

NEW QUANTUM CRYPTOGRAPHIC PROTOCOL

Cătălin ANGHEL

Faculty of Computer Science, University "Dunărea de Jos" of Galati
 2 Științei, 800146 Galati, Romania, e-mail: catalin.anghel@ugal.ro

Abstract: One of the main research directions of quantum cryptography is to discover new algorithms and to improve the existing ones. This paper proposes a new quantum cryptographic algorithm based on BSTS algorithm with QBTT method of eavesdropper detection which can realize a perfectly secure communication between two computers.

Keywords: quantum cryptography, quantum physics, quantum key distribution, qkd, quantum algorithm, bsts, qbtt.

1. BASE SELECTION AND TRANSMISSION SYNCHRONIZATION PROTOCOL

After the Secret Key Reconciliation and Privacy Amplification (Bennett, 1992) process of any quantum cryptographic algorithm, the *final key* obtained by *Sender* and *Receiver* is too small comparing with the initial binary sequence s , fig. 1.

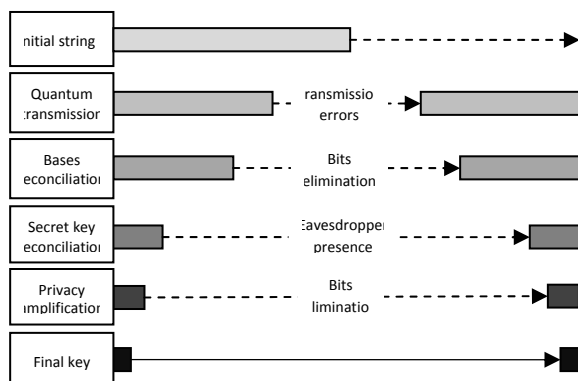


Fig.1. Final key comparing to initial string s

We can use the *final key* to implement the Base Selection and Transmission Synchronization algorithm (Anghel, and Coman, 2009), which can realize a perfectly secure communication between two computers.

In order to create the quantum communication process between *Sender* and *Receiver*, we need to use

some special devices that can transmit, polarize and receive photons and without a computer, with special software, this communication cannot be done. This software can be implemented in order to transmit, receive and analyze the photon transmission between *Sender* and *Receiver*.

This communication protocol will establish, accordingly to the *final key*, which pair of bases, between *rectilinear* (0° , 90°), *diagonal* (45° , 135°) and *circular* (left - *spinL*, right - *spinR*), will be used for photons polarizations. Accordingly to the *final key*, the communication protocol will establish also the polarization base for each photon that has to be transmitted, so the *Sender* and *Receiver* will know for each particular photon the polarization base – this process will be named *base selection*. Finally, accordingly to the *final key*, the communication protocol will establish the moments in time when *Sender* will send a photon and *Receiver* will read the photon – this process will be named *transmission synchronization*.

In the rest of the time *Sender* will send out fake arbitrary polarized photons which will be ignored by the *Receiver*.

1.1. Steps in Base Selection and Transmission Synchronization protocol

Accordingly to the *final key*, which is common to *Sender* and *Receiver*, the steps of the BSTS protocol are:

1. First two bits from *final key* will be used to establish the two polarization bases which will be used to polarize the photons for current transmission:

Table 1. Base selection

Bit 1	Bit 2	Base 1	Base 2
0	0	R(rectilinear)	D(diagonal)
0	1	R(rectilinear)	C(circular)
1	0	C(circular)	D(diagonal)
1	1	R(rectilinear)	D(diagonal)

2. Next four bits from *final key*, converted in 10 bases + 1, will be a number that represents the timing interval expressed in milliseconds. Accordingly to the timing interval, the *Sender* will send photons and *Receiver* will read photons. *Sender* can communicate to *Receiver*, thru the public channel, the moments of start and the end of transmission.

Table 2. Time

Bit 3	Bit 4	Bit 5	Bit 6	Time (ms)
0	0	0	0	1
0	0	0	1	2
.....				
1	1	1	1	16

3. The remaining bits from *final key* will represent the polarization base of each photon that we have to transmit or to receive:

Table 3. Base

Bit	0	1
Polarization	Base 1	Base 2

After the last bit from *final key* the process of polarization will be continued from the bit number 7 and so on.

4. *Sender* and *Receiver* communicate thru the classical channel and divide their bit sequences into blocks and compare each other's parity for each block. Whenever their respective parities for any given block do not match they will retransmit that block.

1.2. Theoretical Example

Let us suppose that the bits in *final key* are: 01100110011...

Table 4. Bits in final key

Nr	1	2	3	4	5	6	7	8	9	10	11	...
Bit	0	1	1	0	0	1	1	0	0	1	1	...

Sender and *Receiver* have the same bits in *final key* and they make the following actions:

1. Determine the two bases that will be used by *Sender* and *Receiver* for photons polarization

Table 5. Bits 1, 2 from final key

Bit 1	Bit 2	Base 1	Base 2
0	1	R (rectilinear)	C (circular)

They will use for photons polarization the rectilinear and circular bases.

2. Determine the interval for sending and receiving real photons.

Table 6. Bits 3,4,5,6 from final key

Bit 3	Bit 4	Bit 5	Bit 6	Time (ms)
1	0	0	1	9

Sender will transmit the fake photons all the time but from 9 to 9 ms it will transmit the real photons to the *Receiver*. Also the *Receiver* will read photons only from 9 to 9 ms.

3. Determine each photon polarization base

Table 7. Bits 3,4,5,6 from final key

Bit	0	1
Polarization	Base 1	Base 2

Table 8. Bits 3,4,5,6 from final key

Nr	1	2	3	4	5	6	7	8	9	10	11
Bit	0	1	1	0	0	1	1	0	0	1	1
Base							C	R	R	C	C

So the first bit, that we have to transmit, will be represented by a photon polarized in circular base, the second one will be represented by a photon polarized in rectilinearly base, and so on. After the last bit from *final key* the process of polarization will be continued from the bit number 7.

4. At the end of quantum transmission, *Sender* and *Receiver* divide their bit sequences into blocks of 16 bits. They communicate thru the classical channel, comparing each other's blocks parity, and retransmit blocks that the parity did not mach.

1.3. Logical diagram of BSTS protocol

In figure 2 we present the logical diagram of Base Selection and Transmission Synchronization quantum transmission protocol.

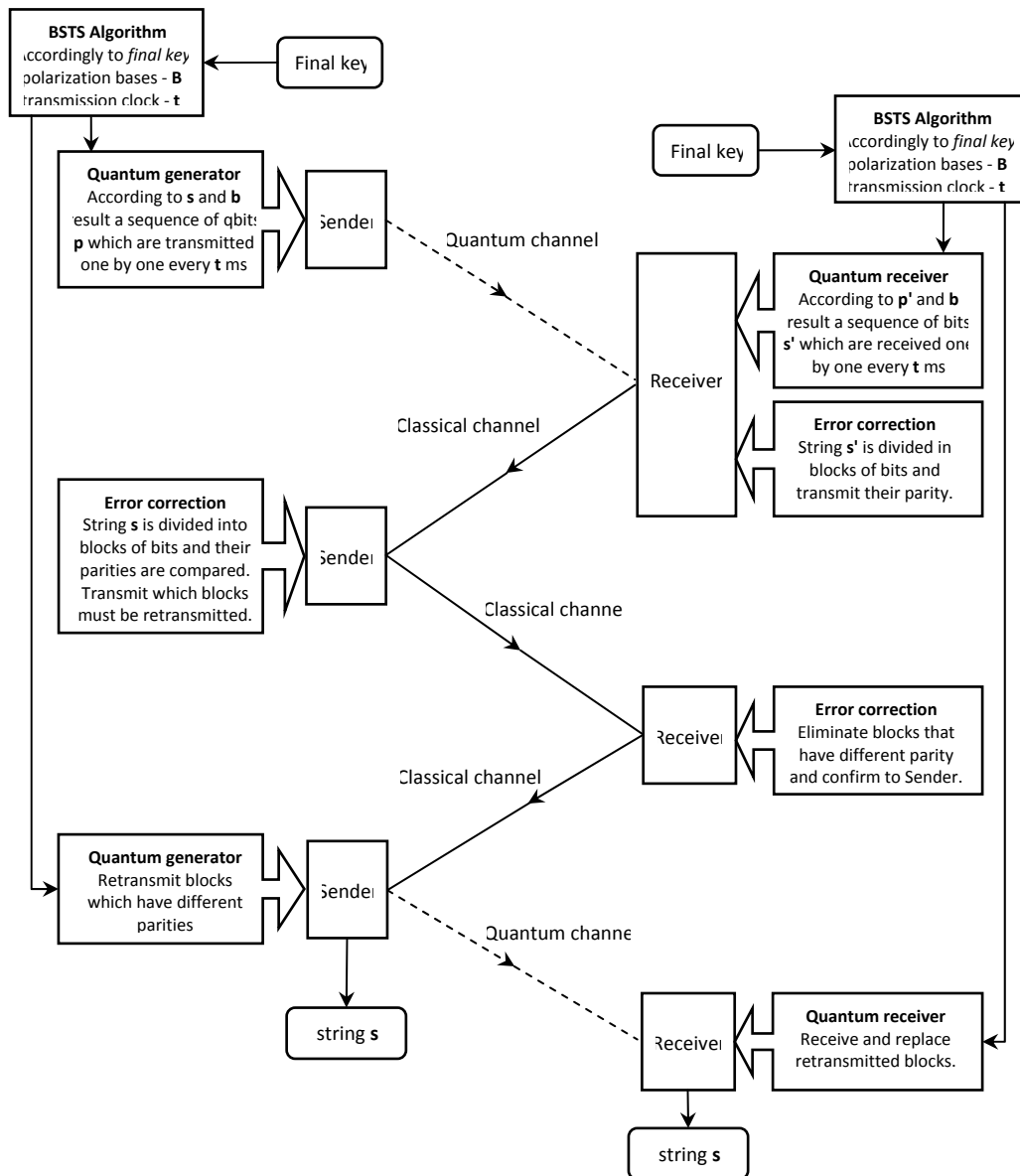


Fig.2. Logical diagram of BSTS protocol

1.4. Pseudo code of the BSTS protocol

Step 1 – Base Selection

Sender and Receiver:

```

IF s[1] == 0
    IF s[2] == 0
        base1 = R
        base2 = D
    ELSE //s[2] = 1
        base1 = R
        base2 = C
    ENDIF
ELSEIF //s[1] = 1
    IF s[2] == 0
        base1 = C
        base2 = D
    ELSE //s[2] = 1
        base1 = R
        base2 = D
    
```

```

ENDIF
ENDIF

```

Step 2 – Transmission Synchronization

Sender and Receiver:

$t = \text{convert bits } [3, 4, 5, 6] \text{ from binary to decimal} + 1$

Step 3 – Photon Polarization

Sender and Receiver:

```

FOR (i = 7; i <= s.length; i++)
    IF s[i] == 0
        b[j] = base1
    ELSE // c[i] = 1
        b[j] = base2
    ENDIF
ENDIF
ENDFOR

```

Step 4 – Quantum Transmission

Sender:

```

FOR (k = 0; k <= str.length; k++)
    time = 0

```

```

polarize photon in base b[k] result qbit p[k]
send qbit p[k]
DO
    send fake photons
WHILE (time < t)
ENDFOR

```

Receiver:

```

receive qbit p[k]
wait t ms

```

Step 5 – Error Correction

Sender and Receiver:

```

FOR (k = 0; k <= str.length; k++)
    divide string in 16 bits blocks
    FOR (each block compute parity pp)
        send pp
        receive pp'
        IF pp ≠ pp'
            resend block
        ENDIF
    ENDFOR
ENDFOR

```

2. QUANTUM BIT TRAVEL TIME
EAVESDROPPER DETECTION METHOD

The Quantum Bit Travel Time – QBTT method can be implemented in every type of quantum key distribution system to replace the classical eavesdropper detection method and to increase the security of the system.

2.1. Quantum Bit Travel Time principle

The Quantum Bit Travel Time – QBTT method can be implemented in every type of quantum key distribution system. It has the advantage that the *Eavesdropper* can be detected by *Receiver*, during the quantum transmission, after each transmitted qbit and it is not confused with errors caused by noise because noises does not induce time delays.

The QBTT method uses the fact that the optical components (polarization filters) induce time delays. Every polarization filter applied to a photon induces a specific time delay.

So it is reasonable for a particle to experience a time delay ΔT when it passes through the polarization system on *Sender's* side and detection system on *Receiver's* side. This delay can be measured and if, an eavesdropper try to read a photon, he will induce an additional time delay Δt . *Receiver* can measure these time delays and use them to detect the *Eavesdropper's* presence because the final time delay will be:

$$(1) \Delta T' = \Delta T + \Delta t.$$

2.2. Detecting Eavesdropper's presence

For each qbit received there is a time delay ΔT between the moment of transmission and the moment of reception. If an *Eavesdropper* tries to tap the quantum channel, that imply he have to read the qbits with a polarization filter, he will induce a new time delay Δt . The final time delay for each tapped qbit will be $\Delta T' = \Delta T + \Delta t$. This allows *Sender* and *Receiver* to detect the *Eavesdropper's* presence, and to reschedule their communications accordingly.

3. A NEW QUANTUM CRYPTOGRAPHIC
PROTOCOL







Founded on Base Selection and Transmission Synchronization (Anghel, and Coman, 2009) quantum cryptographic protocol and Quantum Bit Travel Time eavesdropper detection method, I proposed a new quantum cryptographic protocol, named, from now on, Base Selection and Polarization Agreement – BSPA.

Based on the bits from the *final key*, common to *Sender* and *Receiver*, targeted parameters in Base Selection and Polarization Agreement quantum cryptographic protocol are:

1. Which pair of bases, between *rectilinear* (0° , 90°), *diagonal* (45° , 135°) and *circular* (left - *spinL*, right - *spinR*), will be used for photons polarizations.
2. The polarization base for each photon, that has to be transmitted, so the *Sender* and *Receiver* will know for each particular photon the polarization base.
3. Eavesdropper detection by monitoring the travel time, from *Sender* to *Receiver*, of each photon.
4. Comparison the parity of the blocks received, at the end of quantum transmission and retransmission of the corresponding blocks.

For photon polarization we use the convention from table 9.

Table 9. Photon polarization

Base	L	D	C	C	L	D
Polarization	0°	45°	spinL	spinR	90°	135°
Qbit						
Bit	0	0	0	1	1	1

In Base Selection and Polarization Agreement quantum communication protocol, *Sender* and *Receiver* will establish in common, accordingly to the *final key*, which pair of bases, rectilinear-diagonal, rectilinear-circular or diagonal-circular will be used for photons polarizations.

Also, accordingly to the *final key*, *Sender* and *Receiver* will establish exactly which polarization base to apply for each photon that has to be transmitted or received.

During quantum transmission, after every received qbit, *Receiver* will verify the time delay ΔT of the photon from the moment of transmission and the moment of reception.

If the delay time ΔT is not in normal limit, limits established by earlier communications, *Receiver* will stop the transmission.

At the end of quantum transmission, *Sender* and *Receiver* divide their bit sequences into blocks. They communicate thru the classical channel, comparing each other's blocks parity and retransmitting blocks that the parity did not match.

3.1. Block diagram of BSPA protocol

In figure 3 we present the block diagram of Base Selection and Polarization Agreement quantum transmission protocol.

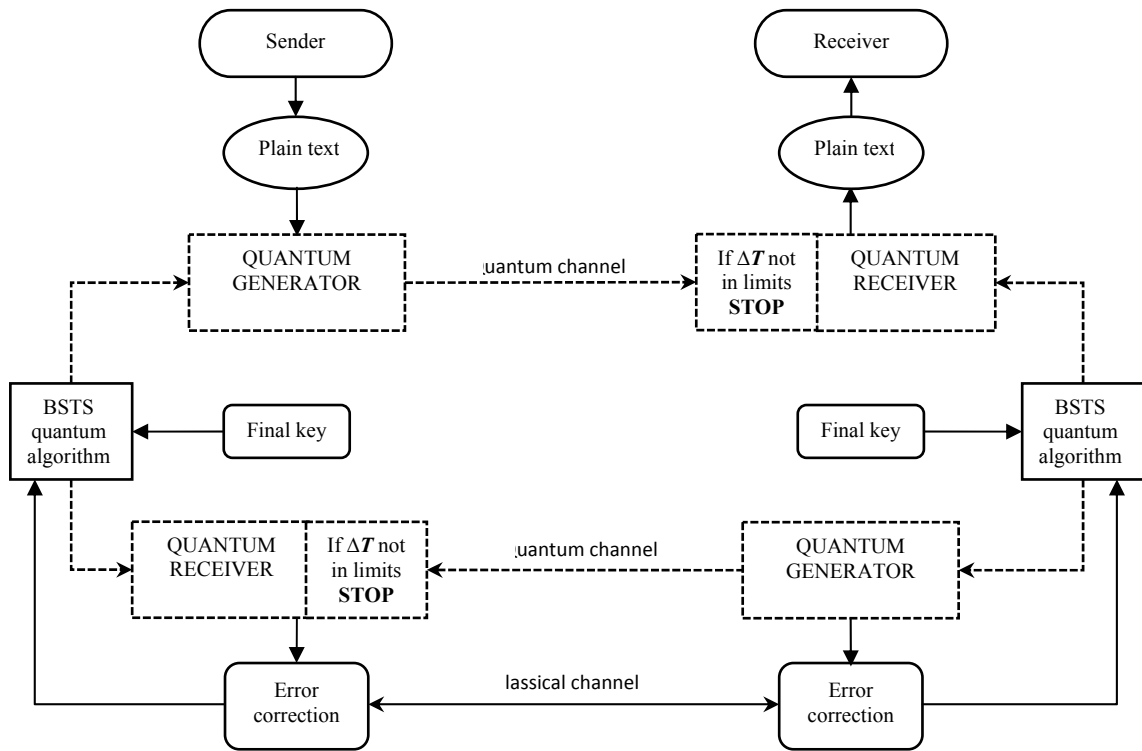


Fig.3. Block diagram of BSPA protocol

3.2. Steps in Base Selection and Polarization Agreement protocol

Accordingly to the *final key*, the steps of the BSPA protocol are:

1. First two bits from *final key* will be used to establish the two polarization bases which will be used to polarize the photons for current transmission:

Table 10. Base selection

Bit 1	Bit 2	Base 1	Base 2
0	0	R	D
0	1	R	C
1	0	C	D
1	1	R	D

2. The remaining bits from *final key* will represent the polarization base of each photon that we have to transmit or to receive:

Table 11. Polarization Agreement

Bit	0	1
Polarization	Base 1	Base 2

After the last bit from *final key* the process of polarization will be continued from the bit number 3 from *final key* and so on.

3. For every received qbit, *Sender* transmits to *Receiver*, thru the classical channel, the timestamp of the moment of transmission – TsS. For every received qbit, *Receiver* generates timestamp of the moment of reception – TsR and will calculate ΔT .

$$(2) \Delta T = T_{sR} - T_{sS}$$

If, for a particular qbit, the delay time ΔT is bigger than usual that imply the Eavesdropper has tapped that qbit and stops the communication.

4. *Sender* and *Receiver* divide their bit sequences into blocks of 16 bits. They communicate thru the classical channel, comparing each other's blocks parity and retransmit blocks that the parity did not match.

3.3 Pseudo code of the BSPA protocol

Step 1 – Base Selection

Sender and Receiver:

```

IF s[1] == 0
  IF s[2] == 0
    base1 = R
    base2 = D
  ELSE // s[2] = 1
    base1 = R
    base2 = C
  ENDIF
ELSEIF // s[1] = 1
  IF s[2] == 0
    base1 = C
    base2 = D
  ELSE // s[2] = 1
    base1 = R
    base2 = D
  ENDIF
ENDIF

```

Step 2 – Polarization Agreement

Sender and Receiver:

```

FOR (i = 3; i <= s.length; i++)
  IF s[i] == 0
    b[j] = base1
  ELSE // s[i] = 1
    b[j] = base2
  ENDIF
ENDFOR

```

Step 3 – Quantum polarization and transmission

Sender:

```

FOR (k = 0; k <= str.length; k++)
  polarize photon in base b[k] result qbit p[k]
  generate timestamp T
  send T to Receiver // classical channel
  send qbit p[k] to Receptor // quantum channel
ENDFOR

```

Receiver :

DO

```

receive qbit p[k]
generate timestamp T'
calculate ΔT = T' - T
IF ΔT NOT in limits
  Eavesdropper present
  STOP transmission
ENDIF
WHILE (transmission end)

```

Step 4 – Error Correction

Sender and Receiver:

```

FOR (k = 0; k <= str.length; k++)
  divide str in 16 bits blocks
  FOR (each block calculate parity pp)
    send pp
    receive pp'
    IF pp ≠ pp'
      resend block
    ENDIF
  ENDFOR

```

3.4. Advantages of BSPA protocol

Main advantages of the Base Selection and Polarization Agreement quantum communication protocol are:

- *Eavesdropper* can be detected during quantum transmission after each transmitted qbit, comparing to other quantum key distribution algorithms (Bennett, and Brassard, 1984; Bennett, 1992; Ekert, 1991) in which cases eavesdropper can be detected only at the end of quantum transmission after Bases Reconciliation stage on classical channel.

- *Eavesdropper* cannot be confused with quantum channel noises because noises do not induce a time delay.

- Base Selection and Polarization Agreement quantum communication protocol is faster than Base Selection and Transmission Synchronization protocol due to the elimination of the Transmission Synchronization stage.

- Base Selection and Polarization Agreement quantum communication protocol can realize a quantum network communication protocol between two computers.

3.5. Logical diagram of BSPA protocol

In figure 4 we present the logical diagram of BSPA quantum communication protocol.

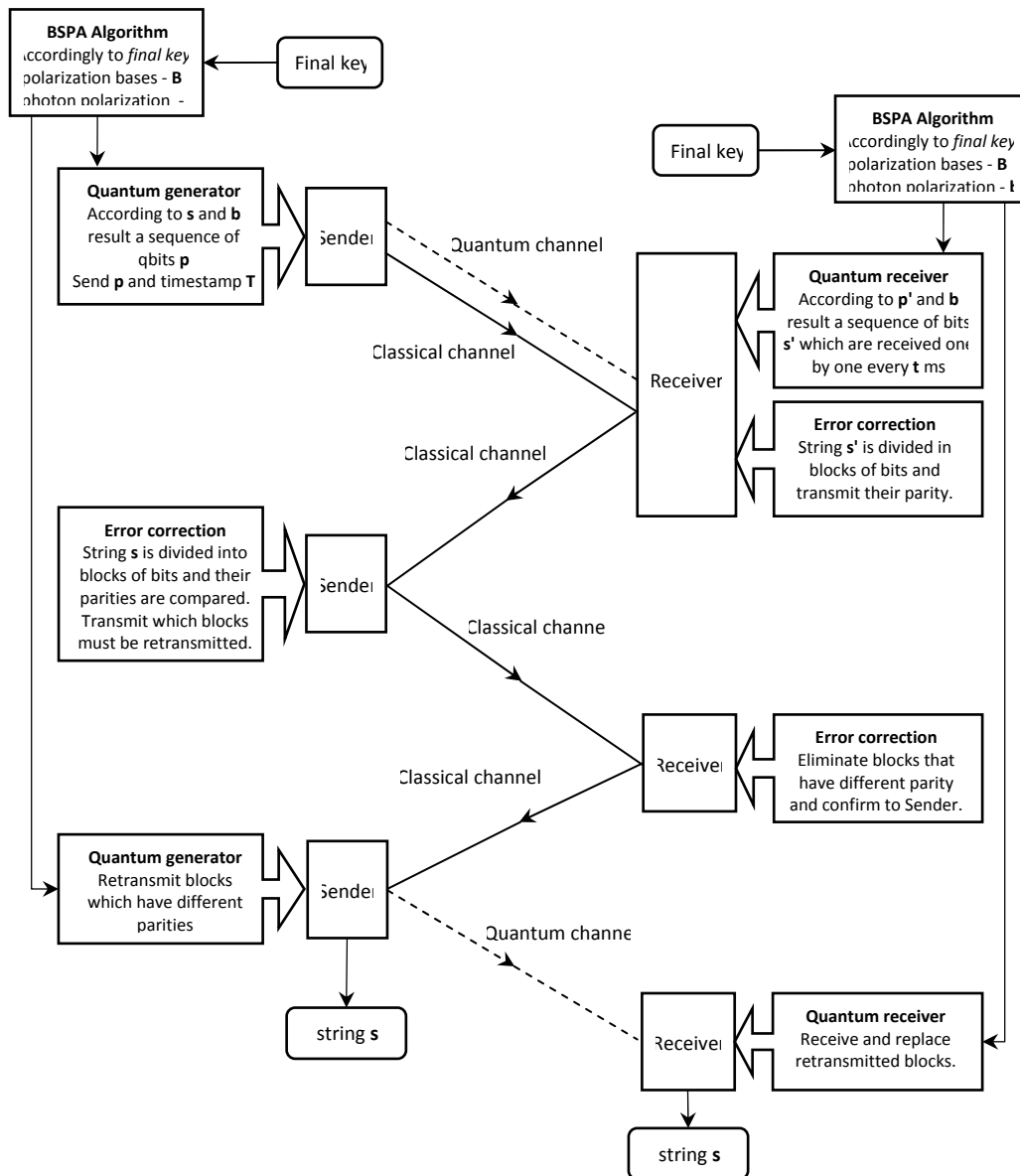


Fig.4. Logical diagram of BSPA protocol

4. CONCLUSIONS

This paper proposes a new quantum cryptographic communication protocol named Base Selection and Polarization Agreement.

The main advantages of this protocol are that it can realize a bidirectional quantum transmission between *Sender* and *Receiver* and the *Eavesdropper* can be detected instantly and precisely.

Instantly means that the *Eavesdropper* can be detected during the quantum transmission.

Precisely means that the *Eavesdropper* cannot be confused with noise errors because noises do not induce time delays.

REFERENCES

- Anghel, C. and Coman, G. (2009). Base selection and transmission synchronization algorithm in quantum cryptography. *Proceedings CSCS17 - 17th International Conference on Control Systems and Computer Science*, vol. 1, pp. 281-284, 2009, Bucharest, Romania, ISSN : 2066-4451.
- Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pp. 175-179, Bangalore, India.
- Bennett, C.H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, vol. 68, pp. 3121-3124.
- Ekert, A. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, vol. 67, nr. 6, pp. 661-663.