rangle + \beta |1\rangle & |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$

Quantum Mechanics: Quantum Bit States' Probability

Quantum Mechanics: Quantum Bit States' Probability

Born's Rule

The probability that a quantum state $|\psi\rangle$ will collapse into one of the possible classical states $|0\rangle, |1\rangle$ upon observation is, e. g.,

$$P(|\psi\rangle = |0\rangle) = ||\alpha||^2 = |a + bi| \cdot |a - bi| = a^2 + b^2$$

Quantum Mechanics: Quantum Bit States' Probability

Born's Rule

The probability that a quantum state $|\psi\rangle$ will collapse into one of the possible classical states $|0\rangle, |1\rangle$ upon observation is, e. g.,

$$P(|\psi\rangle = |0\rangle) = ||\alpha||^2 = |a + bi| \cdot |a - bi| = a^2 + b^2$$

- Then the qubit is more precisely defined as,

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad ||\alpha||^2 + ||\beta||^2 = 1 \quad \text{Hilbert Space over } \mathbb{C}^2$$

Quantum Mechanics: Schrodinger's Cat

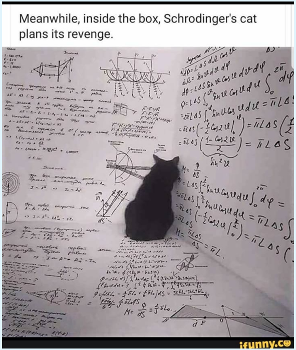

Figure: Schrodinger's cat.

- What if $\alpha = \beta = \frac{1}{\sqrt{2}}$?

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}\,|\text{dead}\rangle + \frac{1}{\sqrt{2}}\,|\text{alive}\rangle$$

$$\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$$

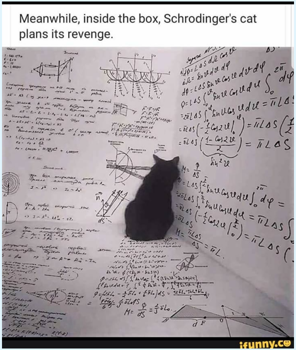

Figure: Schrodinger's cat.

Quantum Mechanics: Schrodinger's Cat

- What if $\alpha = \beta = \frac{1}{\sqrt{2}}$?

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}\,|\text{dead}\rangle + \frac{1}{\sqrt{2}}\,|\text{alive}\rangle$$

$$\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$$

- What is the probability of cat being either dead or alive? What is the quantum state of the cat?

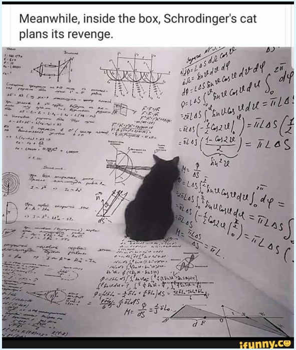

Figure: Schrodinger's cat.

Quantum Mechanics: Schrodinger's Cat

- What if $\alpha = \beta = \frac{1}{\sqrt{2}}$?

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}|\text{dead}\rangle + \frac{1}{\sqrt{2}}|\text{alive}\rangle$$

$$\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$$

- What is the probability of cat being either dead or alive? What is the quantum state of the cat?
- Two such quantum states,

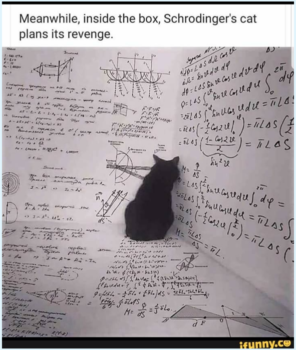

Figure: Schrodinger's cat.

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Quantum Mechanics: Orthogonal States

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

Computational Basis:

Hadamard Basis:

Quantum Mechanics: Orthogonal States

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

Computational Basis:

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha = 1, \beta = 0$.

Hadamard Basis:

Quantum Mechanics: Orthogonal States

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

Computational Basis:

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$ for $\alpha = 1, \beta = 0.$
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$ for $\alpha = 0, \beta = 1.$

Hadamard Basis:

Quantum Mechanics: Orthogonal States

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

Computational Basis:

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$ for $\alpha = 1, \beta = 0$.
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$ for $\alpha = 0, \beta = 1$.

Hadamard Basis:

- $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$ for $\alpha = \frac{1}{\sqrt{2}}, \beta = \frac{1}{\sqrt{2}}$.

Quantum Mechanics: Orthogonal States

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

Computational Basis:

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha = 1, \beta = 0$.
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha = 0, \beta = 1$.

Hadamard Basis:

- $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha = \frac{1}{\sqrt{2}}, \beta = \frac{1}{\sqrt{2}}$.
- $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha = \frac{1}{\sqrt{2}}, \beta = -\frac{1}{\sqrt{2}}$.

Quantum Mechanics: Measuring States

Quantum Mechanics: Measuring States

- We have to know which basis were used for encoding to be sure of the measurement results.

Quantum Mechanics: Measuring States

- We have to know which basis were used for encoding to be sure of the measurement results.
- Measurements are defined by a matrix,

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Quantum Mechanics: Measuring States

- We have to know which basis were used for encoding to be sure of the measurement results.
- Measurements are defined by a matrix,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- If we know the original basis used for encoding, we observe a state with probability 1!

Quantum Mechanics: Measurement Examples

Quantum Mechanics: Measurement Examples

$$\mathbb{I}\,|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

Quantum Mechanics: Measurement Examples

$$\mathbb{I}\left|0\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left|0\right\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

$$\mathbb{I}\left|1\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left|1\right\rangle \qquad ||\beta||^2 = ||1||^2 = 1$$

Quantum Mechanics: Measurement Examples

$$\mathbb{I}\,|0\rangle = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = |0\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

$$\mathbb{I}\,|1\rangle = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = |1\rangle \qquad ||\beta||^2 = ||1||^2 = 1$$

$$H|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |0\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

Quantum Mechanics: Measurement Examples

$$\mathbb{I}\,|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

$$\mathbb{I}\,|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad ||\beta||^2 = ||1||^2 = 1$$

$$H|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |0\rangle \qquad ||\alpha||^2 = ||1||^2 = 1$$

$$H|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |1\rangle \qquad ||\beta||^2 = ||1||^2 = 1$$

Quantum Mechanics: Measurement Examples

Quantum Mechanics: Measurement Examples

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

Quantum Mechanics: Measurement Examples

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

Quantum Mechanics: Measurement Examples

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$\mathbb{I}\,|+\rangle = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

Quantum Mechanics: Measurement Examples

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$\mathbb{I}\,|+\rangle = |+\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

$$\mathbb{I}\,|-\rangle = |-\rangle \qquad ||\alpha||^2 = ||\beta||^2 = \frac{1}{2}$$

Quantum Mechanics: Desirable Properties

Quantum Mechanics: Desirable Properties

Inherent randomness Qunta have an inherent randomness with respect to their states and being able to measure those states, i. e., observation may cause the state to change (meddling detection)!

Quantum Mechanics: Desirable Properties

Inherent randomness Qunta have an inherent randomness with respect to their states and being able to measure those states, i. e., observation may cause the state to change (meddling detection)!

No-Cloning theorem Unlike classical states, quantum states can not always be cloned. E. g., you can make a copy of a document but that does not copy the polarisation states of all the ink-photons from the original to the new document.

Quantum Mechanics: Linearity

Quantum Mechanics: Linearity

Linearity Axiom of Quantum Mechanics [4]

For all functions U of $|\psi\rangle$ as in $U|\psi\rangle$, U is a matrix. I. e., quantum mechanics is linear.

Quantum Mechanics: Linearity

Quantum Mechanics: Linearity

Proof by contradiction of the no-cloning theorem.

Quantum Mechanics: Linearity

Proof by contradiction of the no-cloning theorem.

1. Assume there exists as a universal copier U then,

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \end{aligned}$$

Quantum Mechanics: Linearity

Proof by contradiction of the no-cloning theorem.

1. Assume there exists as a universal copier U then,

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \end{aligned}$$

2. While since U is a matrix by the axiom above,

$$\begin{aligned} U|\psi\rangle|0\rangle &= U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \\ &= \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle \\ &= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \qquad U|1\rangle|0\rangle = |1\rangle|1\rangle \end{aligned}$$

$$\alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \neq \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$$

Proof by contradiction of the no-cloning theorem.

1. Assume there exists as a universal copier U then,

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \end{aligned}$$

2. While since U is a matrix by the axiom above,

$$\begin{aligned} U|\psi\rangle|0\rangle &= U(\alpha|0\rangle + \beta|1\rangle)|0\rangle \\ &= \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle \\ &= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \end{aligned} \qquad U|1\rangle|0\rangle = |1\rangle|1\rangle$$

$$\alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \neq \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$$

3. Only true for classical states, $(\alpha, \beta) = (0, 1)$ or $(\alpha, \beta) = (1, 0)$.

QUOD ERAT DEM■

Bennett-Brassard 1984 (BB84): Qubit Realisation

Bennett-Brassard 1984 (BB84): Qubit Realisation

1. A classical bit is the current or a lack thereof on the wire.

Bennett-Brassard 1984 (BB84): Qubit Realisation

1. A classical bit is the current or a lack thereof on the wire.
2. What is a qubit?

Bennett-Brassard 1984 (BB84): Qubit Realisation

1. A classical bit is the current or a lack thereof on the wire.
2. What is a qubit?
3. It can be implemented in many ways, e. g., nitrogen atoms (spin based), photons (polarisation based).

Bennett-Brassard 1984 (BB84): Qubit Realisation

1. A classical bit is the current or a lack thereof on the wire.
2. What is a qubit?
3. It can be implemented in many ways, e. g., nitrogen atoms (spin based), photons (polarisation based).
4. "The polarization of light specifies the geometrical orientation of the oscillation of the electromagnetic field associated with its wave [4]".

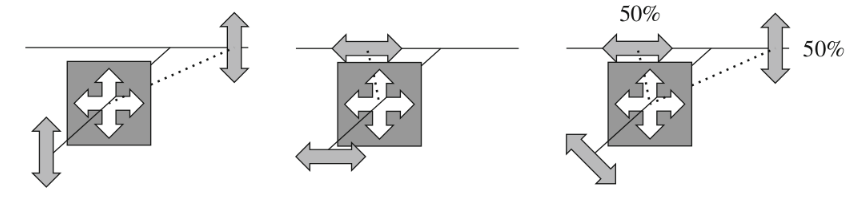

Figure: Polarisation filters corresponding to the $\mathbb{I}$ and H [4].

BB84 Protocol: Steps

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

3. Bob also generates a bit string b' of length $4n$.

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

3. Bob also generates a bit string b' of length $4n$.
4. Bob receives the qubits and measures them in $\mathbb{I}$ or H according to b'.

$$a_i' = \texttt{decode}(|a_i\rangle) = \begin{cases} \mathbb{I}\,|a_i\rangle, & b_i = 0 \\ H|a_i\rangle, & b_i = 1 \end{cases}$$

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

3. Bob also generates a bit string b' of length $4n$.
4. Bob receives the qubits and measures them in $\mathbb{I}$ or H according to b'.

$$a'_i = \texttt{decode}(|a_i\rangle) = \begin{cases} \mathbb{I}\,|a_i\rangle, & b_i = 0 \\ H|a_i\rangle, & b_i = 1 \end{cases}$$

5. Alice shares b with Bob over a public channel and they discard any a_i, a'_i where $b_i \neq b'_i$. Now there are approximately $2n$ bits leftover.

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

3. Bob also generates a bit string b' of length $4n$.
4. Bob receives the qubits and measures them in $\mathbb{I}$ or H according to b'.

$$a'_i = \texttt{decode}(|a_i\rangle) = \begin{cases} \mathbb{I}\,|a_i\rangle\,, & b_i = 0 \\ H|a_i\rangle\,, & b_i = 1 \end{cases}$$

5. Alice shares b with Bob over a public channel and they discard any a_i, a'_i where $b_i \neq b'_i$. Now there are approximately $2n$ bits leftover.
6. Alice and Bob compare n bits to check for error and eavesdropping.

BB84 Protocol: Steps

1. Alice randomly generates two classical bit strings a, b of length $4n$.
2. Then if $b_i = 1$ Alice encodes a_i in Hadamard basis as a qubit, computational basis otherwise.

$$\texttt{encode}(a_i) \in \begin{cases} \{|0\rangle, |1\rangle\}, & b_i = 0 \\ \{|+\rangle, |-\rangle\}, & b_i = 1 \end{cases}$$

3. Bob also generates a bit string b' of length $4n$.
4. Bob receives the qubits and measures them in $\mathbb{I}$ or H according to b'.

$$a'_i = \texttt{decode}(|a_i\rangle) = \begin{cases} \mathbb{I}\,|a_i\rangle, & b_i = 0 \\ H|a_i\rangle, & b_i = 1 \end{cases}$$

5. Alice shares b with Bob over a public channel and they discard any a_i, a'_i where $b_i \neq b'_i$. Now there are approximately $2n$ bits leftover.
6. Alice and Bob compare n bits to check for error and eavesdropping.
7. If the error is explained by the amount of noise present, then they take the remaining n bits as the shared key.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\lvert+\rangle$	$\lvert 1\rangle$	$\lvert-\rangle$	$\lvert-\rangle$	$\lvert 0\rangle$	$\lvert-\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert-\rangle$	$\lvert+\rangle$	$\lvert+\rangle$	$\lvert 1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1
$b \stackrel{?}{=} b'$	OK	OK		OK	OK	OK				OK		OK

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1
$b \stackrel{?}{=} b'$	OK	OK		OK	OK	OK				OK		OK
Sifted	0	1		1	0	1				0		1

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1
$b \stackrel{?}{=} b'$	OK	OK		OK	OK	OK				OK		OK
Sifted	0	1		1	0	1				0		1
$a \stackrel{?}{=} a'$	0	1								0		1

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1
$b \stackrel{?}{=} b'$	OK	OK		OK	OK	OK				OK		OK
Sifted	0	1		1	0	1				0		1
$a \stackrel{?}{=} a'$	0	1								0		1
$a = a'$	OK	OK								OK		OK

Table: BB84 Example.

BB84 Protocol: Example

Alice's a	0	1	1	1	0	1	0	1	1	0	0	1
Alice's b	H	$\mathbb{I}$	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$	H	H	H	$\mathbb{I}$
Qubits	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's b'	H	$\mathbb{I}$	$\mathbb{I}$	H	$\mathbb{I}$	H	H	H	$\mathbb{I}$	H	$\mathbb{I}$	$\mathbb{I}$
Bob's a'	0	1	0	1	0	1	1	1	0	0	0	1
$b \stackrel{?}{=} b'$	OK	OK		OK	OK	OK				OK		OK
Sifted	0	1		1	0	1				0		1
$a \stackrel{?}{=} a'$	0	1								0		1
$a = a'$	OK	OK								OK		OK
Key				1	0	1						

Table: BB84 Example.

Real Word Problems

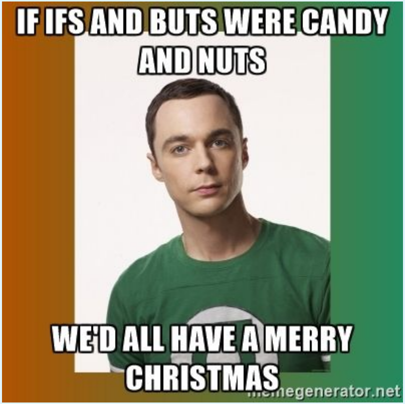

Figure: Idiom on theory.

Real Word Problems: Noise

NOISE

Real Word Problems: Noise

NOISE

If we have a lot of noise, then how do we tell the difference between changes due to eavesdropping and just channel lose?

Real Word Problems: Checks

- How many checks with the assumption of no noise? Let ε be the probability that we fail to detect Eve.

$$\lceil -\lg(\varepsilon) \rceil$$

Real Word Problems: Checks

- How many checks with the assumption of no noise? Let ε be the probability that we fail to detect Eve.

$$\lceil -\lg(\varepsilon) \rceil$$

- But with noise δ, we need,

$$\lceil -nf(\delta)\lg(\varepsilon) \rceil, \quad f(\delta) = \begin{cases} 0.0015, & \delta > 0.001 \\ -\lg(\delta^{0.04}) + 0.29 & \end{cases}$$

Real Word Problems: Checks

- How many checks with the assumption of no noise? Let ε be the probability that we fail to detect Eve.

$$\lceil -\lg(\varepsilon) \rceil$$

- But with noise δ, we need,

$$\lceil -nf(\delta)\lg(\varepsilon) \rceil, \quad f(\delta) = \begin{cases} 0.0015, & \delta > 0.001 \\ -\lg(\delta^{0.04}) + 0.29 & \end{cases}$$

- This was the result of my undergraduate honours thesis [3].

Real Word Problems: Avoiding Noise

- The channel loss (of fibres and terrestrial free-space) is not avoidable.

Real Word Problems: Avoiding Noise

- The channel loss (of fibres and terrestrial free-space) is not avoidable.
- Signal strength (number of photons) can not be amplified due to no-cloning.

Real Word Problems: Avoiding Noise

- The channel loss (of fibres and terrestrial free-space) is not avoidable.
- Signal strength (number of photons) can not be amplified due to no-cloning.
- The maximum distance Quantum Key Distribution (QKD) was done within is about 13 km.

Real Word Problems: Avoiding Noise

- The channel loss (of fibres and terrestrial free-space) is not avoidable.
- Signal strength (number of photons) can not be amplified due to no-cloning.
- The maximum distance Quantum Key Distribution (QKD) was done within is about 13 km.
- Can you think of a solution?

Real Word Problems: Satellites

- Earth's atmosphere is about 480 km thick, but most of it is 16 km of the sea-level.

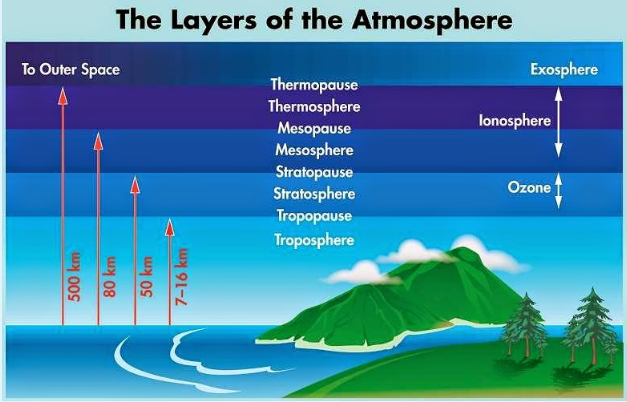

Figure: edugeneral.org.

Real Word Problems: Satellites

- Earth's atmosphere is about 480 km thick, but most of it is 16 km of the sea-level.
- Space is mostly noiseless!

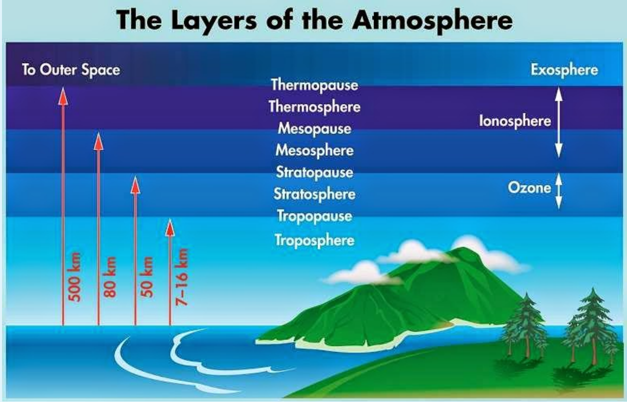

Figure: edugeneral.org.

Real Word Problems: Micius [1]

- Named after an ancient Chinese scholar and scientist.

Real Word Problems: Micius [1]

- Named after an ancient Chinese scholar and scientist.
- Set off on 16^{th} August 2016 from Jiuquan, China.

Real Word Problems: Micius [1]

- Named after an ancient Chinese scholar and scientist.
- Set off on 16^{th} August 2016 from Jiuquan, China.
- Flies in a sun-synchronous orbit at the altitude of about 500 km.

Real Word Problems: Micius [1]

- Named after an ancient Chinese scholar and scientist.
- Set off on 16^{th} August 2016 from Jiuquan, China.
- Flies in a sun-synchronous orbit at the altitude of about 500 km.

Figure: Wikipedia and extremetech.com

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.
- What about the link efficiency?

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.
- What about the link efficiency?
- There are three major error inducing factors.

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.
- What about the link efficiency?
- There are three major error inducing factors.
- Beam diffraction.

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.
- What about the link efficiency?
- There are three major error inducing factors.
- Beam diffraction.
- Pointing Error.

Challenges

- Micius aims to perform QKD with the ground observatory in Xinglong.
- What about the link efficiency?
- There are three major error inducing factors.
- Beam diffraction.
- Pointing Error.
- Turbulence and absorption.

Challenges: Beam diffraction

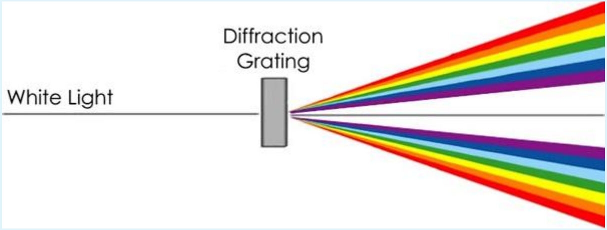

Figure: Diffraction

- What causes this since we are in space?

Challenges: Beam diffraction

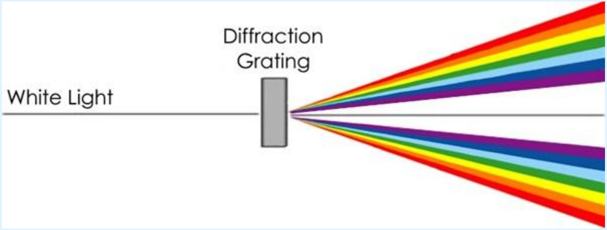

Figure: Diffraction

- What causes this since we are in space?
- The telescope sending the photons.

Challenges: Beam diffraction

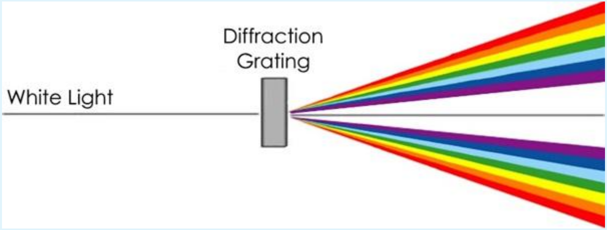

Figure: Diffraction

- What causes this since we are in space?
- The telescope sending the photons.
- Diffraction loss is about 22dB at 1200km.

$$22\text{dB} \Rightarrow 10^{-22/10} \approx 10^{-2} = \frac{1}{100}\text{times less photons.}$$

Challenges: Beam diffraction

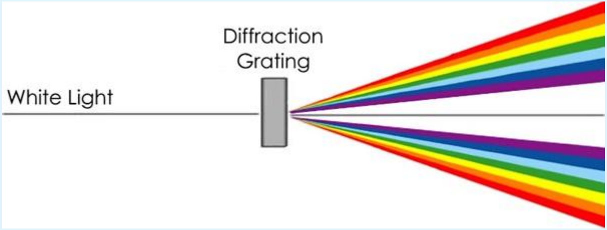

Figure: Diffraction

- What causes this since we are in space?
- The telescope sending the photons.
- Diffraction loss is about 22dB at 1200km.

$$22\text{dB} \Rightarrow 10^{-22/10} \approx 10^{-2} = \frac{1}{100} \text{times less photons.}$$

- Solution: Cassegrain telescope.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.

Figure: From the paper.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.
- Solution: Acquiring, Pointing and Tracking (APT) system.

Figure: From the paper.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.
- Solution: Acquiring, Pointing and Tracking (APT) system.
- Initial coarse orientation is done by forecast position of satellite in orbit ($\sim 0.5^\circ$). Green beacon beams and feedback closed loop.

Figure: From the paper.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.
- Solution: Acquiring, Pointing and Tracking (APT) system.
- Initial coarse orientation is done by forecast position of satellite in orbit ($\sim 0.5^\circ$). Green beacon beams and feedback closed loop.

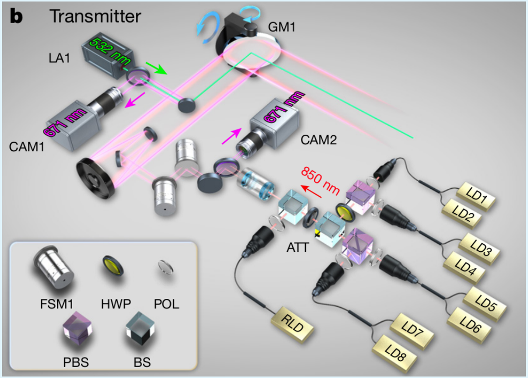

Figure: From the paper.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.
- Solution: Acquiring, Pointing and Tracking (APT) system.
- Initial coarse orientation is done by forecast position of satellite in orbit ($\sim 0.5^\circ$). Green beacon beams and feedback closed loop.

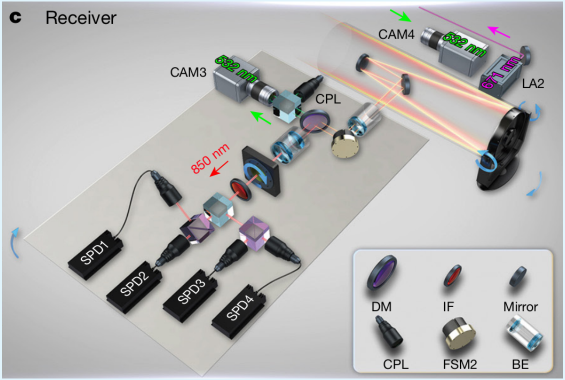

Figure: From the paper.

Challenges: Pointing Error

- Error caused by the ground and satellite telescope not being in line.
- Solution: Acquiring, Pointing and Tracking (APT) system.
- Initial coarse orientation is done by forecast position of satellite in orbit ($\sim 0.5^\circ$). Green beacon beams and feedback closed loop.

Figure: From the paper.

Challenges: Turbulence and Absorption

- Error caused by weather conditions and external lights.
- Solution: operate during night.

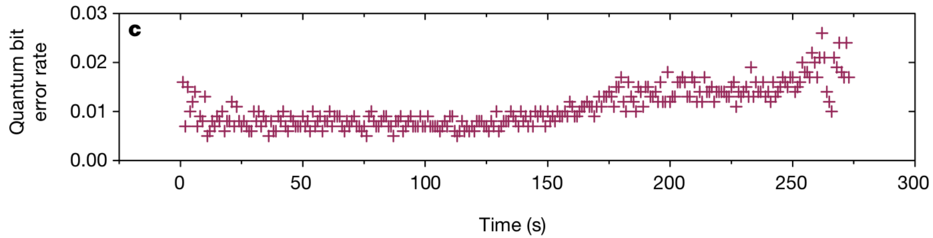

Figure: Beijing to the south of Xinglong (Right side of the graph).

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.
- The APT system starts and the bidirectional beams are used to lock the transmitter and receiver points.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.
- The APT system starts and the bidirectional beams are used to lock the transmitter and receiver points.
- At an elevation angle of 15°, when everything is pointing correctly and locked, quantum key exchanges start.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.
- The APT system starts and the bidirectional beams are used to lock the transmitter and receiver points.
- At an elevation angle of 15°, when everything is pointing correctly and locked, quantum key exchanges start.
- At an elevation angle of 10°, on the other side, a single orbit experiment ends.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.
- The APT system starts and the bidirectional beams are used to lock the transmitter and receiver points.
- At an elevation angle of 15°, when everything is pointing correctly and locked, quantum key exchanges start.
- At an elevation angle of 10°, on the other side, a single orbit experiment ends.
- The entire process takes about 5 minutes.

Key Exchange: Experiments

- Sun synchronous orbit: Passes the same point on earth at the same time everyday.
- Micius passes the ground station at around 12:50 PM local time.
- At an elevation angle of 5°, pointing accuracy of 0.5° is achieved.
- The APT system starts and the bidirectional beams are used to lock the transmitter and receiver points.
- At an elevation angle of 15°, when everything is pointing correctly and locked, quantum key exchanges start.
- At an elevation angle of 10°, on the other side, a single orbit experiment ends.
- The entire process takes about 5 minutes.
- We wait for the next day.

Key Exchange: Results

- QKD performed routinely since September 2016 under good weather.

Key Exchange: Results

- QKD performed routinely since September 2016 under good weather.
- Performed key exchange successfully at a distance of 1200km with over 1000 Hz key rate.

Key Exchange: Results

- QKD performed routinely since September 2016 under good weather.
- Performed key exchange successfully at a distance of 1200km with over 1000 Hz key rate.
- 20 orders of magnitude more efficient than optic fibre as a channel.

Key Exchange: Results

- QKD performed routinely since September 2016 under good weather.
- Performed key exchange successfully at a distance of 1200km with over 1000 Hz key rate.
- 20 orders of magnitude more efficient than optic fibre as a channel.

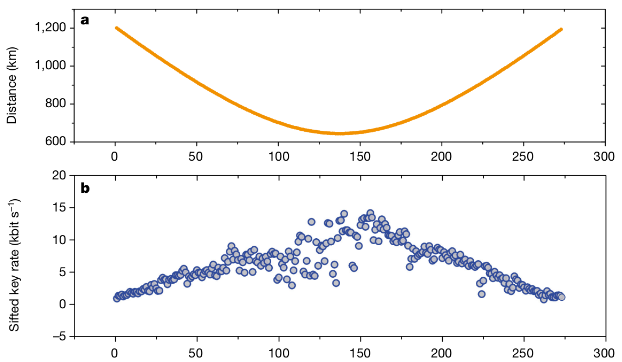

Figure: From the paper, Time (s)

In the News

BBC | Home | News | Sport | Reel | Worklife

Home | Coronavirus | Climate | Video | World | US & Canada | UK | Business

Science

China's quantum satellite in big leap

By Roland Pease
BBC Radio Science Unit

15 June 2017 | Comments

Micius went up from the Jiuquan Satellite Launch Centre in China's north west

The term "spy satellite" has taken on a new meaning with the successful test of a novel Chinese spacecraft.

Figure: BBC news article about the project.

Conclusion

1. Computational security has no proof of security.
2. Information theoretical security and one-time pad.
3. Description for a key machine.
4. Quantum mechanics for definition a quantum bit.
5. Proof of no-cloning theorem.
6. Bennett-Brassard 1984 protocol for Quantum key exchange.
7. Quantum key exchange in the real world using a satellite.

References

Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al.
Satellite-to-ground quantum key distribution.
Nature, 549(7670):43–47, 2017.

Claude E Shannon.
Communication theory of secrecy systems.
The Bell system technical journal, 28(4):656–715, 1949.

Ahmad Tashfeen.
Error and noise analysis in a quantum key exchange.
2018.

Ramona Wolf.
Quantum Key Distribution: An Introduction with Exercises, volume 988.
Springer Nature, 2021.

Thank You!

Questions?