Master-Key Controlled Quantum Key Distribution

Tabish Qureshi

Centre for Theoretical Physics
Jamia Millia Islamia
New Delhi - 110025.

Collaborators: T. Shibli, Aditi Sheel

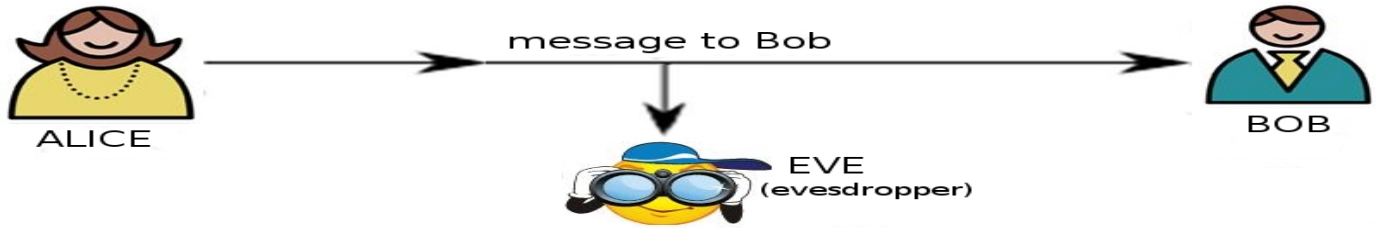
Outline

1. Cryptography
2. Quantum Key Distribution
3. Three-particle entanglement
4. Two new protocols
   - MKC-QKD
   - MKS-QKD

Outline

1. Cryptography
2. Quantum Key Distribution
3. Three-particle entanglement
4. Two new protocols
   - MKC-QKD
   - MKS-QKD

Cryptography: an old art



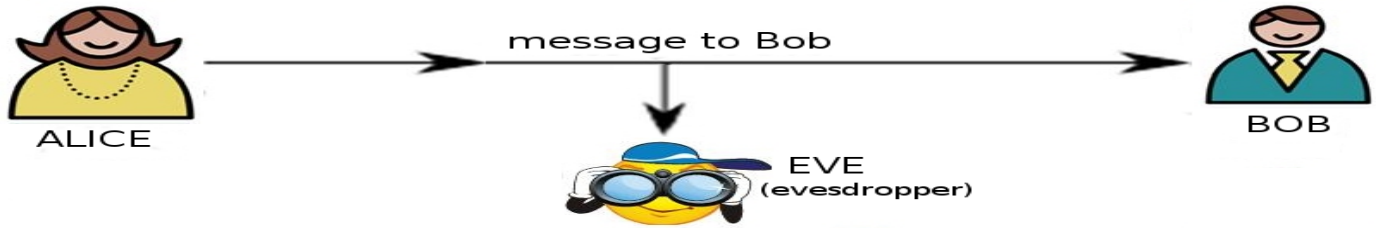
Alice and Bob exchange confidential information. Eve is trying to eavesdrop and steal that information

One solution is to encrypt the messages

- Alice and Bob encrypt their messages. Can Eve decrypt their messages?
- Various cryptographic methods: Some more difficult to decrypt.
- RSA encryption: Used in e-commerce and secure web communication. Based on the fact that it is very difficult to factorize large numbers.

RSA will crumble as soon as quantum computers become a reality!

Cryptography: an old art



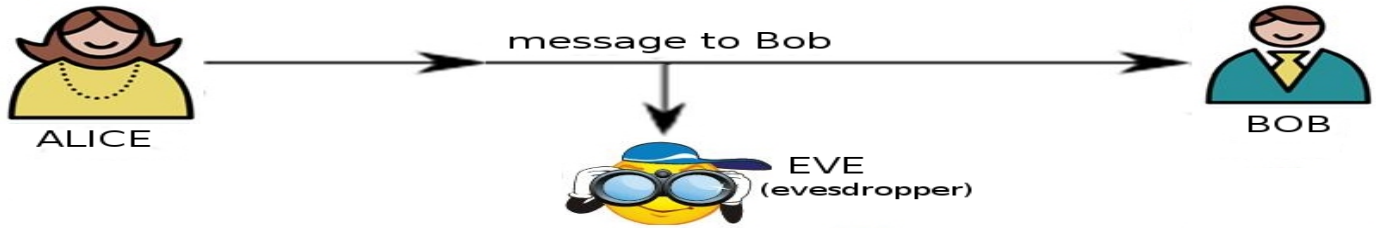
Alice and Bob exchange confidential information. Eve is trying to eavesdrop and steal that information

One solution is to encrypt the messages

- Alice and Bob encrypt their messages. Can Eve decrypt their messages?
- Various cryptographic methods: Some more difficult to decrypt.
- RSA encryption: Used in e-commerce and secure web communication. Based on the fact that it is very difficult to factorize large numbers.

RSA will crumble as soon as quantum computers become a reality!

Cryptography: an old art



Alice and Bob exchange confidential information. Eve is trying to eavesdrop and steal that information

One solution is to encrypt the messages

- Alice and Bob encrypt their messages. Can Eve decrypt their messages?
- Various cryptographic methods: Some more difficult to decrypt.
- RSA encryption: Used in e-commerce and secure web communication. Based on the fact that it is very difficult to factorize large numbers.

RSA will crumble as soon as quantum computers become a reality!

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20

The problem boils down to:

How to a share a new secret key between two remote parties?

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20

The problem boils down to:

How to a share a new secret key between two remote parties?

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20
Decoded Message:	23	08	05	18	05	00	09	19	00	15	19	01	13	01	27

The problem boils down to:

How to a share a new secret key between two remote parties?

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20
Decoded Message:	23	08	05	18	05	00	09	19	00	15	19	01	13	01	27
Message:	W	H	E	R	E		I	S		O	S	A	M	A	?

The problem boils down to:

How to a share a new secret key between two remote parties?

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20
Decoded Message:	23	08	05	18	05	00	09	19	00	15	19	01	13	01	27
Message:	W	H	E	R	E		I	S		O	S	A	M	A	?

Vernam Cipher is unbreakable IF one key is used only once!

The problem boils down to:

How to a share a new secret key between two remote parties?

Vernam Cipher (One-time pad)

The only known unbreakable encryption system

Number the letters

	A	B	C	D	E	···	···	X	Y	Z	?	,	.
00	01	02	03	04	05	···	···	24	25	26	27	28	29

To encrypt: Add the key to the message, letter by letter, modulo 30.

To decrypt: Subtract the key from the encrypted message.

EXAMPLE

Coded Message:	12	12	26	27	19	11	04	23	17	12	20	09	09	04	17
Key:	19	04	21	09	14	11	25	04	17	27	01	08	26	03	20
Decoded Message:	23	08	05	18	05	00	09	19	00	15	19	01	13	01	27
Message:	W	H	E	R	E		I	S		O	S	A	M	A	?

Vernam Cipher is unbreakable IF one key is used only once!

The problem boils down to:

How to a share a new secret key between two remote parties?

Outline

1. Cryptography
2. Quantum Key Distribution
3. Three-particle entanglement
4. Two new protocols
   - MKC-QKD
   - MKS-QKD

Quantum Key Distribution

BB84 (Bennett & Brassard, 1984), E91 (Ekert 1991)

1. Entangled spin-1/2 particle source produces a sequence of particles pairs, in the state $(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)/\sqrt{2}$
2. Alice, Bob measure the spin states by randomly choosing the x-component of the spin or the z-component.
3. At the end, Alice and Bob publicly declare the basis they used in each measurement.
4. Results for which their bases do not match, are discarded.
5. Alice: $|+\rangle = 1 \quad |-\rangle = 0 \quad |\uparrow\rangle = 1 \quad |\downarrow\rangle = 0$
   Bob: $|+\rangle = 0 \quad |-\rangle = 1 \quad |\uparrow\rangle = 0 \quad |\downarrow\rangle = 1$

Quantum Key Distribution

BB84 (Bennett & Brassard, 1984), E91 (Ekert 1991)

1. Entangled spin-1/2 particle source produces a sequence of particles pairs, in the state $(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)/\sqrt{2}$
2. Alice, Bob measure the spin states by randomly choosing the x-component of the spin or the z-component.
3. At the end, Alice and Bob publicly declare the basis they used in each measurement.
4. Results for which their bases do not match, are discarded.
5. Alice: $|+\rangle = 1 \quad |-\rangle = 0 \quad |\uparrow\rangle = 1 \quad |\downarrow\rangle = 0$
   Bob: $|+\rangle = 0 \quad |-\rangle = 1 \quad |\uparrow\rangle = 0 \quad |\downarrow\rangle = 1$

Quantum Key Distribution

BB84 (Bennett & Brassard, 1984), E91 (Ekert 1991)

1. Entangled spin-1/2 particle source produces a sequence of particles pairs, in the state $(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)/\sqrt{2}$
2. Alice, Bob measure the spin states by randomly choosing the x-component of the spin or the z-component.
3. At the end, Alice and Bob publicly declare the basis they used in each measurement.
4. Results for which their bases do not match, are discarded.
5. Alice: $|+\rangle = 1$ $|-\rangle = 0$ $|\uparrow\rangle = 1$ $|\downarrow\rangle = 0$
   Bob: $|+\rangle = 0$ $|-\rangle = 1$ $|\uparrow\rangle = 0$ $|\downarrow\rangle = 1$

Quantum Key Distribution

BB84 (Bennett & Brassard, 1984), E91 (Ekert 1991)

1. Entangled spin-1/2 particle source produces a sequence of particles pairs, in the state $(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)/\sqrt{2}$
2. Alice, Bob measure the spin states by randomly choosing the x-component of the spin or the z-component.
3. At the end, Alice and Bob publicly declare the basis they used in each measurement.
4. Results for which their bases do not match, are discarded.
5.

Alice:	$\|+\rangle = 1$	$\|-\rangle = 0$	$\|\uparrow\rangle = 1$	$\|\downarrow\rangle = 0$
Bob:	$\|+\rangle = 0$	$\|-\rangle = 1$	$\|\uparrow\rangle = 0$	$\|\downarrow\rangle = 1$

Quantum Key Distribution continued . . .

6. Alice announces the results of a small subset of her measurements. Bob checks if he has identical results. Any discrepency here indicates a possible evesdropping attempt.
7. If there is no discrepancy, the rest of the binary sequence is treated as the new key, and is identical for both Alice and Bob.

This QKD protocol is proven to be 100 secure (for ideal detectors and noisefree environment).

There are currently three companies offering commercial QKD systems; *id Quantique* (Geneva), *MagiQ Technologies* (New York) and *QuintessenceLabs* (Australia).

Various attacks have been successfully demonstrated against commercial QKD systems:

C.-H. F. Fung et al., Phys. Rev. A 75, 032314 (2007); F. Xu, B. Qi and H.-K. Lo, New J. Phys. 12, 113026 (2010).

B. Qi et al., Quantum Inf. Comput. 7, 73 (2007); Y. Zhao et al., Phys. Rev. A 78, 042333 (2008); L. Lydersen et al., Nature Photon. 4, 686 (2010); I. Gerhardt et al., Nature Commun. 2, 349 (2011).

Quantum Key Distribution continued . . .

6. Alice announces the results of a small subset of her measurements. Bob checks if he has identical results. Any discrepency here indicates a possible evesdropping attempt.
7. If there is no discrepancy, the rest of the binary sequence is treated as the new key, and is identical for both Alice and Bob.

This QKD protocol is proven to be 100 secure
(for ideal detectors and noisefree environment).

There are currently three companies offering commercial QKD systems; *id Quantique* (Geneva), *MagiQ Technologies* (New York) and *QuintessenceLabs* (Australia).

Various attacks have been successfully demonstrated against commercial QKD systems:


C.-H. F. Fung et al., Phys. Rev. A 75, 032314 (2007); F. Xu, B. Qi and H.-K. Lo, New J. Phys. 12, 113026 (2010).


B. Qi et al., Quantum Inf. Comput. 7, 73 (2007); Y. Zhao et al., Phys. Rev. A 78, 042333 (2008); L. Lydersen et al., Nature Photon. 4, 686 (2010); I. Gerhardt et al., Nature Commun. 2, 349 (2011).

Quantum Key Distribution continued . . .

6. Alice announces the results of a small subset of her measurements. Bob checks if he has identical results. Any discrepency here indicates a possible evesdropping attempt.
7. If there is no discrepancy, the rest of the binary sequence is treated as the new key, and is identical for both Alice and Bob.

This QKD protocol is proven to be 100 secure (for ideal detectors and noisefree environment).

There are currently three companies offering commercial QKD systems; *id Quantique* (Geneva), *MagiQ Technologies* (New York) and *QuintessenceLabs* (Australia).

Various attacks have been successfully demonstrated against commercial QKD systems:

C.-H. F. Fung et al., Phys. Rev. A 75, 032314 (2007); F. Xu, B. Qi and H.-K. Lo, New J. Phys. 12, 113026 (2010).

B. Qi et al., Quantum Inf. Comput. 7, 73 (2007); Y. Zhao et al., Phys. Rev. A 78, 042333 (2008); L. Lydersen et al., Nature Photon. 4, 686 (2010); I. Gerhardt et al., Nature Commun. 2, 349 (2011).

Outline

1. Cryptography
2. Quantum Key Distribution
3. Three-particle entanglement
4. Two new protocols
   - MKC-QKD
   - MKS-QKD

Three-particle entanglement

The GHZ (Greenberger-Zeilenger-Horne) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle_3 + |\downarrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle_3)$$

$|\uparrow\rangle_i, |\downarrow\rangle_i$ are eigenstates of the operator $\boldsymbol{\sigma}_{iz}$.

Any two, of the three, particles are not entangled:
The results of measurement of $\boldsymbol{\sigma}_{1z}$ and $\boldsymbol{\sigma}_{2z}$ will be correlated, but those of $\boldsymbol{\sigma}_{1x}$ and $\boldsymbol{\sigma}_{2x}$ will not be correlated.

$$|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

Making measurements on particle 1 and 2, in coincidence with particle 3 appearing in state $|+\rangle_3$, will make 1 and 2 entangled!
Same will be true if coincidence is done with $|-\rangle_3$.

Disentanglement has been erased!

Quantum Disentanglement Eraser [1]

[1] R. Garisto, L. Hardy, "Entanglement of projection and a new class of quantum erasers," *Phys. Rev.* 60, 827–831 (1999).

Three-particle entanglement

The GHZ (Greenberger-Zeilenger-Horne) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle_3 + |\downarrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle_3)$$

$|\uparrow\rangle_i, |\downarrow\rangle_i$ are eigenstates of the operator $\boldsymbol{\sigma}_{iz}$.

Any two, of the three, particles are not entangled:
The results of measurement of $\boldsymbol{\sigma}_{1z}$ and $\boldsymbol{\sigma}_{2z}$ will be correlated, but those of $\boldsymbol{\sigma}_{1x}$ and $\boldsymbol{\sigma}_{2x}$ will not be correlated.

$$|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

Making measurements on particle 1 and 2, in coincidence with particle 3 appearing in state $|+\rangle_3$, will make 1 and 2 entangled!
Same will be true if coincidence is done with $|-\rangle_3$.

Disentanglement has been erased!

Quantum Disentanglement Eraser [1]

[1] R. Garisto, L. Hardy, "Entanglement of projection and a new class of quantum erasers," *Phys. Rev.* 60, 827–831 (1999).

Three-particle entanglement

The GHZ (Greenberger-Zeilenger-Horne) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle_3 + |\downarrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle_3)$$

$|\uparrow\rangle_i, |\downarrow\rangle_i$ are eigenstates of the operator $\boldsymbol{\sigma}_{iz}$.

Any two, of the three, particles are not entangled:
The results of measurement of $\boldsymbol{\sigma}_{1z}$ and $\boldsymbol{\sigma}_{2z}$ will be correlated, but those of $\boldsymbol{\sigma}_{1x}$ and $\boldsymbol{\sigma}_{2x}$ will not be correlated.

$$|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

Making measurements on particle 1 and 2, in coincidence with particle 3 appearing in state $|+\rangle_3$, will make 1 and 2 entangled!
Same will be true if coincidence is done with $|-\rangle_3$.

Disentanglement has been erased!

Quantum Disentanglement Eraser [1]

[1] R. Garisto, L. Hardy, "Entanglement of projection and a new class of quantum erasers," *Phys. Rev.* 60, 827–831 (1999).

Three-particle entanglement

The GHZ (Greenberger-Zeilenger-Horne) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle_3 + |\downarrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle_3)$$

$|\uparrow\rangle_i, |\downarrow\rangle_i$ are eigenstates of the operator $\boldsymbol{\sigma}_{iz}$.

Any two, of the three, particles are not entangled:
The results of measurement of $\boldsymbol{\sigma}_{1z}$ and $\boldsymbol{\sigma}_{2z}$ will be correlated, but those of $\boldsymbol{\sigma}_{1x}$ and $\boldsymbol{\sigma}_{2x}$ will not be correlated.

$$|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

Making measurements on particle 1 and 2, in coincidence with particle 3 appearing in state $|+\rangle_3$, will make 1 and 2 entangled!
Same will be true if coincidence is done with $|-\rangle_3$.

Disentanglement has been erased!

Quantum Disentanglement Eraser [1]

[1] R. Garisto, L. Hardy, "Entanglement of projection and a new class of quantum erasers," *Phys. Rev.* **60**, 823–831 (1999).

Three-particle entanglement

The GHZ (Greenberger-Zeilenger-Horne) state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\uparrow\rangle_2|\uparrow\rangle_3 + |\downarrow\rangle_1|\downarrow\rangle_2|\downarrow\rangle_3)$$

$|\uparrow\rangle_i, |\downarrow\rangle_i$ are eigenstates of the operator $\boldsymbol{\sigma}_{iz}$.

Any two, of the three, particles are not entangled:
The results of measurement of $\boldsymbol{\sigma}_{1z}$ and $\boldsymbol{\sigma}_{2z}$ will be correlated, but those of $\boldsymbol{\sigma}_{1x}$ and $\boldsymbol{\sigma}_{2x}$ will not be correlated.

$$|\psi\rangle = \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \frac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

Making measurements on particle 1 and 2, in coincidence with particle 3 appearing in state $|+\rangle_3$, will make 1 and 2 entangled!
Same will be true if coincidence is done with $|-\rangle_3$.

Disentanglement has been erased!

Quantum Disentanglement Eraser [1]

[1] R. Garisto, L. Hardy, "Entanglement of projection and a new class of quantum erasers," *Phys. Rev. A* 60, 827-831 (1999).

QKD with three particles

The GHZ state:

$$|\psi\rangle = \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

The GHZ state (in another basis):

$$|\psi\rangle = \tfrac{1}{2}(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)|-\rangle_3.$$

QKD with three particles

The GHZ state:

$$|\psi\rangle = \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

The GHZ state (in another basis):

$$|\psi\rangle = \tfrac{1}{2}(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)|-\rangle_3.$$

- Measurements on 1 & 2 in the z-basis always give identical results.

QKD with three particles

The GHZ state:

$$|\psi\rangle = \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

The GHZ state (in another basis):

$$|\psi\rangle = \tfrac{1}{2}(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)|-\rangle_3.$$

- Measurements on 1 & 2 in the z-basis always give identical results.
- Measurements on 1 & 2 in the x-basis give identical results if 3 is found in $|+\rangle_3$

QKD with three particles

The GHZ state:

$$|\psi\rangle = \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

The GHZ state (in another basis):

$$|\psi\rangle = \tfrac{1}{2}(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)|-\rangle_3.$$

- Measurements on 1 & 2 in the z-basis always give identical results.
- Measurements on 1 & 2 in the x-basis give identical results if 3 is found in $|+\rangle_3$
- Measurements on 1 & 2 in the x-basis give opposite results if 3 is found in $|-\rangle_3$

QKD with three particles

The GHZ state:

$$|\psi\rangle = \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 + |\downarrow\rangle_1|\downarrow\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|\uparrow\rangle_1|\uparrow\rangle_2 - |\downarrow\rangle_1|\downarrow\rangle_2)|-\rangle_3.$$

The GHZ state (in another basis):

$$|\psi\rangle = \tfrac{1}{2}(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)|+\rangle_3 + \tfrac{1}{2}(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)|-\rangle_3.$$

- Measurements on 1 & 2 in the z-basis always give identical results.
- Measurements on 1 & 2 in the x-basis give identical results if 3 is found in $|+\rangle_3$
- Measurements on 1 & 2 in the x-basis give opposite results if 3 is found in $|-\rangle_3$
- All results on 1 & 2 can be made identical with the additional information on which cases yield $|-\rangle_3$.

Particle 3 can be used to control a quantum key distribution.

Outline

1. Cryptography
2. Quantum Key Distribution
3. Three-particle entanglement
4. Two new protocols
   - MKC-QKD
   - MKS-QKD

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Master:
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if Alice, Bob used x-basis
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \to 1, |\downarrow\rangle \to 0, |+\rangle \to 1, |-\rangle \to 0.$
   Master:
   $|+\rangle \to 0, |-\rangle \to 1$, if Alice, Bob used x-basis
   $|+\rangle \to 0, |-\rangle \to 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \to 1, |\downarrow\rangle \to 0, |+\rangle \to 1, |-\rangle \to 0.$
   Master:
   $|+\rangle \to 0, |-\rangle \to 1$, if Alice, Bob used x-basis
   $|+\rangle \to 0, |-\rangle \to 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Master:
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if Alice, Bob used x-basis
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Master:
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if Alice, Bob used x-basis
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Master-Key Controlled Quantum Key Distribution

MKC-QKD

1. A 3-particle source is held by the Master: Particle 1 goes to Alice, particle 2 to Bob and particle 3 remains with the Master.
2. Alice & Bob measure their particles in x- or z-basis, randomly.
3. The Master measures his particle in x-basis.
4. Alice & Bob publicly declare their bases for each measurement.
5. Measurements, for which the two bases don't agree, are discarded by Alice, Bob & Master.
6. Alice & Bob: $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Master:
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if Alice, Bob used x-basis
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if Alice, Bob used z-basis
7. All three now have a key, but Alice and Bob's key doesn't match.
8. The Master announces his key publicly which Bob adds to his key bit by bit, modulo 2.
9. At this stage, the keys generated by Alice and Bob are identical.

Possible uses of MKC-QKD

- The master-key can be like the master-key held by bank lockers, without which a customer cannot open his locker with his own key.
- The master-key can be used to introduce a delay in sharing the actual key, after the protocol has been completed.
  The Master decides when a key is ready to be used.
- MKC-QKD does not provide any additional security over BB84/E91 protocols.

Can one modify the technique to make the key distribution more secure?

Yes, one can construct a Master-Key-Secured Quantum Key Distribution (MKS-QKD)

Possible uses of MKC-QKD

- The master-key can be like the master-key held by bank lockers, without which a customer cannot open his locker with his own key.
- The master-key can be used to introduce a delay in sharing the actual key, after the protocol has been completed.
  The Master decides when a key is ready to be used.
- MKC-QKD does not provide any additional security over BB84/E91 protocols.

Can one modify the technique to make the key distribution more secure?

Yes, one can construct a Master-Key-Secured Quantum Key Distribution (MKS-QKD)

Possible uses of MKC-QKD

- The master-key can be like the master-key held by bank lockers, without which a customer cannot open his locker with his own key.
- The master-key can be used to introduce a delay in sharing the actual key, after the protocol has been completed.
  The Master decides when a key is ready to be used.
- MKC-QKD does not provide any additional security over BB84/E91 protocols.

Can one modify the technique to make the key distribution more secure?

Yes, one can construct a Master-Key-Secured Quantum Key Distribution (MKS-QKD)

Master-Key Secured Quantum Key Distribution

1. The 3-particle source is held by Alice, particles 2, 3 go to Bob and particle 1 remains with the Alice.
2. Alice measures her particle in x- or z-basis, randomly.
3. Bob uses one particle to generate his secure key and one for generating the master-key.
   For each pair, he randomly decides which particle to use for which key.
4. For master-key, Bob measures the particle in x-basis.
   For secure-key, he measures the particle in x- or z-basis, randomly.
5. Alice & Bob publicly declare their bases for each measurement for the secure key.
6. Measurements, for which the two bases don't agree, are discarded.

Master-Key Secured Quantum Key Distribution

1. The 3-particle source is held by Alice, particles 2, 3 go to Bob and particle 1 remains with the Alice.
2. Alice measures her particle in x- or z-basis, randomly.
3. Bob uses one particle to generate his secure key and one for generating the master-key .
   For each pair, he randomly decides which particle to use for which key.
4. For master-key, Bob measures the particle in x-basis.
   For secure-key, he measures the particle in x- or z-basis, randomly.
5. Alice & Bob publicly declare their bases for each measurement for the secure key.
6. Measurements, for which the two bases don't agree, are discarded.

Master-Key Secured Quantum Key Distribution

1. The 3-particle source is held by Alice, particles 2, 3 go to Bob and particle 1 remains with the Alice.
2. Alice measures her particle in x- or z-basis, randomly.
3. Bob uses one particle to generate his secure key and one for generating the master-key .
   For each pair, he randomly decides which particle to use for which key.
4. For master-key, Bob measures the particle in x-basis.
   For secure-key, he measures the particle in x- or z-basis, randomly.
5. Alice & Bob publicly declare their bases for each measurement for the secure key.
6. Measurements, for which the two bases don't agree, are discarded.

MKS-QKD continued . . .

7. Alice & Bob, for secure-key : $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Bob, for master-key :
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if he used x-basis for secure-key
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if he used z-basis for secure-key.
8. At this stage Alice & Bob's secure-keys do not match.
9. Bob adds his master-key to his secure-key bit by bit, modulo 2.
10. At this stage, the keys generated by Alice and Bob are identical.

Any evesdropper will to correctly guess which particle Bob used for which key, for every pair he received from Alice.

Even if he manages this Herculean task, the remaining security is still that of standard BB84 protocol.

MKS-QKD provides an additional layer of complexity over BB84.

MKS-QKD continued . . .

7. Alice & Bob, for secure-key : $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Bob, for master-key :
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if he used x-basis for secure-key
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if he used z-basis for secure-key.
8. At this stage Alice & Bob's secure-keys do not match.
9. Bob adds his master-key to his secure-key bit by bit, modulo 2.
10. At this stage, the keys generated by Alice and Bob are identical.

Any evesdropper will to correctly guess which particle Bob used for which key, for every pair he received from Alice.

Even if he manages this Herculean task, the remaining security is still that of standard BB84 protocol.

MKS-QKD provides an additional layer of complexity over BB84.

MKS-QKD continued . . .

7. Alice & Bob, for secure-key : $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Bob, for master-key :
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if he used x-basis for secure-key
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if he used z-basis for secure-key.
8. At this stage Alice & Bob's secure-keys do not match.
9. Bob adds his master-key to his secure-key bit by bit, modulo 2.
10. At this stage, the keys generated by Alice and Bob are identical.

Any evesdropper will to correctly guess which particle Bob used for which key, for every pair he received from Alice.

Even if he manages this Herculean task, the remaining security is still that of standard BB84 protocol.

MKS-QKD provides an additional layer of complexity over BB84.

MKS-QKD continued . . .

7. Alice & Bob, for secure-key : $|\uparrow\rangle \rightarrow 1$, $|\downarrow\rangle \rightarrow 0$, $|+\rangle \rightarrow 1$, $|-\rangle \rightarrow 0$.
   Bob, for master-key :
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 1$, if he used x-basis for secure-key
   $|+\rangle \rightarrow 0$, $|-\rangle \rightarrow 0$, if he used z-basis for secure-key.
8. At this stage Alice & Bob's secure-keys do not match.
9. Bob adds his master-key to his secure-key bit by bit, modulo 2.
10. At this stage, the keys generated by Alice and Bob are identical.

Any evesdropper will to correctly guess which particle Bob used for which key, for every pair he received from Alice.

Even if he manages this Herculean task, the remaining security is still that of standard BB84 protocol.

MKS-QKD provides an additional layer of complexity over BB84.

Conclusions

- A 3-particle GHZ state has been used to construct two quantum key distribution protocols.
- MKC-QKD presents the possibility of a third person, the Master, to control the quantum key distribution between two parties.
- MKS-QKD is a protocol using three particles which provides an additional layer of complexity over the standard BB84/E91 protocol.
- Both the protocols use the concept of quantum disentanglement eraser.

T. Qureshi, T. Shibli, A. Sheel
Master Key Secured Quantum Key Distribution
Arxiv:1301.5015 [quant-ph]