Symmetric Incoherent Eavesdropping against MDI QKD

Arpita Maitra[1] and Goutam Paul[2]

[1]Indian Statistical Institute, Kolkata, India
[2]Jadavpur University, Kolkata, India

WCC 2013, Bergen, Norway
April 18, 2013

Outline

1. Review of Quantum Information

Outline

1. Review of Quantum Information
2. Key Distribution using BB84
   - The Protocol
   - Security Issues

Outline

Outline

Outline

Outline

Outline

Roadmap

Basic Quantum Algebra for a Single Particle

Basic Quantum Algebra for a Single Particle

- The state $|\psi\rangle$ of a single particle is a normalized complex vector $\begin{pmatrix}\alpha \\ \beta\end{pmatrix}$ in two dimensions.

Basic Quantum Algebra for a Single Particle

- The state $|\psi\rangle$ of a single particle is a normalized complex vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ in two dimensions.
- A standard measurement is an orthonormal basis $\{|m_1\rangle, |m_2\rangle\}$ of two dimensional complex vectors. If the initial state is $|\psi\rangle$, then after the measurement, the probability of the outcome $|m_i\rangle$ is $|\langle\psi|m_i\rangle|^2$.

Basic Quantum Algebra for a Single Particle

- The state $|\psi\rangle$ of a single particle is a normalized complex vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ in two dimensions.
- A standard measurement is an orthonormal basis $\{|m_1\rangle, |m_2\rangle\}$ of two dimensional complex vectors. If the initial state is $|\psi\rangle$, then after the measurement, the probability of the outcome $|m_i\rangle$ is $|\langle\psi|m_i\rangle|^2$.
- Every allowed reversible physical transformation on the state of a particle is represented by a 2×2 unitary matrix U.

Basic Quantum Algebra for a Single Particle

- The state $|\psi\rangle$ of a single particle is a normalized complex vector $\begin{pmatrix}\alpha \\ \beta\end{pmatrix}$ in two dimensions.
- A standard measurement is an orthonormal basis $\{|m_1\rangle, |m_2\rangle\}$ of two dimensional complex vectors. If the initial state is $|\psi\rangle$, then after the measurement, the probability of the outcome $|m_i\rangle$ is $|\langle\psi|m_i\rangle|^2$.
- Every allowed reversible physical transformation on the state of a particle is represented by a 2×2 unitary matrix U.
- The basis $\left\{ \begin{pmatrix}1 \\ 0\end{pmatrix}, \begin{pmatrix}0 \\ 1\end{pmatrix} \right\}$ is called the computational basis and is represented by $\{|0\rangle, |1\rangle\}$.

From One to Many Particles

From One to Many Particles

- For two particles in states $(\alpha_1|0\rangle + \beta_1|1\rangle)$ and $(\alpha_2|0\rangle + \beta_2|1\rangle)$, the joint state is given by the tensor product
  $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$
  $= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$,
  which is a complex vector in 4 dimensions.

From One to Many Particles

- For two particles in states $(\alpha_1|0\rangle + \beta_1|1\rangle)$ and $(\alpha_2|0\rangle + \beta_2|1\rangle)$, the joint state is given by the tensor product $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$ $= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$, which is a complex vector in 4 dimensions.
- In general, the state for n particles is a complex vector in 2^n-dimensional complex vector space (called a Hilbert Space).

Conjugate Bases

Conjugate Bases

- Suppose, $\{|\psi_i\rangle \ : \ i = 1, \ldots, N\}$ and $\{|\phi_i\rangle \ : \ i = 1, \ldots, N\}$ are two orthonormal bases for an N dimensional Hilbert space.

Conjugate Bases

- Suppose, $\{|\psi_i\rangle \; : \; i = 1, \ldots, N\}$ and $\{|\phi_i\rangle \; : \; i = 1, \ldots, N\}$ are two orthonormal bases for an N dimensional Hilbert space.
- The above pair of bases are called conjugate, if and only if $|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{N}$ for any i, j.

Conjugate Bases

- Suppose, $\{|\psi_i\rangle \ : \ i = 1, \ldots, N\}$ and $\{|\phi_i\rangle \ : \ i = 1, \ldots, N\}$ are two orthonormal bases for an N dimensional Hilbert space.
- The above pair of bases are called conjugate, if and only if $|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{N}$ for any i, j.
- For $N = 2$, the bases $\{|\psi_1\rangle, |\psi_2\rangle\}$ and $\{|\phi_1\rangle, |\phi_2\rangle\}$ are conjugate, if and only if we have $|\langle\psi_1|\phi_1\rangle|^2 = |\langle\psi_1|\phi_2\rangle|^2 = |\langle\psi_2|\phi_1\rangle|^2 = |\langle\psi_2|\phi_2\rangle|^2 = 1/2$.

Entanglement

Entanglement

- Consider the state

$$\gamma_1|00\rangle + \gamma_2|11\rangle$$

with $\gamma_1 \neq 0, \gamma_2 \neq 0$.

Entanglement

- Consider the state
$$\gamma_1|00\rangle + \gamma_2|11\rangle$$
with $\gamma_1 \neq 0, \gamma_2 \neq 0$.
- This cannot be written as a tensor product $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$.

Entanglement

- Consider the state
$$\gamma_1|00\rangle + \gamma_2|11\rangle$$
with $\gamma_1 \neq 0, \gamma_2 \neq 0$.
- This cannot be written as a tensor product $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$.
- This is called entanglement. An example of entangled state is
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Entanglement

- Consider the state
$$\gamma_1|00\rangle + \gamma_2|11\rangle$$
with $\gamma_1 \neq 0, \gamma_2 \neq 0$.
- This cannot be written as a tensor product $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$.
- This is called entanglement. An example of entangled state is
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$
- Physical meaning: knowledge of the state of one particle reveals the state of the other.

Roadmap

BB84 Protocol

BB84 Protocol

- C. H. Bennett and G. Brassard.
  Quantum Cryptography: Public key distribution and coin tossing.
  In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).

BB84 Protocol

- C. H. Bennett and G. Brassard.
  Quantum Cryptography: Public key distribution and coin tossing.
  In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).
- Uses two conjugate bases $+ = \{\uparrow, \rightarrow\}$ and $\times = \{\nearrow, \nwarrow\}$ to establish a secret key between two parties at a distance.

BB84 Protocol

- C. H. Bennett and G. Brassard.
  Quantum Cryptography: Public key distribution and coin tossing.
  In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, IEEE, New York (1984).
- Uses two conjugate bases $+ = \{\uparrow, \rightarrow\}$ and $\times = \{\nearrow, \nwarrow\}$ to establish a secret key between two parties at a distance.
- Suppose they fix the convention that the first vector in each basis represents 0 and the second vector in each basis represents 1.

A Pictorial Description

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Basic Eavesdropping: Measure and Resend

Basic Eavesdropping: Measure and Resend

- No cloning theorem (Wooters & Zurek, Nature 299, 1982) assures that Eve cannot replicate a particle of unknown state.

Basic Eavesdropping: Measure and Resend

- No cloning theorem (Wooters & Zurek, Nature 299, 1982) assures that Eve cannot replicate a particle of unknown state.
- Eve has to measure the photons sent by Alice before sending them on to Bob.

Basic Eavesdropping: Measure and Resend

- No cloning theorem (Wooters & Zurek, Nature 299, 1982) assures that Eve cannot replicate a particle of unknown state.
- Eve has to measure the photons sent by Alice before sending them on to Bob.
- Since Eve will not know what bases Alice used to encoded the bit until after Alice and Bob discuss their measurements, Eve will be forced to guess the basis randomly.

Basic Eavesdropping: Measure and Resend (contd ...)

Basic Eavesdropping: Measure and Resend (contd ...)

- If she measures on the incorrect bases, Bob will read a bit incorrectly 50% of the time.

Basic Eavesdropping: Measure and Resend (contd ...)

- If she measures on the incorrect bases, Bob will read a bit incorrectly 50% of the time.
- Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice.

Basic Eavesdropping: Measure and Resend (contd ...)

- If she measures on the incorrect bases, Bob will read a bit incorrectly 50% of the time.
- Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice.
- If Eve has eavesdropped on all the bits, then after n bit comparisons by Alice and Bob, they will reduce the probability that Eve will go undetected to 0.75^n.

BB84 in Practice

BB84 in Practice

- Alice sends $4n + \delta$ photons to Bob.

BB84 in Practice

- Alice sends $4n + \delta$ photons to Bob.
- After discarding the photons with disagreeing bases, roughly $2n$ bits are left.

BB84 in Practice

- Alice sends $4n + \delta$ photons to Bob.
- After discarding the photons with disagreeing bases, roughly $2n$ bits are left.
- Alice selects a subset of n qubits to serve as check bits against the noise and interference of any possible eavesdropper Eve.

BB84 in Practice

- Alice sends $4n + \delta$ photons to Bob.
- After discarding the photons with disagreeing bases, roughly $2n$ bits are left.
- Alice selects a subset of n qubits to serve as check bits against the noise and interference of any possible eavesdropper Eve.
- If the number of disagreement is more than an acceptable limit then the protocol is aborted.

BB84 in Practice

- Alice sends $4n + \delta$ photons to Bob.
- After discarding the photons with disagreeing bases, roughly $2n$ bits are left.
- Alice selects a subset of n qubits to serve as check bits against the noise and interference of any possible eavesdropper Eve.
- If the number of disagreement is more than an acceptable limit then the protocol is aborted.
- Information reconciliation and privacy amplification are performed by Alice and Bob on the remaining n bits to obtain m shared key bits.

Two Sources of Security in BB84

Two Sources of Security in BB84

- The quantum channel, where any measurement introduces error (qubits cannot be copied).

Two Sources of Security in BB84

- The quantum channel, where any measurement introduces error (qubits cannot be copied).
  Note: because of no-cloning, quantum channel is a perfectly secure communication channel from classical point of view.

Two Sources of Security in BB84

- The quantum channel, where any measurement introduces error (qubits cannot be copied).
  Note: because of no-cloning, quantum channel is a perfectly secure communication channel from classical point of view.
- Orthogonal basis to represent 0 and 1 (non-orthogonal states cannot be distinguished).

Roadmap

Basic Idea

Basic Idea

- Measurement Device Independent (MDI) Quantum Key Distribution (QKD) idea has been presented very recently by Lo, Curty and Qi (PRL, 2012).

Basic Idea

- Measurement Device Independent (MDI) Quantum Key Distribution (QKD) idea has been presented very recently by Lo, Curty and Qi (PRL, 2012).
- The idea is to resist detector side channel attacks.

Basic Idea

- Measurement Device Independent (MDI) Quantum Key Distribution (QKD) idea has been presented very recently by Lo, Curty and Qi (PRL, 2012).
- The idea is to resist detector side channel attacks.
- All the measurements are executed at Eve's end, an untrusted third-party.

Basic Idea

- Measurement Device Independent (MDI) Quantum Key Distribution (QKD) idea has been presented very recently by Lo, Curty and Qi (PRL, 2012).
- The idea is to resist detector side channel attacks.
- All the measurements are executed at Eve's end, an untrusted third-party.
- It is natural to consider that Eve herself will try to gather information about the secret key while assisting Alice and Bob.

Bell States

- The MDI QKD algorithm uses *Bell states*.
- These are two-qubit entangled states.
- Denoted by $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$, $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$.
- They form an orthogonal basis in a four-dimensional Hilbert space.

Description of MDI QKD

Description of MDI QKD

- Alice and Bob send random bit strings to Eve after encoding them in either Z or X basis randomly.

Description of MDI QKD

- Alice and Bob send random bit strings to Eve after encoding them in either Z or X basis randomly.
- Eve measures each pair (one from Alice and one from Bob) in the Bell basis and publicly announces the results.

Description of MDI QKD

- Alice and Bob send random bit strings to Eve after encoding them in either Z or X basis randomly.
- Eve measures each pair (one from Alice and one from Bob) in the Bell basis and publicly announces the results.
- Alice and Bob announces the bases and discards the mismatched ones.

Description of MDI QKD

- Alice and Bob send random bit strings to Eve after encoding them in either Z or X basis randomly.
- Eve measures each pair (one from Alice and one from Bob) in the Bell basis and publicly announces the results.
- Alice and Bob announces the bases and discards the mismatched ones.
- For the matched bases, one of Alice and Bob flips the bit, if
  - both are in Z basis and Eve's outcome are $|\Psi^{\pm}\rangle$, OR
  - both are in X basis and Eve's outcome are $|\Phi^{-}\rangle$ or $|\Psi^{-}\rangle$.

Description of MDI QKD

- Alice and Bob send random bit strings to Eve after encoding them in either Z or X basis randomly.
- Eve measures each pair (one from Alice and one from Bob) in the Bell basis and publicly announces the results.
- Alice and Bob announces the bases and discards the mismatched ones.
- For the matched bases, one of Alice and Bob flips the bit, if
  - both are in Z basis and Eve's outcome are $|\Psi^{\pm}\rangle$, OR
  - both are in X basis and Eve's outcome are $|\Phi^{-}\rangle$ or $|\Psi^{-}\rangle$.
- Error estimation, information reconciliation and privacy amplification are performed by Alice and Bob on the bits at their ends to obtain the final shared key bits.

Different Cases

Qubits sent by		Probability (Eve's end)				Flip
Alice	Bob	$\vert\Phi^+\rangle$	$\vert\Phi^-\rangle$	$\vert\Psi^+\rangle$	$\vert\Psi^-\rangle$	
$\vert 0\rangle$	$\vert 0\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	No
$\vert 0\rangle$	$\vert 1\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	Yes
$\vert 1\rangle$	$\vert 0\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	Yes
$\vert 1\rangle$	$\vert 1\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	No
$\vert +\rangle$	$\vert +\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	No
$\vert +\rangle$	$\vert -\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	Yes
$\vert -\rangle$	$\vert +\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	Yes
$\vert -\rangle$	$\vert -\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	No

Roadmap

Eavesdropping: Different Models

- Will Eve work on each individual qubit or a set of qubits together?
  - the first one is called the *incoherent attack*,
  - the second one is known as *coherent attack*.
- Will there be equal error probability at Bob's end corresponding to different bases?
  - If this is indeed equal, then we call it *symmetric*.
  - Otherwise, we call it *asymmetric*.

How does Eve interact?

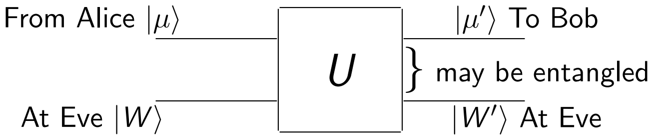

Figure: The model of Eavesdropping

The unitary interactions at Eve's end

$$
\begin{aligned}
U|0\rangle|W\rangle &= \sqrt{1-D}|0\rangle|E_{00}\rangle + \sqrt{D}|1\rangle|E_{01}\rangle, \\
U|1\rangle|W\rangle &= \sqrt{1-D}|1\rangle|E_{11}\rangle + \sqrt{D}|0\rangle|E_{10}\rangle,
\end{aligned}
$$

where D is the disturbance and $1-D$ is the fidelity and E_{pq} is the state of Eve's ancilla qubits after the interaction.

Expressions for Eve's post-interaction states

$$
\begin{aligned}
|E_{00}\rangle &= \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\
|E_{01}\rangle &= \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} - \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}}, \\
|E_{10}\rangle &= \sqrt{1-D}\frac{|01\rangle + |10\rangle}{\sqrt{2}} + \sqrt{D}\frac{|01\rangle - |10\rangle}{\sqrt{2}}, \\
|E_{11}\rangle &= \sqrt{1-D}\frac{|00\rangle + |11\rangle}{\sqrt{2}} - \sqrt{D}\frac{|00\rangle - |11\rangle}{\sqrt{2}}.
\end{aligned}
$$

It can be shown that Eve can correctly guess the qubit sent by Alice and received by Bob with probability $\frac{1}{2} + \sqrt{D(1-D)}$.

The unitary interactions at Eve's end

$$
\begin{aligned}
U|0\rangle_A|W\rangle_A &= \sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A, \\
U|1\rangle_A|W\rangle_A &= \sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A,
\end{aligned}
$$

where D is the disturbance and $1-D$ is the fidelity and E_{pq} is the state of Eve's ancilla qubits after the interaction.

The overall state at Eve's end

An example case: both Alice and Bob send 0.

$$
\begin{aligned}
& (\sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A)|0\rangle_B \\
= \quad & \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\phi^+\rangle_{AB} + \sqrt{\frac{1-D}{2}}|E_{00}\rangle_A|\phi^-\rangle_{AB} \\
& + \sqrt{\frac{D}{2}}|E_{01}\rangle_A|\psi^+\rangle_{AB} - \sqrt{\frac{D}{2}}|E_{01}\rangle_A|\psi^-\rangle_{AB}.
\end{aligned}
$$

The unitary interactions at Eve's end

$$\begin{aligned}
U|0\rangle_A|W\rangle_A &= \sqrt{1-D}|0\rangle_A|E_{00}\rangle_A + \sqrt{D}|1\rangle_A|E_{01}\rangle_A, \\
U|1\rangle_A|W\rangle_A &= \sqrt{1-D}|1\rangle_A|E_{11}\rangle_A + \sqrt{D}|0\rangle_A|E_{10}\rangle_A, \\
U|0\rangle_B|W\rangle_B &= \sqrt{1-D}|0\rangle_B|E_{00}\rangle_B + \sqrt{D}|1\rangle_B|E_{01}\rangle_B, \\
U|1\rangle_B|W\rangle_B &= \sqrt{1-D}|1\rangle_B|E_{11}\rangle_B + \sqrt{D}|0\rangle_B|E_{10}\rangle_B.
\end{aligned}$$

The overall state at Eve's end

An example case: when Alice sends 0 and Bob sends 1.

$$\left(\frac{1-D}{\sqrt{2}}|F_{0011}\rangle + \frac{D}{\sqrt{2}}|F_{0110}\rangle\right)\Psi^+_{AB} + \left(\frac{1-D}{\sqrt{2}}|F_{0011}\rangle - \frac{D}{\sqrt{2}}|F_{0110}\rangle\right)$$
$$+\left(\sqrt{\frac{D(1-D)}{2}}|F_{0111}\rangle + \sqrt{\frac{D(1-D)}{2}}|F_{0010}\rangle\right)\Phi^+_{AB}$$
$$+\left(\sqrt{\frac{D(1-D)}{2}}|F_{0010}\rangle - \sqrt{\frac{D(1-D)}{2}}|F_{0111}\rangle\right)\Phi^-_{AB}.$$

Here, $|F_{pqrs}\rangle = |E_{pq}\rangle_A|E_{rs}\rangle_B$.

The effective disturbance at Alice and Bob's end

Proposition

When Eve eavesdrops on both the sides, the effective disturbance at Alice and Bob's end is given by $\Delta(D) = 2D(1 - D)$.

Roadmap

Eve's Likelihoods $P(V = v \mid A = a, B = b)$

V	$A = 0$, $B = 0$	$A = 0$, $B = 1$	$A = 1$, $B = 0$	$A = 1$, $B = 1$
00	$(1-D)d$	$(1-D)d$	$(1-D)d'$	$(1-D)d'$
01	Dd'	Dd'	Dd	Dd
10	Dd	Dd	Dd'	Dd'
11	$(1-D)d'$	$(1-D)d'$	$(1-D)d$	$(1-D)d$

Here $d = \frac{1}{2} + \sqrt{D(1-D)}$ and $d' = \frac{1}{2} - \sqrt{D(1-D)}$.

Success Probability Expressions

Theorem

The optimal success probability of Eve in guessing the bit sent by Alice is given by $\frac{1}{2} + \sqrt{D(1-D)}$.

Corollary

Success probability for guessing both Alice's and Bob's bit is $P_1(D) = \frac{1}{2}d = \frac{1}{4} + \frac{1}{2}\sqrt{D(1-D)}$.

Eve's Likelihoods $P(V = v \mid A = a, B = b)$

V	$A=0, B=0$	$A=0, B=1$	$A=1, B=0$	$A=1, B=1$
0000	$\frac{1}{4}(1-D)^2 d_+$	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_-$
0001	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_+$	$\frac{1}{4}D(1-D)d_-$	$\frac{1}{4}D(1-D)d_2$
0010	$\frac{1}{4}D(1-D)d_+$	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_-$
0011	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_+$	$\frac{1}{4}(1-D)^2 d_-$	$\frac{1}{4}(1-D)^2 d_2$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
1100	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_-$	$\frac{1}{4}(1-D)^2 d_+$	$\frac{1}{4}(1-D)^2 d_2$
1101	$\frac{1}{4}D(1-D)d_-$	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_+$
1110	$\frac{1}{4}D(1-D)d_2$	$\frac{1}{4}D(1-D)d_-$	$\frac{1}{4}D(1-D)d_+$	$\frac{1}{4}D(1-D)d_2$
1111	$\frac{1}{4}(1-D)^2 d_-$	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_2$	$\frac{1}{4}(1-D)^2 d_+$

Here $d_\pm = (\sqrt{1-D} \pm \sqrt{D})^4$ and $d_2 = (1-2D)^2$.

Success Probability Expressions

Theorem

The optimal success probability of Eve in guessing a pair of bits sent by Alice and Bob is given by
$P_2(D) = \frac{1}{4} + D(1-D) + \sqrt{D(1-D)}$.

Corollary

Introducing a disturbance Δ, the optimal success probability of Eve in guessing a pair of bits sent by Alice and Bob is given by
$\frac{1}{4} + \frac{\Delta}{2} + \sqrt{\frac{\Delta}{2}}$.

Eve's optimal guesses corresponding to her measurement outcomes

V	0000	0001	0010	0011	0100	0101	0110	0111
G_A, G_B	0, 0	0, 1	0, 0	0, 1	1, 0	1, 1	1, 0	1, 1
V	1000	1001	1010	1011	1100	1101	1110	1111
G_A, G_B	0, 0	0, 1	0, 0	0, 1	1, 0	1, 1	1, 0	1, 1

Roadmap

Error Location in BB84

- If Alice sends $|0\rangle$, then Eve will obtain either $|E_{00}\rangle$ or $|E_{01}\rangle$.
- Eve now measures in $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis.
- If Eve observes $|00\rangle$ or $|11\rangle$, then she knows that Bob obtained $|0\rangle$, i.e., no error has been introduced.
- If Eve observes $|01\rangle$ or $|10\rangle$, then she knows that Bob obtained $|1\rangle$, i.e., error has been introduced.
- Thus, in BB84 protocol, Eve can decide with certainty whether her interaction has introduced an error or not.

Error Location: One-sided Eavesdropping

- In this case Alice and Bob produce the bits independently.
- So, looking at Alice's bit, it is not possible to know what happens in case of Bob's bit.
- Thus, Alice has no advantage.

Error Location: Two-sided Eavesdropping

A	B	G_A	G_B	$P(A, B, G_A, G_B)$	Error Guessed by Eve correctly
0	0	0	0	$\frac{1}{16}d_+$	Y
		0	1	$\frac{1}{16}d_2$	N
		1	0	$\frac{1}{16}d_2$	N
		1	1	$\frac{1}{16}d_-$	Y
0	1	0	0	$\frac{1}{16}d_2$	N
		0	1	$\frac{1}{16}d_+$	Y
		1	0	$\frac{1}{16}d_-$	Y
		1	1	$\frac{1}{16}d_2$	N

Similarly, AB $=$ 10 and 11 can also be analyzed.

Probability of Eve's Guessing the Error Location

Theorem

Eve can guess whether an error has been introduced between Alice and Bob or not with probability $\frac{1}{2} + 2D(1 - D)$.

Roadmap

Summary

Summary

- We have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD.

Summary

- We have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD.
- It can be shown that for the one-sided case, Eve needs to measure only the second qubit and for the two-sided case she needs to measure only the second and the fourth qubits.

Summary

- We have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD.
- It can be shown that for the one-sided case, Eve needs to measure only the second qubit and for the two-sided case she needs to measure only the second and the fourth qubits.
- Performing the attack on only one side is equivalent to performing the attack on both sides and then observing the result for only one side.

Summary

- We have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD.
- It can be shown that for the one-sided case, Eve needs to measure only the second qubit and for the two-sided case she needs to measure only the second and the fourth qubits.
- Performing the attack on only one side is equivalent to performing the attack on both sides and then observing the result for only one side.
- The attack on BB84 is sharper than that on MDI QKD. But the latter case is more challenging for Eve.

Summary

- We have studied eavesdropping strategy on a recently proposed variant of BB84, which is refereed to as MDI QKD.
- It can be shown that for the one-sided case, Eve needs to measure only the second qubit and for the two-sided case she needs to measure only the second and the fourth qubits.
- Performing the attack on only one side is equivalent to performing the attack on both sides and then observing the result for only one side.
- The attack on BB84 is sharper than that on MDI QKD. But the latter case is more challenging for Eve.
- In terms of location of errors, MDI-QKD leaks less information than BB84.

Future Work

- To analyze different "device independent" protocols under similar attack models.
- To investigate countermeasures against this type of attacks.