



The Secret of Quantum Secrecy

A. Pathak

Jaypee Institute of Information Technology, Noida, India

and

R. Srikanth

*Poornaprajna Institute of Scientific Research & Raman Research
Institute, Bengaluru, India*

Let us ask some simple questions:

- What is purely quantum in quantum cryptography?
- Are all quantum resources used in quantum cryptography essential?
- If not, what is essential?
- Can we classify existing quantum cryptographic protocols on the basis of what quantum resource provides the security?
- If yes, is there any particular class which is more primitive than the others\other?

We wish to understand: What characteristic of quantum mechanics provides unconditional security?

General terms and definitions

- **Cryptography**: The art of rendering a message unintelligible to any unauthorized party.
- **Cryptoanalysis**: The art of code breaking
- **Cryptology**=Cryptography+Cryptoanalysis
- **Cryptosystem or Cipher**: An algorithm which combines the message to be encrypted with some additional information known as the **key**—and produce a **cryptogram**.
Note: Ideally: A cryptogram is impossible to unlock the without the key. In practice, the message should remain protected at least as long as the information it contains is valuable.
- **BER**= bit error rate **QBER**=Quantum bit error rate
- **Symmetrical crypto system**: Alice and Bob uses same key for encryption and decryption respectively.
- **Asymmetrical or public key cryptosystem**: Different keys are used for encryption and decryption.

Important note

One way (one step) quantum cryptography is nothing but quantum key generation/distribution

Message: 01010010

+ Key:10011010

Cryptogram:11001000

+ Key:10011010

Decoded Message: 01010010

Historical Note

- ❖ In 1970 Stephan Wiesner wrote a seminal paper entitled Conjugate Coding. The paper contained the root of many future developments of quantum information theory and quantum computing. To be precise, no cloning theorem, was implicitly used in this paper and the basic idea of quantum cryptography was also introduced in this paper. This is an interesting paper but its publication history is more interesting. In 1970, Wiesner submitted this paper in IEEE Transactions on Information Theory. This paper was immediately rejected because it was written in a jargon which was not familiar to computer scientists. The paper was finally published in its original form in 1983 in the newsletter of ACM SIGACT (Association for Computing Machinery, Special Interest Group in Algorithms and Computation Theory).
- ❖ The credit of formal introduction of no-cloning theorem normally goes to Wootters and Zurek but almost simultaneously and independently it was introduced by Dieks in 1982. Actually no-cloning theorem in some form or other were known to many people before 1982 but its relevance was not probably clear to them. In this context it would be apt to quote a relevant comment of Peres, "these things were well known to those who know things well". An excellent history of origin and development of no-cloning theorem may be found in A. Peres's article, "How the no-cloning theorem got its name", Fortschritte der Physik, 51 (2003) 458. The article can also be read freely at <http://arxiv.org/pdf/quant-ph/0205076>.

"we say again deliberately that human ingenuity cannot concoct a cypher which human ingenuity cannot resolve." Edger Alan Poe

Quantum cryptography: The art of getting positive results from the following negative rules of quantum mechanics

1. **Wave function collapse or state vector reduction principle:** One cannot take a measurement without perturbing the system. Since Eve cannot make a copy of the qubit sent by Alice, she has to measure the qubit to know what information Alice has sent. The moment she measures the bit the wave function will collapse to one of the possible states and the system will be perturbed. Later Alice and Bob can compare their states and find whether the state was perturbed due to the measurement of Eve or not.
2. **Uncertainty principle:** One cannot simultaneously and accurately measure the value of two non-commuting observables. For example, one cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and in the diagonal basis.
3. **No-cloning theorem:** One cannot duplicate an unknown quantum state. This implies a restriction on Eve that she cannot make a copy of the qubit sent by Alice and keep it for future use.

How it helps: One cannot take a measurement without perturbing the system.

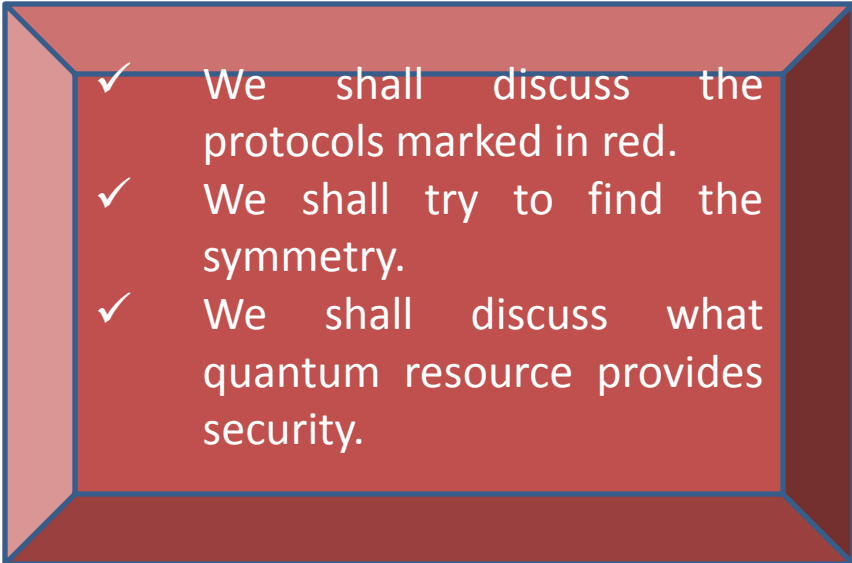
This is applicable to Eve also and we have:

No perturbation \Rightarrow No measurement \Rightarrow

No eavesdropping

A short history of quantum cryptography

1. S. Wiesener was first to introduce the idea in 1970s but his paper appeared in 1983.
2. In 1984 C. H. Bennett and G. Brassard: Introduced **BB84 protocol**. (Four state protocol) **BB84 uses polarisation of photon**
3. In 1991 Artur **Ekert** proposed a cryptographic protocol using EPR pairs (maximally entangled state).
4. In 1992 Bennett introduced two state protocol and shown that two states are sufficient for quantum cryptography. **B-92 uses Mach Zehnder Interferometer**.
5. In 1995 **Goldenberg and Vaidman** introduced a protocol which uses orthogonal states. **Uses Mach Zehnder Interferometer**.
6. In 1998 Bruss and in 1999 Bechmann and Gisin 1999 introduced a six state protocol using the symmetry of the qubit state space.
7. In 2002 Bostrom and Felbinger introduces **Ping-pong protocol** which is two state deterministic protocol and it uses entangled states.
8. In 2003 Hwang introduces **Decoy state protocol** which allows implementation of BB84 in presence of high loss.
9. **In 2005 Lucamarini Manicini's protocol** appeared: a generalization of ping-pong idea but it does not use entangled state.

- 
- ✓ We shall discuss the protocols marked in red.
 - ✓ We shall try to find the symmetry.
 - ✓ We shall discuss what quantum resource provides security.

Different aspects of quantum communication

- ❑ Teleportation (perfect and probabilistic),
- ❑ CT=Controlled teleportation (perfect and probabilistic),
- ❑ QIS=Quantum information splitting,
- ❑ QSS=quantum secret sharing,
- ❑ QKD=quantum key distribution,
- ❑ CV-QKD=Continuous variable QKD,
- ❑ DSQC=deterministic secured quantum communication,
- ❑ QSDC=Quantum secured direct communication,
- ❑ dense-coding, controlled dense-coding and hyper dense-coding.

Problem for students: $CT \subset QIS = QSTS \subset QSS$

Is there anything common in these apparently different protocols?

What provides unconditional security?

- QKD essentially involves splitting of information into 2 or more pieces. Having each piece by itself should be non-revealing of encoded bit.
- It can be non-revealing in two ways, both of which require non-realism. In the GV-class, the diagonal (special) basis is nonlocal (needing the two pieces to be at the same place). This is exploited by preventing Eve's simultaneous access to the two pieces. In the BB84-class, the bits are internet spin/polarization states and thus local. Hence non-orthogonality is needed.

Basic concept: The notion of non-realism

Realism: The assumption that measurement outcomes are well defined prior to and independent of measurements=>Zeilinger et al.

- Given a vector state $r \equiv x\vec{x} + y\vec{y}$ (vector space setting is not necessary)
- If r can be determined in any basis deterministically (not probabilistically), then the theory is realistic. Classical physics is realistic.
- **Example:** If r represents an electric field, then the components x and y , which describe the components of the field, can be determined to arbitrary accuracy (for example by installing tiny dipoles oriented in suitable ways). This remains true for example even if one goes to another basis, say the right/left circular basis.

$$\vec{l} = \frac{1}{\sqrt{2}}(\vec{x} - \vec{y}), \vec{r} = \frac{1}{\sqrt{2}}(\vec{x} + \vec{y})$$

then the components $z^{\pm} = \frac{1}{\sqrt{2}}(x \pm y)$ of $\mathbf{r} \equiv z^{+}\vec{l} + z^{-}\vec{r}$ can also be determined deterministically.

Absence of realism is non-realism. Quantum mechanics is non-realistic.

Is quantum mechanics maximally non-realistic?

- Yes

Consider a quantum state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$. Measurement outcome is probabilistic in computational basis $\{|0\rangle, |1\rangle\}$ but deterministic in diagonal basis $\{|+\rangle, |-\rangle\}$. Thus diagonal basis is special.

For any state $|\psi\rangle$ we can construct a basis set with $|\psi\rangle$ as an element (using Gram-Schmidt procedure). Thus we always have a special basis.

If measurement outcomes were probabilistic in every basis, the theory would presumably be indistinguishable from a purely (realistic) stochastic theory.

On the other hand, **we can presumably construct a continuous family of interpolating theories that are non-maximally non-realistic.**

For example: Think of a measurement rule under which $n > 1$ special basis exist.

**Measurement postulate: Makes quantum mechanics maximally non-realistic.
Provides true random number generator.**

A no-signaling, non-realistic theory that obeys measurement postulate is quantum mechanics we can construct other non-realistic theory that does not obey this.

Some basic concepts

Conjugate Coding:

Theorem: Two non-orthogonal states can not be discriminated with certainty

Logical Proof: If $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal then $|\psi_2\rangle$ can always be decomposed into a nonzero component parallel to $|\psi_1\rangle$ and components orthogonal to $|\psi_1\rangle$. Consequently even if your projective measurement yield $|\psi_1\rangle$, you will not be sure whether it is $|\psi_1\rangle$ or $|\psi_2\rangle$. This is easy to visualize in 2 dimension.

Note: Corresponding measurement operators do not commute. Thus conjugate coding is a consequence of noncommutativity,

Is non-commutativity different from non-realism?

- Yes
- **Let us constructing a theory with non-realism but without the usual commutativity relation:**

Consider a (non-physical) superposition of mutually exclusive possibilities:

$|\psi\rangle = |\sigma_x = +\rangle|\sigma_z = 0\rangle + |\sigma_x = -\rangle|\sigma_z = 1\rangle$ in which the angular momenta X and Z can simultaneously have definite values. Measurement is postulated to yield

$|\sigma_x = +\rangle|\sigma_z = 0\rangle$ or $|\sigma_x = -\rangle|\sigma_z = 1\rangle$ randomly (non-realism), but the specific outcomes have definite X and Z value (no non-commutativity). **This is not a physical example, but a model to show that non-commutativity and non-realism are logically independent.**

- **Non-commutativity without non-realism** given an eigenstate of X, which is $|+\rangle = |0\rangle + |1\rangle$, that is non-eigenstate of Z. We can imagine a non-standard measurement rule in which both outcomes $|0\rangle$ and $|1\rangle$ are obtained when Z is measured. Then we have many-valuedness instead of non-realism.

Which quantum resources are used for secured quantum communication?

1. **No-cloning principle (theorem):** Only linearity is required for proof of nocloning theorem. Therefore, we will see it in classical waves too. Linear theories of classical domain does not provide any nocloning theorem in true sense as perfect measurement will play a role. Simply, one can perfectly measure a state and then copy it. (Non-realism is crucial).
 2. **Entanglement:** It is superposition in tensor product-space. Classical tensor product space exist and that along with linearity (as linearity gives superposition) can yield classical entanglement! Nonlocal nature makes quantum entanglement special. Non-realism creates the fundamental difference between classical and quantum entanglement, appliedd to geographically separated state gives quantum nonlocality. As no-signaling also happens in classical world, Non-realism is crucial.
- **Local variable:** A local variable can be influenced only by events in its backward light cone, not by events outside, and can influence events in its forward light cone only.

Which quantum resources are used for quantum communication?

3. **Noncommutativity:** Yields conjugate coding, it is an important recourse for many QKD and QSDC protocols but is neither sufficient nor essential for QKD. It is not sufficient as random numbers can not be produced without using non-realism and is not essential as we can design QKD, DSQC and QSDC protocols (e.g. Goldenberg-Vaidman protocol and its variant) without using it (just by using non-realism).

Uncertainty relation arises from non-commutivity and are used for CV-QKD.

- **What yields non-realism:** The assumption that quantum measurement yields probabilistic outcomes in accordance to Born rule.
 - A. **Non-realism in particular and quantum measurement postulate in general provides us the essential features of quantum communication.**
 - B. Second most important quantum resource is non-commutivity.

Depending upon which of the above is used to obtain the unconditional security; quantum cryptographic protocols can be classified into two types.

Anybody who is not shocked by quantum theory has not understand it =>Bohr

A simple minded idea of generation of quantum keys: Protocol 1

- Assume that Alice prepares n number of entangled states all prepared in $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle \pm |1_A 1_B\rangle)$, keeps the first photons (qubits) with herself and sends the second photons to Bob.
- Now Alice measures (in computational basis) all the qubits available with her.
- The measurement will destroy the entanglement and create a symmetric random key.
- If you need an anticorrelated key then you may start from $|\phi^\pm\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}(|0_A 1_B\rangle \pm |1_A 0_B\rangle)^{\otimes n}$
- In simple words you can think that Alice prepares the entangled states; keeps one photon of each state with herself (home photon) and sends the other (travel photon) to Bob and after Bob confirms that he has received the states, Alice or Bob measures their states and creates a key.
- **Is there anything wrong with this simple minded approach?**

What is wrong with the simple-minded approach?

Can we modify it?

Let us try to attack this protocol:

Assume that Eve measures the Travel qubit. Notes the result and allows the collapsed state to go to Bob. Now all measurements of Bob will be perfectly correlated to Eve's result. Thus Eve has the key.

Can we detect Eve?

Yes, but Alice and Bob has to change their strategy.

Strategy 1: Alice and Bob chooses more than one non-orthogonal bases and does the measurement with respect to them at random. Then they use part of the generated string as verification string. And compares the outcome of that string to calculate the value of correlation function. For particular choice of entangled state and bases Quantum mechanics will provide a particular value of correlation function. If it matches then there is no Eve. If it does not then Eavesdropping is happening.

If the states are not found in expected correlated (anti-correlated) condition then we know that their exist Eve.

Note: Correlation between the state of Alice and Bob may detect Eve

Let us add some complexity to the simple minded protocol and converts strategy 1 into Protocol 2

1. Alice prepares n number of Bell states all prepared in
$$\frac{1}{\sqrt{2}} [|0_A 0_B\rangle + |1_A 1_B\rangle] = \frac{1}{\sqrt{2}} [|+_A +_B\rangle + |-_A -_B\rangle] .$$
 She keeps the first qubit of all the entangled pairs with her and sends the second qubits to Bob.
2. Now Bob randomly measures all the incoming qubits in $\{0, 1\}$ or $\{+, -\}$ basis and announces which basis he has used to measure a particular state. Measurements of Bob will destroy the entanglement and Bob will obtain a random string of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$
3. Alice measures all her qubits using the same basis (as is used and announced by Bob). Thus Alice also obtain a random string of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$.

The strings of Alice and Bob are expected to be symmetric in an ideal case. Conventionally, one attributes the binary value 0 to states $|0\rangle$ and $|+\rangle$ and binary value 1 to the other two states. Thus in an ideal scenario (in absence of Eve and noise) a symmetric and random key is generated.

Protocol 2

4. Bob uses part of the generated string as verification string and publicly announces the result of measurement of those qubits along with their positions. Alice compares these results with her own result. In an ideal scenario, the outcome of Alice and Bob would be same and they would be able to generate a secured key. In presence of Eve the measurement outcome of verification string will not be same for Alice and Bob and that would indicate the presence of Eve or noise. Thus Eve may be detected. If presence of Eve is detected in a channel then we will not use that channel for generation of quantum key. In absence of Eve we have a perfectly symmetric and unconditionally secured quantum key.

Note:

1. Conjugate Coding provides the security. Entanglement is used but not essential
2. Entanglement is used but it is destroyed via measurement. So why don't we allow Alice to do the measurement and create a random string of

$|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$

Protocol 3:

1. Alice prepares n number of Bell states in

$$\frac{1}{\sqrt{2}} [|00\rangle + |11\rangle] = \frac{1}{\sqrt{2}} [|++\rangle + |--\rangle].$$

She randomly measures all the first qubits in $\{0, 1\}$ or $\{+, -\}$ basis and sends all the second qubits to Bob. As the measurement has already destroyed the entanglement. Alice is essentially sending Bob a random string of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. A copy of the same string will remain with Alice.

2. Bob measures all the incoming qubits randomly in $\{0, 1\}$ or $\{+, -\}$ basis and announces which basis he has used to measure a particular state. Bob uses a random number generator to randomly chose the basis. His random number generator is independent from that of Alice.
3. 50% of the time Bob's basis will be same as that of Alice. Alice informs Bob in which cases Bob's basis are same as that of Alice. They keep those qubits which are measured using same basis and discard the rest.
4. The strings of Alice and Bob are expected to be symmetric in an ideal case.
5. Bob uses part of his string as verification string and publicly announces the result of measurement of those qubits along with their positions. Alice compares these results with her own result. If presence of Eve or noise causes an error greater than a previously decided threshold (tolerable limit) then we will not use that channel for generation of quantum key.

Conjugate coding gives security, entanglement is not essential.

Protocol 4: BB-84 protocol

1. Alice prepares and sends Bob a random string of $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$.
The qubits may have been prepared by using spin states or polarization states or by any other means.
2. Bob measures all the incoming qubits randomly in $\{0, 1\}$ or $\{+, -\}$ basis and announces which basis he has used to measure a particular state.
(Bob uses a random-number generator to randomly chose the basis. His random number generator is independent from that of Alice.)
3. 50% of the time Bob's basis will be same as that of Alice. Alice informs Bob in which cases Bob's basis are same as that of Alice. They keep those qubits which are measured using same basis and discard the rest.
4. The strings of Alice and Bob are expected to be symmetric in an ideal case.
5. Bob uses part of his string as verification string and publicly announces the result of measurement of those qubits along with their positions. Alice compares these results with her own result. In presence of Eve the measurement outcome of verification string will not be same for Alice and Bob and that would indicate the presence of Eve or noise.

Conjugate coding provides security entanglement is not used at all.
Can we distinguish between noise and Eve?

A clever trick to distinguish between noise and Eve: Elementary idea of Decoy state

BB-84 protocol works in ideal situation. It requires single photon source but no such source exist. Consequently Photon number splitting (PNS) attack is possible.

PNS

Eve's strategy: First, Eve measures the number of photons of each pulse. When it is one, she just blocks it. When it is more than one she splits the photons.

Note: Eve is restricted by natural laws only but Alice and Bob are restricted by Existing Technology.

DECOY STATE IDEA

In presence of high loss: A legitimate user intentionally and randomly replaces signal pulses by multiphoton pulses (decoy-pulses). AS Eve can not detect which one is signal pulse and which one is Decoy pulse, he applies PNS attack to both. Eavesdropping will cause a considerable loss in signal pulse as it generates single photon most of the time. But it will not cause similar loss to decoy-pulse. On the other hand, effect of channel will be similar to both kind of pulses. Consequently if the loss of the decoy pulses is found to be abnormally less than that of signal pulses, then we conclude that Eve is present and the whole protocol is aborted. Otherwise we continue.

Entanglement is not required but do we need four states?

NO!

B-92 a two state protocol: Protocol 5

1. Alice sends Bob a random string of $|0\rangle$ and $|+\rangle$. We may assume that $|0\rangle$ corresponds to bit value 0 and $|+\rangle$ corresponds to bit value 1.

2. Bob measures all the incoming qubits randomly in one of the basis:

$$\{0, 1\} \text{ or } \{+, -\}$$

3. Bob keeps all those cases where his measurement outcome is $|1\rangle$ or $|-\rangle$ and discard all other cases. Bob neither announces the basis used to make a particular measurement nor the outcome. He just announces which qubits are to be kept and which are to be discarded. Following Bob's announcement Alice discards all such qubits for which Bob has obtained $|0\rangle$ or $|+\rangle$. If Bob's measurement yield $|0\rangle$ he will not be able conclude whether Alice has sent $|0\rangle$ or $|+\rangle$ as 50% of the time the $|+\rangle$ state measured in computational basis will collapse to $|0\rangle$. Consequently, if Bob's measurement yield $|0\rangle$ then he can not conclude anything about the encoding of Alice. Further, if Alice sends $|0\rangle$ then Bob can never get it as $|1\rangle$. This is so because if Bob chooses computational basis he will always get it as $|0\rangle$ and if he chooses diagonal basis then with equal probability he will obtain $|+\rangle$ or $|-\rangle$ state.

Protocol 5

- Thus Bob's measurement can yield $|1\rangle$ iff Alice has sent $|+\rangle$. Therefore, whenever Bob gets $|1\rangle$ he can conclude that Alice has sent $|+\rangle$. Similarly whenever Bob's measurement yields $|-\rangle$ he concludes that Alice has sent him $|0\rangle$ and he can not conclude anything whenever his measurement yields $|+\rangle$. As Bob knows the encoding, he can generate a random bit string (secured random key) which is symmetric with that of Alice.
4. Bob uses part of his string as verification string.

Some observations till now

Ekert's protocol:

Assume that there exist a source of entangled photon between Alice and Bob . It sends one photon to Alice and the other to Bob. It is equivalent to our simple minded approach. Now if Alice and Bob use three basis set to measure the state and find the correlation function's value to detect Eavesdropping then the protocol is called Eckert's protocol. When it uses two bases sets its equivalent to BB-84.

* Protocol 3 is not Ekert's protocol.

Observations

1. Security of Protocol 2-5 are ensured by conjugate coding. But non-realism is required for generation of random numbers.
2. Entanglement is not essential.
3. All these protocols are used to distribute secured key by quantum means.
4. To send a message we have to use this quantum key and some classical encoding techniques and the entire protocol would become hybrid.
5. All these protocols are 1 way and 1 step protocol.

Questions that arise in our mind

1. Can we design protocol for secured direct communication using quantum means
 2. Can we design two way protocols?
 3. Can we design one way two steps protocol?

Let us add some more complexity to the simple minded protocol: Ping-Pong Protocol : Protocol 6

Lets make it two-way:

- Bob prepares a set of bipartite-entangled states
- Bob keeps one photon (home photon) of each state with himself and sends the other photon (travel photon) to Alice.
- Alice wants to encode a key. Alice does nothing if she wants to encode 0 and applies a not gate on her qubit if she wants to encode 1 and resend the qubit to Bob.
- Now Bob does a measurement on both the qubits available with him. If Alice has encoded 0 then Bob will get the state same as what he had sent otherwise following transformation occurs $|\psi^\pm\rangle \leftrightarrow |\phi^\pm\rangle$
- Now Bob can easily identify the key encoded by Alice.
- This two way protocol is known as Ping-Pong protocol and was introduced by Bostrom and Felbinger in 2002. Note that the key is not essentially random and Alice can also send a message directly through this deterministic protocol.

Note

Power of dense-coding is not used. Efficiency can be increased.

Do we need entanglement for two way protocols? No.

The security is still ensured by conjugate coding by using part of the string for verification.

LM 05 a two way protocol without entanglement: Protocol 7

1. Bob prepares and sends Alice a random string of $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$.
2. Alice randomly chooses a set of qubits from the string received by her and forms a verification string. She measures all the qubits of verification string randomly in $\{0, 1\}$ or $\{+, -\}$ basis and announces which basis she has used to measure a particular state, position of that state in the string and outcome. Bob also measures the corresponding qubits using the same basis and compares his results with Alice. In absence of Eve the outcome of Alice and Bob will be perfectly correlated. In case perfect correlation is not observed they compare the error rate with the predecided tolerance limit. If the error due to noise or Eve is within tolerance limit then they continue to the next step otherwise they discard the protocol.
3. Alice wants to encode a key/message. Alice does nothing (does not apply identity operation I) if she wants to encode 0 and applies $iY=ZX$ on her qubit if she wants to encode 1 and resend the qubit to Bob. The encoding will transform the initial states into their orthogonal states as

$$\begin{aligned}
 iY|0\rangle &= ZX|0\rangle = Z|1\rangle = -|1\rangle \\
 iY|1\rangle &= ZX|1\rangle = Z|0\rangle = |0\rangle \\
 iY|\pm\rangle &= \frac{iY}{\sqrt{2}} (|0\rangle \pm |1\rangle) = \frac{1}{\sqrt{2}} (-|1\rangle \pm |0\rangle) = \pm|\mp\rangle
 \end{aligned}$$

Protocol 7

After the encoding Alice send back the qubit to Bob.

4. Presence of Eve during communication from Alice to Bob is checked using the verification string by following the same procedure as described in step 2 of this protocol.
5. Bob can deterministically decode Alice's message by measuring the qubit in the same basis he prepared it.
6. Now Bob can easily identify the key\message encoded by Alice.

Both LM 05 and Ping Pong protocols are two way and two step protocols. Ping Pong does not utilise full benefit of dense-coding. It is possible to design one way one step protocol.

Ping-pong and LM 05 are QSDC

- In both Ping-pong and LM-05 protocol Bob does not require classical communication from Alice to decode the message. Avoiding the use of a classical channel during message mode increases both the security and the efficiency of the protocol. All such direct communication protocols which does not require any classical communication for decoding of the encoded message are referred as QSDC protocols. In contrary all those protocols which require such communication are referred as Direct Secured Quantum Communication (DSQC) protocol. We have not yet described any DSQC protocol. We will describe one such protocol in next section.
- In QSDC protocols Alice can do the encoding without knowing the incoming state.
- Note that this task can not be achieved with two states. As long as we use conjugate coding. We need at least 4 states for 2 way direct communication. It would be interesting to see what happens when we don't use conjugate coding.
- LM-05 kind of protocols (which does not use entanglement) will always be less efficient compared to Ping-type of two way protocols and Deng type of one way protocol of QSDC which uses dense-coding. Use of dense-coding or hyper-dense-coding will increase efficiency.

A one way protocol for direct communication: Protocol 8 (Deng Protocol)

1. Alice prepares n copies of Bell states in $\frac{1}{\sqrt{2}} [|00\rangle + |11\rangle] = \frac{1}{\sqrt{2}} [|++\rangle + |--\rangle]$. She keeps the first qubit of all the entangled pairs with her and sends the second qubits to Alice.
2. Now Alice randomly chooses a set of qubits from her string and forms a verification string. She measures all the qubits of verification string randomly in $\{0, 1\}$ or $\{+, -\}$ basis and announces which basis she has used to measure a particular state, position of that state in the string and outcome. Bob also measures the corresponding qubits using the same basis and compares his results with Alice. This step is same as Protocol 2. Only difference is that here only part of the string (verification string) is measured to detect Eve. This step can detect Eve. In absence of Eve the outcome of Alice and Bob will be perfectly correlated. In case perfect correlation is not observed they compare the error rate with the pre-decided tolerance limit. If the error due to noise or Eve is within tolerance limit then they continue to the next step otherwise they discard the protocol. Thus part of the remaining string is kept for verification of Eavesdropping in return path and rest of the string is used to encode a message\key.

Protocol 8

3. Alice wants to encode a key/message. Alice does the encoding by usual dense coding operations I, X, iY, Z , which are by mutual agreement taken to designate bits 00, 01, 10, 11. Thus if Alice applies $U_{00} = I, U_{01} = X, U_{10} = iY, U_{11} = Z$ respectively to encode 00, 01, 10 and 11 respectively. Then after the encoding initial Bell state $|\psi^+\rangle$ is mapped to $|\psi^+\rangle, |\phi^+\rangle|\phi^-\rangle$ and $|\psi^-\rangle$ respectively if 00, 01, 10 and 11 are encoded respectively. After encoding Alice send back the qubits to Bob.
4. Presence of Eve during the communication from Alice to Bob is checked using the verification string by following the same procedure as described in step 2 of this protocol.
5. Now Bob performs a Bell measurement on both the qubits available with him. If Alice has encoded 00 then Bob will get back $|\psi^+\rangle$ (same as what he had sent), if Alice has sent 01, 10 or 11 respectively then Bob obtains $|\phi^+\rangle, |\phi^-\rangle$ and $|\psi^-\rangle$ respectively. Since these states are orthogonal to each other a Bell measurement will deterministically distinguish them and consequently decode the message encrypted by Alice.

In this two step protocol entire superposition is not available in the channel at a given time. This is the essence of Goldenberg and Vaidman protocol.

Can be converted to one step DSQC protocol with the help of rearrangement of ordering of particles.

DSQC using GHZ-like states without complete utilization of densecoding: Protocol 9

1. Alice prepares n copies of one of the GHZ-like states. Without loss of generality we may assume that Alice has prepared n copies of the GHZ-like state:

$$|\lambda\rangle = \frac{|\phi^{+0}\rangle + |\psi^{+1}\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} (|010\rangle + |100\rangle + |001\rangle + |111\rangle).$$

Now Alice prepares a sequence P of n ordered triplet of entangled particles as $P = \{p_1, p_2, \dots, p_n\}$, where the subscript 1,2,...,n denotes the order of a particle triplet $p_i = \{h_1^i, t_1^i, t_2^i\}$, which is in the state $|\lambda\rangle$. Symbol h and t are used to indicate home photon (h) and travel photon (t) respectively.

2. Alice encodes her secret message on sequence P by applying one of the four two qubit unitary operations $\{U_{00} = X \otimes I, U_{01} = I \otimes I, U_{10} = I \otimes Z, U_{11} = I \otimes iY\}$
3. on the particles (h_1^i, t_1^i) of each triplet. The unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ encodes $\{00, 01, 10, 11\}$ respectively. Here These operations $U_{ij}(i, j \in \{0, 1\})$ will transform the GHZ-like state $|\lambda\rangle$ into another GHZ-like state $|\lambda_{ij}\rangle$, where

$$\begin{aligned} |\lambda_{00}\rangle &= U_{00}|\lambda\rangle = \frac{1}{2}X \otimes I (|010\rangle + |100\rangle + |001\rangle + |111\rangle) = \frac{1}{2} (|110\rangle + |000\rangle + |101\rangle + |011\rangle) = \frac{|0\psi^+\rangle + |1\phi^+\rangle}{\sqrt{2}} \\ |\lambda_{01}\rangle &= U_{01}|\lambda\rangle = \frac{1}{2}I \otimes I (|010\rangle + |100\rangle + |001\rangle + |111\rangle) = \frac{1}{2} (|010\rangle + |100\rangle + |001\rangle + |111\rangle) = \frac{|0\phi^+\rangle + |1\psi^+\rangle}{\sqrt{2}} \\ |\lambda_{10}\rangle &= U_{10}|\lambda\rangle = \frac{1}{2}I \otimes Z (|010\rangle + |100\rangle + |001\rangle + |111\rangle) = \frac{1}{2} (-|010\rangle + |100\rangle + |001\rangle - |111\rangle) = \frac{|0\phi^-\rangle + |1\psi^-\rangle}{\sqrt{2}} \\ |\lambda_{11}\rangle &= U_{11}|\lambda\rangle = \frac{1}{2}I \otimes iY (|010\rangle + |100\rangle + |001\rangle + |111\rangle) = \frac{1}{2} (-|000\rangle + |110\rangle + |011\rangle - |101\rangle) = -\frac{|0\psi^-\rangle + |1\phi^-\rangle}{\sqrt{2}} \end{aligned}$$

Protocol 9

- Alice keeps the home photon (h_1) of each triplet with her and prepares a ordered sequence, $P_A = [p_1(h_1), p_2(h_2), \dots, p_n(h_n)]$. Similarly, she uses all the travel photons to prepare an ordered sequence
$$P_B = [p_1(t_1, t_2), p_2(t_1, t_2), \dots, p_n(t_1, t_2)].$$
- Alice disturbs the order of the pair of travel photons in P_B and create a new sequence $P'_B = [p'_1(t_1, t_2), p'_2(t_1, t_2), \dots, p'_n(t_1, t_2)]$. The actual order is known to Alice only.
- For preventing the eavesdropping, Alice prepares m decoy photons $\otimes_{j=1}^m |P_j\rangle, |P_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}, (j = 1, 2, \dots, m)$. Then Alice randomly inserts these decoy photons into the sequence P'_B and creates a new sequence P'_{B+m} which she transmits to Bob. P_A remains with Alice.
- After confirming that Bob has received the entire sequence P'_{B+m} , Alice announces the positions of the decoy photons. Bob measures the corresponding particles in the sequence P'_{B+m} by using X basis or Z basis at random.

After measurement, Bob publicly announces the result and the basis used. Alice has to discard the 50% cases where, Bob has chosen wrong basis. From the remaining outcomes Alice can compute the error rate and check whether it exceeds the predecided threshold or not. If it exceeds the threshold, then Alice and Bob abort this communication and repeat the procedure from the beginning. Otherwise they go on to the next step.

7. After knowing the position of the decoy photons Bob has already obtained the sequence P'_B . Now Alice discloses the actual order of the sequence and Bob uses this information to convert the reordered sequence P'_B to the original sequence P_B .

8. Now Alice measures her home qubit in computational basis (Z basis) and announces the result. Bob measures his qubits in Bell basis. Knowing the results of measurements of Alice and that of his own measurement, Bob can easily decode the encoded information. For clarity in Table 1 below we have provided a relation between the measurement outcomes and the secret messages in Table below.

Alice's measurement result	Bob's measurement result	Decoded secret
0	ψ^+	00
	ψ^-	11
	ϕ^+	01
	ϕ^-	10
1	ψ^+	01
	ψ^-	10
	ϕ^+	00
	ϕ^-	11

Protocol 10: Goldenberg and Vaidman (GV) protocol

Let $|a\rangle$ and $|b\rangle$ be two localized wave packets, which are sent from Alice to Bob along two separated channels. We shall take two orthogonal states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, linear combinations of $|a\rangle$ and $|b\rangle$, to represent bit value “0” and bit value “1,” respectively:

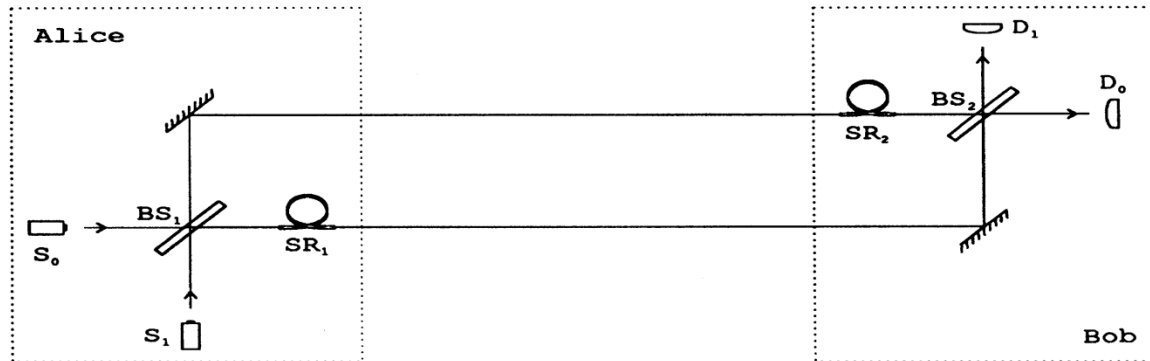
$$|\Psi_0\rangle = 1/\sqrt{2} (|a\rangle + |b\rangle), \quad (1)$$

$$|\Psi_1\rangle = 1/\sqrt{2} (|a\rangle - |b\rangle). \quad (2)$$

Alice sends to Bob either $|\Psi_0\rangle$ or $|\Psi_1\rangle$. The two localized wave packets, $|a\rangle$ and $|b\rangle$, are not sent together, but wave packet $|b\rangle$ is delayed for some time τ . For simplicity, we choose τ to be larger than the traveling time of the particles from Alice to Bob, θ . Thus $|b\rangle$ starts traveling towards Bob only when $|a\rangle$ already has reached Bob, such that the two wave packets are never found together in the transmission channels.

Note: Information is encoded in a superposition state but the entire superposition is not available in the channel at any time. Entangled state is superposition in tensor product space. Consequently in the last few protocols we are doing the same thing.

Mach-Zehnder interferometer and quantum cryptography with orthogonal state



Vaidman and Goldenberg protocol

 Cryptographic scheme based on a Mach-Zehnder interferometer. The device consists of two particle sources S_0 and S_1 , a beam splitter BS_1 , two mirrors, two storage rings SR_1 and SR_2 , a beam splitter BS_2 , and two detectors D_0 and D_1 . The device is tuned in such a way that, if no eavesdropper is present, a particle emitted by S_0 (S_1) is finally detected by D_0 (D_1).

Goldenberg and Vaidman protocol

Alice and Bob perform two tests to detect Eve (using a classical channel) .

1. They compare the sending time t_s with the receiving time t_r for each particle. Since the travelling time is θ and the delay time is τ , we must have $t_r = t_s + \theta + \tau$.
2. They look for changes in the data by comparing a portion of the transmitted bits with the same portion of the received bits.

Generalization of Goldeberg-Vaidman idea: DSQC and QSDC using orthogonal states

1. Assume that in the above protocol Bob sends a random string of $|\psi_0\rangle$ and $|\psi_1\rangle$ to Alice and Alice encodes 0 or 1 by applying identity and phase flip operations and returns the state by using Vaidman-Goldenberg protocol. Bob will measure the final state and since he knows the initial state he will be able to decode Alice's message. (Eve may learn the final state but since he does not know the initial state he knows nothing about the encoded message, this is Ping Pong with orthogonal states.
2. Above tests implied to protocol 8 and 9 will make them free of Conjugate coding. Thus we can do all these tasks by using non-realism only.

Is GV protocol fundamentally different from BB-84 kind of Protocols?

Objections and observations related to GV protocol

1. Peres (PRL 76 (1996) 3264) : For Eve the states are non-orthogonal in both BB-84 and GV protocol.
2. Gao et al (Phys. Lett. A 355 (2006) 172): Introduces Mid protocol and claims that information splitting is essence of both BB-84 and GV protocols.
3. Tal Mor (PRL 80 (1998) 3137): No cloning of orthogonal state.

Is GV protocol fundamentally different from BB-84 kind of Protocols?

What provides security to GV protocol?

the two bit states of the GV protocol can be represented as

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

$$|1\rangle = \frac{1}{\sqrt{2}}(|\mathit{here}\rangle - |\mathit{there}\rangle)$$

Because of maximal non-realism, there is precisely one basis in which the logical bit states can be decoded deterministically, namely $\{\frac{1}{\sqrt{2}}(|\mathit{here}\rangle + |\mathit{there}\rangle), \frac{1}{\sqrt{2}}(|\mathit{here}\rangle - |\mathit{there}\rangle)\}$.

Security of the GV protocol comes from the geographic constraint that by ensuring that the `here' (proximal) and `there' (distal) pieces are not available simultaneously at one place, thus the special basis cannot be implemented. In fact, security is maximal in that the only basis that can be implemented is $\{|\mathit{here}\rangle, |\mathit{there}\rangle\}$, and

$$\text{Prob}(|0\rangle|\mathit{here}) = \text{Prob}(|0\rangle|\mathit{there}) = \text{Prob}(|1\rangle|\mathit{here}) = \text{Prob}(|1\rangle|\mathit{there}) = \frac{1}{2}.$$

On the other hand, by being able to access this special basis, Bob can safely decode the logical bit states.

Is GV protocol fundamentally different from BB-84 kind of Protocols?

Note that the last statement subsumes

1. The important clarification of Tal Mor [PRA 80 (1998) 3137] that nonlocal states like $|0\rangle$ and $|1\rangle$ cannot be cloned even though they are orthogonal, unless the proximal and distal pieces are made simultaneously available;
2. Measurement in a basis other than the special basis disturbs the system. Otherwise cloning or non-destructive measurement could be used to determine the state, contrary to assumption of maximal non-realism.
3. In a BB84-class protocol, the encoding use internal degrees of freedom like polarization or spin. In this case, no geographic or suchlike constraint can be imposed to prohibit the measurement of the set of coding states in their special basis. Thus we add another set of coding states, with a different special basis. The ambiguity between the two bases is the basic idea of security in such protocols. (This is where GV is different)
4. Assume that the special basis is equivalent to an observable (a hermitian operator) of which the coding states are eigenstates, then it is easy to see that the two bases must correspond to non-commuting observables. Thus these protocols require the use of non-orthogonal states over and above non-realist physics.

Conclusion

- GV-class protocols are the more primitive, in that they require only non-realism for their security, whereas BB84-class protocols require both non-realism and non-orthogonal state encoding (conjugate coding).

Protocol 11: Orthogonal State Based Modified Ping Pong Protocol

1. Bob prepares n number of orthogonal states randomly prepared in $|\psi_0\rangle$ or $|\psi_1\rangle$ and communicate that to Alice by following the GV protocol (i.e. by sending the wave packet $|a\rangle$ first and by sending $|b\rangle$ at a later time after $|a\rangle$ reaches Alice).
2. Alice and Bob compare the sending time t_s with the receiving time t_r for each wave packet. Since the travelling time is θ and the delay time is τ , we must have $t_r = t_s + \theta + \tau$. This ensures that Eve can not delay $|a\rangle$ and wait for $|b\rangle$ to reach so that he can appropriately superpose them.

Alice randomly chooses a set of orthogonal states from the states received by her and forms a verification string. She measures all the qubits of verification string and compares her results with Bob. This step can detect Eve. In absence of Eve the outcome of Alice and Bob will be perfectly correlated. Now, absence of Eve in the communication from Bob to Alice does not exclude the possibility of Eavesdropping during the communication from Alice to Bob. Thus part of the remaining string is kept for verification of Eavesdropping in return path and rest of the string (message string) is used to encode a message\key.

Orthogonal State Based Modified Ping Pong Protocol

3. Alice wants to encode a key\message. Alice does nothing if she wants to encode 0 and applies a phase-flip gate on her state if she wants to encode 1 . The encoding is done only on the message string. After the encoding operation Alice send back the qubit to Bob by using GV protocol.
4. Presence of Eve during the communication from Alice to Bob is checked using the verification string by following the same procedure as described in step 2 of this protocol.
5. Bob will measure the final state in $\{|\psi_0\rangle, |\psi_1\rangle\}$ basis since $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal to each other and as Bob knows the initial state, he will be able to decode Alice's message.

Eve may learn the final state but since he does not know the initial state he knows nothing about the encoded message.

Is anything interesting in this orthogonal state based QSDC protocol?

1. This is the first orthogonal state based protocol of QSDC.
2. This is the first protocol of QSDC which requires only two states. Traditionally it was believed that two non-orthogonal states are sufficient for QKD but at least 4 states are required for DSQC or QSDC. This is true for conjugate coding based protocols as conjugate coding based protocols of QSDC or DSQC will require at least 4 states but superposition based protocols (orthogonal state based Ping Pong protocol can do it in two steps). Further, we would like to note that the above modifications of B-92 makes it equivalent to LM-05 protocol.
3. iii) This is clearly a QSDC protocol without entanglement. Thus we obtain a kind of modified LM-05 protocol without non-orthogonal states.
4. All the existing protocol of QSDC uses either non-orthogonal states or entangled states but the above protocol does not use any of them in general.

Protocol 12: Orthogonal state based DSQC protocol

1. Alice prepares a random string n Bell states (i.e. a random string of

$$|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle \text{ and } |\phi^-\rangle.$$

Now Alice prepares a sequence P of n ordered pair of entangled particles as

$$P = \{(p_1(1), p_1(2)), (p_2(1), p_2(2)) \dots\dots\dots, (p_n(1), p_n(2))\},$$

where $p_i(1)$ denotes the first particle of the i th Bell state and similarly $p_i(2)$ denotes the second particle of the i th Bell state, $i=1,2,\dots,n$. Alice uses the first qubit of each Bell state to form an ordered sequence, $P_A = [p_1(1), p_2(1), \dots, p_n(1)]$. Similarly, she uses all the second qubits to prepare an ordered sequence $P_B = [p_1(2), p_2(2), \dots, p_n(2)]$.

2. Alice uses part of the sequence P_A for encoding of message\key and remaining part for verification. Which qubits are to be used for verification is chosen randomly by Alice and it remains known only to Alice till she discloses it. We may think that sequence P_A contains two sequences $P_{A,m}$ used for encoding of message and sequence $P_{A,v}$ used for verification. Similarly P_B is also comprises of $P_{B,m}$ and $P_{B,v}$. No encoding is done on $P_{B,m}$, simply i th particle of $P_{B,m}$ is entangled with the i th particle of in $P_{A,m}$ and similarly i th particle of $P_{B,v}$ are entangled with the i th particle of in $P_{A,v}$.

Orthogonal state based DSQC protocol

3. Alice encodes her secret message on sequence $P_{A,m}$ by applying one of the four two qubit unitary operations $\{U_{00} = X, U_{01} = I, U_{10} = iY, U_{11} = Z\}$ on the first particles of each Bell states that are chosen for message encryption. The unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ encodes $\{00, 01, 10, 11\}$ respectively.
4. Alice disturbs the order of the qubits in sequence P_B and create a new sequence $P'_B = [p'_1(2), p'_2(2), \dots, p'_n(2)]$. The actual order is known to Alice only.
5. Alice sends both the sequence $(P_A \text{ and } P'_B)$ to Bob and following GV protocol confirms that Bob has received all the particles of sequence P_A and P'_B in appropriate time.

Orthogonal state based DSQC protocol

6. After confirming that Bob has received the entire sequences P_A and P_B , Alice announces the positions of the verification qubits in both the sequences (i.e. she announces $P_{A,v}$ and $P'_{B,v}$) and which particle of sequence $P_{A,v}$ is entangled with which particle of sequence $P'_{B,v}$. Bob does the Bell measurement on each entangled pairs and publicly announces the results of his measurements. From Bob's announcement Alice can compute the error rate and check whether it exceeds the pre-decided threshold or not. If it exceeds the threshold, then Alice and Bob abort this communication and repeat the procedure from the beginning. Otherwise they go on to the next step. Even if Eve exist she will not obtain any meaningful information as the exact sequence and initial states are known to Alice only.
7. After knowing the position of the verification qubits Bob has already obtained the message sequence $P_{A,m}$ and $P'_{B,m}$. Now Alice discloses the actual order of the sequence and the initial states. Bob uses the actual order to convert the reordered sequence $P'_{B,m}$ to the original sequence $P_{B,m}$ and does Bell measurement with qubit of $P_{A,m}$ and i th qubit of $P_{B,m}$. Since Bob already knows the initial state, he easily obtain the message\key encoded by Alice.

Thank you