Journal of Computer Science

Original Research Paper

A Quantum Key Distribution Protocol Based on Random Bell Pair Selection

Devendar Rao Babu and Ramkumar Jayaraman

Department of Computing Technologies, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India

Article history
Received: 01-06-2023
Revised: 03-07-2023
Accepted: 27-07-2023

Corresponding Author:
Ramkumar Jayaraman
Department of Computing Technologies, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India
Email: ram.kumar537@gmail.com

Abstract: The traditional security system, which depends on asymmetric and symmetric key exchange protocol, is now under threat due to recent developments in quantum computing. In order to generate the safe key without storing the qubit by the sender or recipient trustworthy parties, a unique Quantum Key Distribution (QKD) protocol was presented. Four random classical bits coupled to generate a pair of bell states in any of the places {(1,2,3,4), (1,3,2,4) and (1,4,2,3)}. "n/2" groups were used to generate the raw key while the remaining groups were used to check for Eve. The flying bell states scatter into four separate bell states as a result of Eve's involvement in choosing the incorrect measurement basis, which causes entanglement swapping and its identification during communication. The sender will alter the key in accordance with the receiver's position preference because, in traditional communication, key receiving parties must announce the position information. Under the intercept-measure-resend attack, the trade-off between the key generating rate and disturbance is computed and security is examined. Circuit simulation is demonstrated graphically in IBM Quantum Lab and the proposed protocol is implemented.

Keywords: Bell Pair, Entanglement Swapping, Superdense Coding, Quantum Key Distribution

Introduction

The development in the quantum era had made the modern days security system in threat and infeasible to rely on for further communication (Shor, 1999). Quantum impacts the security and increases the performance of the algorithm by speeding up as compared to classical ones. Advanced research development occurs in a quantum network (Wu *et al*., 2015), Quantum internet (Cacciapuoti *et al*., 2019), and quantum machine learning (Sierra-Sosa *et al*., 2020). Various research progresses are happening in the field of quantum security like quantum secret sharing (Hillery *et al*., 1999), quantum signature (Guo *et al*., 2013), quantum dialogue (Lin *et al*., 2015), and Quantum privacy query (Yang and Wen, 2009). Quantum communication developed by the properties of quantum mechanics like Heisenberg principles (Chang, 2017), entanglement, quantum teleportation (Lu *et al*., 2017), super dense coding (Dong *et al*., 2009), and No cloning theorem (Wootters and Zurek, 1982). The evolution of quantum key distribution from quantum phenomenon comes to the rescue to avoid the threats caused by a quantum computer. Many QKD protocols have been developed from the initial protocol, like BB84 (polarization) (Bennett, 1992; Bruß, 1998; Bennett and Brassard, 2020) and Ekret91 (Entanglement) (Ekert, 1991; Stucki *et al*., 2005; Chou *et al*., 2014; Abushgra and Elleithy, 2015). QKD protocol security depends on randomness; therefore, a Quantum Random Number Generator (QRNG) (Stipčević *et al*., 2014) provides true randomness compared to classical pseudo-random numbers. In the last decades, exponential progress takes place in the field of quantum cryptography. Many new QKD protocols developed with different real-time scenarios. The practical implementation of QKD devices faces problems in generating and measuring quantum states, but adversaries have control over devices. Therefore, the Device Independent QKD protocol (DIQKD) (Acín *et al*., 2007) was developed similarly to Ekert (1991); Alice and Bob receive some unknown bell states, perform the random measurement and generate results to obtain keys.

To avoid side-channel attacks, Measurement Independent Quantum Key Distribution (MIQKD) (Xu *et al*., 2014) was developed. Since key distribution entirely takes place in a quantum approach, Semi Quantum Key Distribution (SQKD) (Boyer *et al*., 2007) was developed, where the server has quantum capabilities and the client has the classical capabilities.

Materials and Methods

The proposed work is completed using quantum circuit simulation and no material associated with the work proposed. And related to methods, bell pairs with entanglement swapping property is already discussed in the section bell states and entanglementa swapping.

The major issue in the QKD is the delayed measurement, the protocol has to store the qubit until the measurement basis exchange takes place in the classical channel:

$$\left|\psi^{+}\right\rangle_{12}\otimes\left|\psi^{+}\right\rangle_{34}=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right)_{12}\otimes\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right)_{34} \quad (1)$$

$$=\frac{1}{2}(|0_1 1_2 0_3 1_4>+|0_1 1_2 1_3 0_4>+|1_1 0_2 0_3 1_4>+|1_1 0_2 1_3 0_4>) \quad (2)$$

$$=\frac{1}{2}(|0_1 1_2 0_3 0_4>+|0_1 1_2 1_3 1_4>+|1_1 0_2 1_3 1_4>+|1_1 0_2 0_3 0_4>) \quad (3)$$

$$=\frac{1}{2\sqrt{2}}\left(\begin{array}{l}\left|0_1 1_2 0_3 0_4\right\rangle+\left|1_1 1_2 0_3 0_4\right\rangle+\left|0_1 1_2 1_3 1_4\right\rangle+\left|1_1 1_2 1_3 1_4\right\rangle+\\ \left|0_1 0_2 1_3 1_4\right\rangle-\left|1_1 0_2 1_3 1_4\right\rangle+\left|0_1 0_2 0_3 0_4\right\rangle-\left|1_1 0_2 0_3 0_4\right\rangle\end{array}\right) \quad (4)$$

$$=\frac{1}{4}\left(\begin{array}{l}\left|0_1 0_2 0_3 0_4\right\rangle-\left|0_1 1_2 0_3 0_4\right\rangle+\left|1_1 0_2 0_2 0_4\right\rangle-\left|1_1 1_2 0_3\right\rangle+\left|0_1 0_2 1_3 1_4\right\rangle\\ -\left|0_1 1_2 1_3 1_4\right\rangle+\left|1_1 0_2 1_3 1_4\right\rangle-\left|1_1 1_2 1_3 1_4\right\rangle+\left|0_1 0_2 1_3 1_4\right\rangle+\left|0_1 1_2 1_3 1_4\right\rangle\\ -\left|1_1 0_2 1_3 1_4\right\rangle-\left|1_1 1_2 1_3 1_4\right\rangle+\left|0_1 0_2 0_2 0_4\right\rangle+\left|0_1 1_2 0_3 0_4\right\rangle-\left|1_1 0_2 0_3 0_4\right\rangle+\left|1_1 1_2 0_3 0_4\right\rangle\end{array}\right) \quad (5)$$

$$=\frac{1}{2}\left(\left|0_1 0_2 0_3 0_4\right\rangle+\left|0_1 0_2 1_3 1_4\right\rangle-\left|1_1 1_2 0_3 0_4\right\rangle-\left|1_1 1_2 1_3 1_4\right\rangle\right) \quad (6)$$

$$=\frac{1}{2}(|0_1 0_3>|0_2 0_4>+|0_1 1_3>|0_2 1_4>-|1_1 0>|1_2 0_4>-|1_1 1_3>|1_2 1_4>) \quad (7)$$

$$=\frac{1}{2}\left(\left|\phi^{+}\right\rangle_{13}\left|\phi^{+}\right\rangle_{24}+\left|\Psi^{+}\right\rangle_{13}\left|\Psi^{+}\right\rangle_{24}-\left|\phi^{-}\right\rangle_{13}\left|\phi^{-}\right\rangle_{24}-\left|\Psi^{-}\right\rangle_{13}\left|\Psi^{-}\right\rangle_{24}\right) \quad (8)$$

Many QKD protocol performs well by storing the qubit either by communicating with parties in theoretical research or failing in actual implementation. The first approach to solve the ultra-shortage in storage time of qubit, EQKD protocol was developed based on entangled and dense coding mechanism. The EQKD protocol requires the storage of the qubit in process, so the operability is low in development. MEQKD protocol (M-Mini) (Li *et al*., 2018) was extended based on EQKD where 4 classical bits are combined using bell states. GEQKD protocol (G-Group) (Li *et al*., 2021) provides full use of every group qubit instead of half group discarded in MEQKD protocol. The major problem faced in MEQKD and GEQKD protocol is the key generating rate and information gain by an adversary.

The Entanglement and superdense coding techniques are used for the proposed QKD to solve qubit's ultra-short storage time limitation. Since the proposed method uses the concept of "ping pong protocol" from Quantum Secure Direct Communication (QSDC) (Boström and Felbinger, 2002; Deng *et al*., 2003), therefore we restrict the generation of the random key instead of sending a meaningful message. An efficient quantum circuit design simulation for the protocol in the IBM Qiskit Composer and implements the protocol using IBM Qiskit Lab (IBM Quantum, 2021).

Bell States and Entangled Swapping

Generally, two qubits are entangled to form a bell state by applying a Hadamard and the CNOT gate leads to an inseparable state. Performing measurement in computational or diagonal bases will collapse the bell states into different classical bits compared to the original bits sent. Measurement of bell states using Bell States Measurement (BSM) will generate the same classical bits as initially sent. Various Pauli gates like {I, X, Z, Y} applied to bell states will transfer the bell states from one form to another without collapsing it, as shown in Table 1. Classical information can be transferred from one party to another using the superdense coding concept (Nielsen and Chuang, 2010).

Let suppose take group of four classical bits {0, 1, 0, 1}, generation of bell states in the position {(1,2), (3,4)} will give the resulted bell states as $\{|\Psi^{+}>_{12}, |\Psi^{+}>_{34}\}$. Similarly, the bell states for position {(1,3), (2,4)} and {(1,4), (2,3)} will lead to $\{|\Phi^{+}>_{13}|\Psi^{+}>_{24}\}$ and $\{|\Psi^{+}>_{14}|\Phi^{+}>_{23}\}$ respectively. Measurement of bell states using BSM in the same position leads to the generation of the same classical bits but measurement in different positions generates ¼ probability for getting the same classical bits as in Eq. 8.

One of the attractive properties of measuring two bell states in different BSM locations leads to entanglement swapping (Sarvaghad-Moghaddam, 2019; Ji *et al*., 2022). Let's generate two bell states from position {(1, 2), (3, 4)} as stated in Eq. 1 and perform the tensor product of two bell states as shown in Eq. 2. Measure the bell states using BSM from position {(1, 3), (2, 4)}, therefore apply CNOT gate for qubits 1 and 2 as control bit and qubit 3 and 4 as target bit as shown in Eq. 3. Apply Hadamard operation on qubit 1 and qubit 2, cancel the phase difference state and add the same phase state as shown in Eqs. 4-6. Perform the essential swapping operation by joining the qubit {(1, 3), (2, 4)} together and a pair of 4 new bell states created in Eqs. 7-8, respectively. A new property has evolved in entangle swapping whenever a different position is applied during BSM, which leads to the same difference as sent by the original bell states. If two bell states differ by a value, that value will remain the same even after measurement in different positions, as shown in Table 2.

Table 1: Bell states and its unitary transformation

Classical bits	Bell states	Explanation-classical form	I (00)	X (01)	Z (10)	Y (11)
{0} 00	$\left\|\Phi^+\right\rangle$	$\frac{1}{\sqrt{2}}\left(\left\|00\right\rangle+\left\|11\right\rangle\right)$	$\left\|\Phi^+\right\rangle(00)$	$\left\|\psi^+\right\rangle(01)$	$\left\|\Phi^-\right\rangle(10)$	$\left\|\psi^-\right\rangle(11)$
{1}01	$\left\|\psi^+\right\rangle$	$\frac{1}{\sqrt{2}}\left(\left\|01\right\rangle+\left\|10\right\rangle\right)$	$\left\|\psi^+\right\rangle$ (01)	$\left\|\Phi^+\right\rangle(00)$	$\left\|\psi^-\right\rangle(11)$	$\left\|\Phi^-\right\rangle(10)$
{2}10	$\left\|\Phi^-\right\rangle$	$\frac{1}{\sqrt{2}}\left(\left\|01\right\rangle-\left\|10\right\rangle\right)$	$\left\|\Phi^-\right\rangle(10)$	$\left\|\psi^-\right\rangle(11)$	$\left\|\Phi^+\right\rangle(00)$	$\left\|\psi^+\right\rangle(01)$
{3}11	$\left\|\psi^-\right\rangle$	$\frac{1}{\sqrt{2}}\left(\left\|01\right\rangle-\left\|10\right\rangle\right)$	$\left\|\psi^-\right\rangle(11)$	$\left\|\Phi^-\right\rangle(10)$	$\left\|\psi^+\right\rangle(01)$	$\left\|\Phi^+\right\rangle(00)$

Table 2: Bell states measurement on different position

The difference in bell states position	Entanglement swapping leads to the same difference in bell states after measurement in a different position			
Zero $\left\|\Phi^+\right\rangle_{12}\left\|\Phi^+\right\rangle_{34}$	$\left\|\Phi^+\right\rangle_{13}\left\|\Phi^+\right\rangle_{24}$	$\left\|\Psi^+\right\rangle_{13}\left\|\Psi^+\right\rangle_{24}$	$\left\|\Psi^-\right\rangle_{13}\left\|\Psi^-\right\rangle_{24}$	$\left\|\Phi^-\right\rangle_{13}\left\|\Phi^-\right\rangle_{24}$
One $\left\|\Phi^+\right\rangle_{12}\left\|\Psi^+\right\rangle_{34}$	$\left\|\Phi+\right\rangle_{13}\left\|\Psi^+\right\rangle_{24}$	$\left\|\Psi^+\right\rangle_{13}\left\|\Phi^+\right\rangle_{24}$	$\left\|\Phi^-\right\rangle_{13}\left\|\Psi^-\right\rangle_{24}$	$\left\|\Psi^-\right\rangle_{13}\left\|\Phi^-\right\rangle_{24}$
Two $\left\|\Phi^+\right\rangle_{12}\left\|\Phi^-\right\rangle_{34}$	$\left\|\Phi^+\right\rangle_{13}\left\|\Phi^-\right\rangle_{24}$	$\left\|\Phi^-\right\rangle_{13}\left\|\Phi^+\right\rangle_{24}$	$\left\|\Psi^+\right\rangle_{13}\left\|\Psi^-\right\rangle_{24}$	$\left\|\Psi^-\right\rangle_{13}\left\|\Psi^+\right\rangle_{24}$
Three $\left\|\Phi^+\right\rangle_{12}\left\|\Psi^-\right\rangle_{34}$	$\left\|\Phi^+\right\rangle_{13}\left\|\Psi^-\right\rangle_{24}$	$\left\|\Psi^-\right\rangle_{13}\left\|\Phi^+\right\rangle_{24}$	$\left\|\Phi^-\right\rangle_{13}\left\|\Psi^+\right\rangle_{24}$	$\left\|\Psi^+\right\rangle_{13}\left\|\Phi^-\right\rangle_{24}$

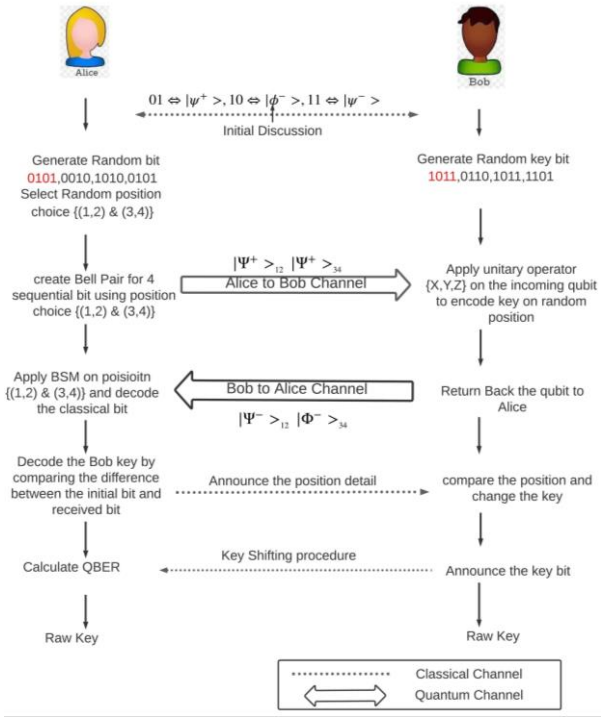

Fig. 1: Proposed protocol working model

The Proposed Protocol

In this protocol, we proposed an effective quantum key distribution based on bell states and the property of Entanglement swapping. The working model of the proposed protocol was shown in Fig. 1.

Initial Procedure

Alice and Bob agree that each of the four bell states can carry two classical bits of information and encode {00 -|Φ^+>,01-|Ψ^+>, 10-|Φ^->, 11-|Ψ^->}. Alice and Bob Agree on the position information {(1,2) and (3,4)} or {(1,3) and (2,4)} or {(1,4) and (2,3)}.

Quantum Procedure

Step 1: Alice generates '*n*' random classical bits and forms a group of 4 classical bits in sequential order
Step 2: Alice picks each group and generates the two bell pairs randomly in any one of the position orders mentioned above and stores the entanglement pair detail and position information of the bell pair
Step 3: Alice sent the generated two bell pairs to Bob
Step 4: Bob applies some unitary operation to encode the key {*X-01, Y-11-, Z-10*} randomly on the incoming qubit and returns it to Alice. Bob stores the unitary information and qubit position information where quantum gates are applied
Step 5: Alice performs the Bell State Measurement (BSM) on the position which she used to generate bell pair and generates the key by calculating the difference between the sent and received bit
Step 6 : Repeat: From step 2 to step 5 until '*n*' classical bits complete

Classical Procedure

Step 1: Alice publishes the position information to Bob
Step 2: Bob generates the key information by using the applied unitary operation {*X=01, Y=11, Z=10*} for every group
Step 3: If Bob's position matches Alice's position, Bob changes its key information by applying the XOR

operation between the used unitary gates and append with the 'I' gate for that particular group. Otherwise, the key remains the same

Key Shifting Procedure (n/2)

Step 1: Alice randomly chooses some group bits and asks Bob to send the key information and generate the QBER

Step 2: Compare the QBER with a threshold value (Shor and Preskill, 2000); if it succeeds, generate the raw key, or else abort the protocol

Step 3: Obtaining the final raw key will further undergo post-processing steps like privacy amplification to generate a finite key length

Alice generates the two EPR pairs for every classical bit in each group by randomly selecting a position and transmitting it to Bob for unitary transformation. Bob randomly selects the position and applies the unitary transformation {'X', 'Y', 'Z'} send back to Alice. Alice will communicate the position detail applied in each group; Bob will alter the key information based on the position information in the classical part. If Alice's position matches Bob's position choice, Bob will apply the XOR operation on the key and append it with the 'I' unitary gates or keep the previously generated key. Compared to the GEQKD protocol, the proposed protocol uses 3 positions choices whereas the existing protocol uses two positions choice for every group transmission.

Results

Security of Proposed Protocol

Intercept measure and Resend attack (IR) is one of the critical categories in the family of an individual attack. IR attacks the incoming bell states from Alice by applying BSM and creates the new bell states transfer to Bob. Again, strikes the incoming bell states from Bob, who used unitary transformation to fetch the needed essential information between both parties. Eve performs an attack twice to fetch the key information, first from Alice to the Bob channel and second from Bob to the Alice channel.

Adversary on the Right Choice

Eve has no information about the bell states position information; therefore, Eve guesses any one of the positions {{(1,2), (3,4)} or {(1,3), (2,4)} or {(1,4), (2,3)}}. If Eve is lucky enough to get the right guess about Alice's position information while applying for BSM, she creates the same bell states as generated by Alice. After the encoding operation done by Bob, Eve applies the same IR attack using the same BSM position to fetch the key information from Bob. Eve will not be detected since it used Bell states position information as Alice, as shown in the first two rows in Table 3. Eve has the probability of a 1/3 chance of getting the same position choice compared to the existing protocol has a 1/2 chance.

Adversary on the Wrong Choice

If Eve is unlucky in getting the Alice position choice, Eve is applying BSM on a qubit of different bell pairs leading to entanglement swapping. The two new qubits will be entangled to form another bell state and have ¼ chance to obtain the same bell states as Alice generated. If all three parties have different position choices, then the eve chance of getting the key information is 100% to Bob, but the detection rate is 75% of being caught, as shown in the 5th row in Table 4. If Alice's choice is similar to Bob's or Eve's choice is similar to Bob, then the probability of obtaining the key information is 0% for Eve, but Eve's detection rate is 75%, as shown in the 3rd and 4th row of Table 4. Eve has the probability of 2/3rd choosing a different position and 3/4th the possibility of being caught during communication.

Two parties are communicated based on three position choices. They have a 100% chance to generate the secret key for secure communication compared with the BB84 protocol has a 50% probability as no third-party adversary is involved in it. Since GEQKD protocol uses the concept of ping-pong methods, therefore a large number of bits are used to detect the presence of an adversary rather than generating the key. The detection probability of Eve during its involvement in communication will be identified by the mismatch between Alice's and Bob's positions.

Let's see, with an example, suppose Alice generates 100 groups with 400 random bits and sends them to Bob, if Eve attacks all togroups,1/3rd $\left\{\frac{1}{9}+\frac{2}{9}=\frac{3}{9}\right\}$ of the time, Eve will cause the same position information as Alice and its detection rate will be null. 2/3rd $\left(\frac{2}{9}+\frac{2}{9}+\frac{2}{9}=\frac{6}{9}\right)$ of the time, Eve will lead to wrong position choice compared with either Alice or Bob. During key shifting phases, Alice's key will match Bob's key in ¼, which means the incorrect key matching leads to the identification of Eve in communication in one group is D_{group} = (1-1/4) =3/4. If Eve performs IR Attack in the entire communication channel, then the total detection rate will be D_{tot}= $\frac{2}{3}*\frac{3}{4}=\frac{1}{2}$ (50%) as in Table 5. In the presence of Eve, during the communication of N groups, out of which $\frac{1}{9}+\frac{2}{9}+\frac{1}{18}+\frac{1}{18}+\frac{1}{18}=\frac{1}{2}$ (N) to groups of Bob key will matches with the Alice key which leads to 50% of identical keys. The key rate generated by the Eve is, $\frac{1}{9}+\frac{2}{9}+\frac{2}{9}+\frac{5}{9}$ (N) the Eve key matches with Bob's key is approximately 55%. If Eve performs an IR attack on all the groups, there is a 50% chance of detection which leads to aborting the protocol and trying with the next iteration.

Table 3: Key exchange without Eve interference

	Bob {same position}				Bob {different position}			
Number of classical bits	1	2	3	4	1	2	3	4
Alice random bit	1	0	1	1	1	0	1	1
Alice sending bell states {(1,2) and (3,4)}	$\|\Phi^+\rangle_{12}$		$\|\Psi^-\rangle_{34}$		$\|\Phi^+\rangle_{12}$		$\|\Psi^-\rangle_{34}$	
Bob apply unitary operation {X, Y->01,11}	X_1 and Y_2				X_1 and Y_3			
Alice performs BSM in same position {(1,2) and (3,4)}	$\|\Phi^+\rangle_{12}$		$\|\Psi^-\rangle_{34}$		$\|\Psi^-\rangle_{12}$		$\|\Phi^+\rangle_{34}$	
Alice generated key	1	0	0	0	0	1	1	1
Publish Alice location	{(1,2), (3,4)}				{(1,2), (3,4)}			
Bob altering key	Bob applying X and Y on same EPR pair (1,2) X⊕Y->01⊕11=10(Z) {No change in (3,4) (I)}				Bob applying X and Y on different EPR pair {No change}			
Bob Key	1	0	0	0	0	1	1	1

Table 4: Key exchange with Eve interference

No	Position choice/ probability	Alice choice	Eve choice (Alice->Bob)	Bob choice	Eve detection (Bob->Alice)	Eve key	Alice detection	Bob key
1	A=B=E (1/9)	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	X_1, Y_2	$\|\Phi^-\rangle_{12}\|\Phi^+\rangle_{34}$	10, 00	$\|\Phi^-\rangle_{12}\|\Phi^+\rangle_{34}$	Same(X1⊕Y2), I, 10, 00
2	A=E, E≠B (2/9)	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	X_1, Y_3	$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{24}$	01, 11	$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{24}$	01, 11
3	A≠E, A=B (2/9)	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	$\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}$	X_1, Y_2	$\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}$	01, 11	$\|\Psi^+\rangle_{12}\|\Psi^-\rangle_{34}$	Same(X_1⊕Y_2), I, 10, 00
			$\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}$		$\|\Phi^+\rangle_{12}\|\Phi^-\rangle_{34}$	
			$\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}$		$\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{34}$	
			$\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24}$		$\|\Phi^-\rangle_{13}\|\Phi+\rangle_{34}$		$\|\Phi^-\rangle_{12}\|\Phi+\rangle_{34}$	
4	A≠E, B=E (2/9)	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	$\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}$	X_1, Y_3	$\|\Phi^-\rangle_{13}\|\Phi+\rangle_{24}$	10, 00	$\|\Psi^+\rangle_{12}\|\Psi^-\rangle_{34}$	01, 11
			$\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{24}$		$\|\Phi^+\rangle_{12}\|\Phi^-\rangle_{34}$	
			$\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}$		$\|\Phi^+\rangle_{12}\|\Phi^-\rangle_{24}$		$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{34}$	
			$\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Phi^-\rangle_{13}\|\Phi+\rangle_{24}$		$\|\Phi^-\rangle_{12}\|\Phi+\rangle_{34}$	
5	A≠B≠E (2/9)	$\|\Phi^+\rangle_{12}\|\Phi^+\rangle_{34}$	$\|\Phi^+\rangle_{13}\|\Phi^+\rangle_{24}$	X_1, Y_4	$\|\Psi^+\rangle_{13}\|\Psi^-\rangle_{24}$	01, 11	$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{34}$	01,11
			$\|\Psi^+\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Phi^+\rangle_{13}\|\Phi^-\rangle_{24}$		$\|\Phi^+\rangle_{12}\|\Phi^-\rangle_{34}$	
			$\|\Phi^-\rangle_{13}\|\Phi^-\rangle_{24}$		$\|\Psi^-\rangle_{13}\|\Psi^+\rangle_{24}$		$\|\Psi^-\rangle_{12}\|\Psi^+\rangle_{24}$	
			$\|\Psi^-\rangle_{13}\|\Psi^-\rangle_{24}$		$\|\Phi^-\rangle_{13}\|\Phi+\rangle_{24}$		$\|\Phi^-\rangle_{12}\|\Phi+\rangle_{34}$	

Table 5: Comparative analysis of different protocol

Protocol	Eve presence in key	No of bits in key shifting process	Key generating rate %
BB84 (Bennett and Brassard, 2020)	0.750	72	25
MEQKD (Li *et al*., 2018)	0.625	41	25
GEQKD (Li *et al*., 2021)	0.625	40	25
Proposed	0.550	32	50

If Eve attacks every group, it will get caught during the shifting process and authenticated parties abort the keys. Eve adopted a random way of attacking the transmitted bell states with some random probability of *M* group out of N to groups then $f = \frac{M}{N}$ states. The mutual information between Alice and Bob will be increased compared with Eve's complete involvement will be $\frac{N}{2}$ to $\frac{N}{2} + \left\{\frac{N}{2} * \frac{M}{N}\right\} = \frac{N+M}{2}$ groups. The mutual information between Eve and Bob will be decreased from $\frac{5N}{9}$ to $\frac{5N}{9} to \frac{5N}{N} * \frac{M}{N} = \frac{5M}{9}$. The Eve detection rate to check the presence of Alice and Bob also reduced from $\frac{1}{2}$ to $\frac{1}{2} * \frac{N}{M}$.

Suppose Eve attacks randomly M = 50 groups compared with N = 100; then the detection rate will be around 25% compared to 50%. The key generation rate between Alice and Bob increased to 75% compared to 50% and Eve's key generating rate decreased from 55-27% drastically. The communicating parties should decide whether to abort or continue with the key based on the QEBR, but no involvement of an adversary leads to a 100% key rate.

A quantum communication channel suffers from noise due to Bit flip and Phase error known as Quantum Bit Error Rate (QBER). During N group transfer, X% of N to groups suffer from noise leading to an increased QBER to a certain threshold, which helps decide whether to use generated key or abort it. The QBER will be set to 11% compared with the BB84 protocol as a base threshold for secure communication (Shor and Preskill, 2000). Alice and Bob announce a few 'n/2' generated keys in the public channel to verify the adversary's presence and remove the announcing bit from the remaining generated key. The probability of finding disagreement and identifying Eve's presence for our proposed protocol is given in Eq. 9.

$$P_d = 1 - \left(\frac{5}{9}\right)^n \tag{9}$$

To detect an eavesdropper with a probability of 0.99999999, Alice and Bob need to compare n = 32 bits for the proposed protocol while the other protocols need more bits, as shown in Table 5.

Discussion

Quantum Circuit Simulation of Proposed Protocol

Due to quantum attacks, QKD has been used theoretically and studied widely to replace public key cryptography (RSA) and symmetric key exchange (Diffie-hellman). A basic protocol like BB84 and Ekret91 has been implemented experimentally and security proof has been given in a real-time environment. Quantum mechanics operations like unitary transformation and measurement can be visualized through quantum circuits, practically realizing QKD protocol experimentally. All unitary transformation operations like {pauli-x, Pauli-y, pauli-z} can be implemented {X, Y, Z} using Quantum circuit gates. Superposition and Entanglement states can be implemented using H and CNOT gates using quantum circuits. The proposed protocol is implemented using the IBM Qiskit tool, which provides two major tools Quantum Composer and Quantum Lab (IBM Quantum, 2021). Quantum composer helps us build, visualize and run the protocol in simulated and real hardware through a cloud. Quantum Lab helps us execute the Python code in a jupyter notebook and provide space to store and run the protocol in the cloud. This study does not raise any ethical issues.

Key Generation without Adversary During Implementation

Initially, Alice chose four classical bits as four-photon/qubits for each group: A classical bit ‘0’ as $|0\rangle$ horizontally polarized qubit and a classical bit ‘1’ as $|1\rangle$ vertically polarized qubit. Alice chose four classical bits as “1110” as a group and converting into polarized form $\{|1\rangle,|1\rangle,|1\rangle,|0\rangle\}$. The initial state of quantum is $|0\rangle$ state for all four photons, then convert it to $|1\rangle$ by applying X gate based on the classical message. Alice randomly chooses position information {(1,2), (3,4)} or {(1,3), (2,4)} or {(1,4), (2,3)} to produce the bell states. Alice needs to perform Hadamard (H) followed by Controlled-Not (CNOT) gates based on the position information to generate the bell states. Once Bob obtains the Photon, he applies the unitary operation {X, Y, Z} on the position {(1,2) or (1,3) or (1,4)}. Once Alice receives the photon, she undergoes Bell States Measurement (BSM) by applying a CNOT gate followed by an H gate to obtain the information. Alice applies the XOR operation between sent and received qubits to generate the key created by Bob for each group.

If Alice and Bob choose different locations, Bob applies the two unitary operations on two different bell pairs; therefore, Alice will decode the correct key generated by Bob, as shown in Fig 2. If Alice and Bob choose the same position, then the two Unitary operations are applied on the same bell pair; therefore, Bob will apply XOR between the bell pair and append the remaining with the 'I' gate during the generation on Bob key. Without interference from Eve, Alice's key will match with Bob's key, as shown in Fig 3. In Existing protocols like BB84 and GEQKD the key generating rate is reduced to 50% due to wrong basis selection. Compared with the existing protocol, the proposed protocol generated a key length similar to the actual photon sent on average as shown in Fig 4.

Key Generation with Adversary During Implementation

Fig. 7 gives the IBM quantum composer for implementing the proposed protocol under Eve’s Attack, all three parties selecting the same position {(1,2), (3,4)}. Eve chose the correct position compared to Alice but mismatched with the Bob position, as shown in Fig. 8. Suppose Alice, Bob, and Eve have chosen different positions. In that case, Bob generated key matching with Eve, but 1/4 probability for Alice to generate the key and ¾ probability for Alice to detect the presence of Eve, as shown in Fig. 9. If Alice and Bob have the same position but Eve has a different position, then Bob will alter the key's information during the public announcement by Alice, as shown in Fig. 10. Eve and Bob have the same position information, but Alice has a different position choice, then bob applies the unitary operation on the same bell states.

DOI: 10.3844/jcssp.2023.1160.1169

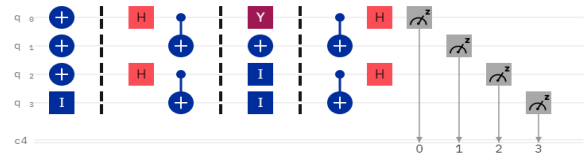

Fig. 2: Alice and Bob have a different position

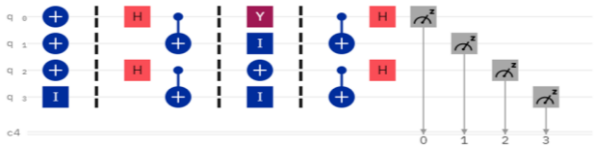

Fig. 3: Alice and Bob have the same position

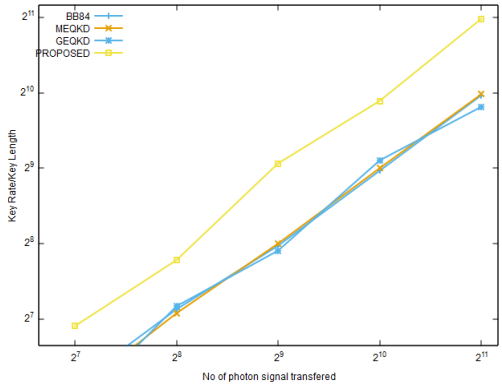

Fig. 4: Key generating rate comparison between existing and proposed protocol without EVE interference

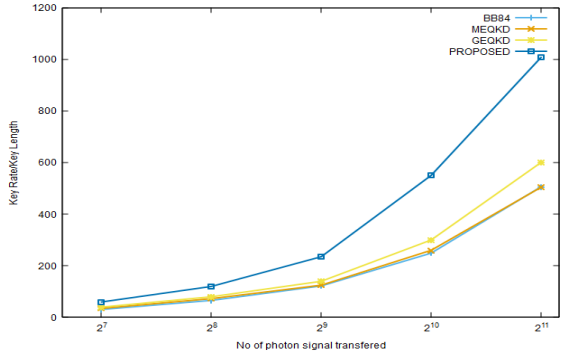

Fig. 5: Key generating rate comparison between existing and proposed protocol with EVE interference

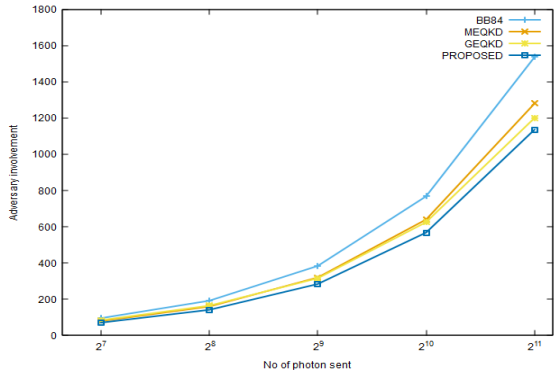

Fig. 6: Adversary Information gain between existing and proposed protocol

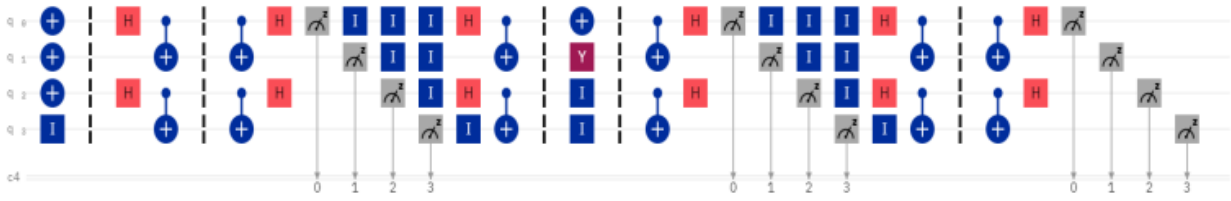

Fig. 7: Alice Bob and Eve have the same position choice

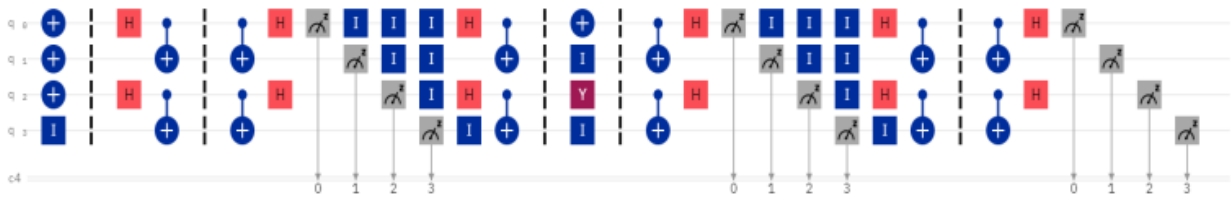

Fig. 8: Alice and Eve have the same position choice but Bob choice is different

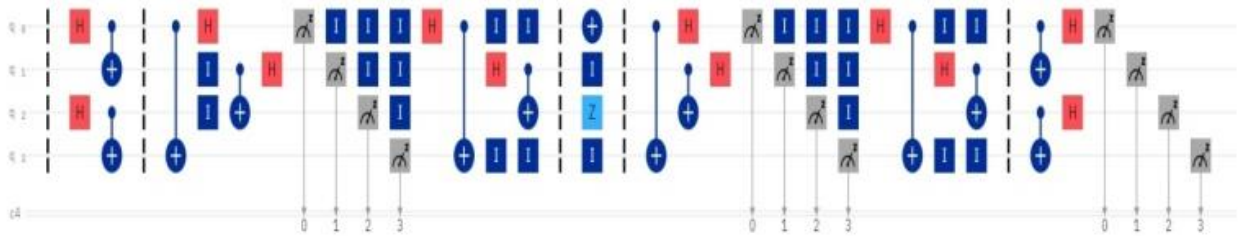

Fig. 9: Alice, Bob, and Eve have different position choice

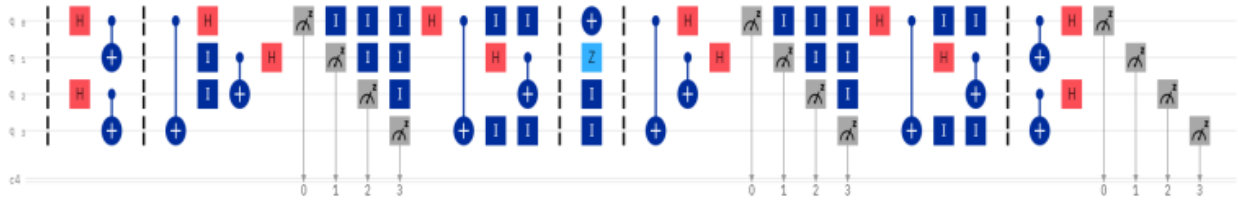

Fig. 10: Alice and Bob have the same position choice but Eve's choice is different

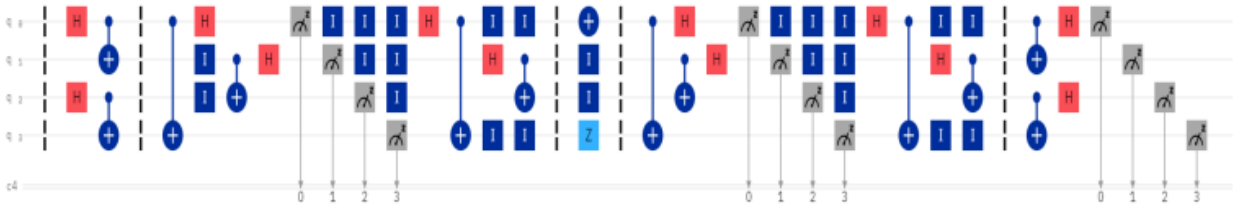

Fig. 11: Eve and Bob have the same position choice but Alice's choice is different

The key generated by Bob will be different for Eve, $1/4^{th}$ chance of remaining the same for Alice, as shown in Fig. 11. Compared with the Existing protocol, the proposed protocol yields a high key rate while Eve's involvement during communication as shown in Fig. 5. Eve obtains key knowledge is less compared with BB84, GEQKD and MEQKD as shown in Fig. 6.

Conclusion

A novel QKD protocol is proposed using entanglement and random position choice, and security is analyzed, which gives the protocol Quas-secure. The proposed QKD protocol for generating the raw key can use secure communication as key exchange instead of two-way communication like the “ping pong” protocol. Results show that the security can be achievable and the qubit storage is not required during communication as in QSDC protocol. The involvement of a third party leads to entanglement swapping, which helps us detect its presence while attacking both the incoming bell states from Alice and Bob. The noisy quantum channels and the imperfect device were not considered during implementation. The proposed protocol is verified visually by IBM quantum composer and implemented in IBM Quantum Lab.

Future Work

Quantum key distribution plays an important role in secure communication between two trusted users. QKD can be further extended to multiple bell states like GHZ states, W states, and cluster states for higher-level communication using superdense coding. Various parameters like key generating rate, adversary information gain, and key length have been discussed. There are various other issues like how to use QKD for long-distance communication and how to distribute a key to the multi-user through a quantum approach. Quantum secure communication is not only limited to key distribution. Various research activities are taking place in Quantum Key Agreement (QKA), Quantum Identity Authentication (QIA), Quantum Secret Sharing (QSS), etc.

Acknowledgment

The authors like to thank the publisher for their support in the publication of this research article. We thank the editorial team in reviewing and editing our work by finding the insight in our article, and also thankful for the opportunity to contribute the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Devendar Rao Babu: Acquisition of data and analysis and interpretation of data and content written.

Ramkumar Jayaraman: Conception and design of the article, intellectual content generation, critically reviewed the article, Contribution in intellectual content ideation, and reviewed the article along with the coordination for publication.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved.

Conflicts of Interest

The authors declare they have no conflicts of interest to report regarding the present study.

References

Abushgra, A., & Elleithy, K. (2015, May). Initiated decoy states in quantum key distribution protocol by 3 ways channel. In *2015 Long Island Systems, Applications and Technology* (pp. 1-5). IEEE. https://doi.org/10.1109/LISAT.2015.7160178

Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., & Scarani, V. (2007). Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, *98*(23), 230501. https://doi.org/10.1103/PhysRevLett.98.230501

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, *68*(21), 3121. https://doi.org/10.1103/PhysRevLett.68.3121

Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*. https://doi.org/10.48550/arXiv.2003.06557

Boström, K., & Felbinger, T. (2002). Deterministic secure direct communication using entanglement. *Physical Review Letters*, *89*(18), 187902. https://doi.org/10.1103/PhysRevLett.89.187902

Boyer, M., Kenigsberg, D., & Mor, T. (2007, January). Quantum key distribution with classical Bob. In *2007 First International Conference on Quantum, Nano and Micro Technologies (ICQNM'07)* (pp. 10-10). IEEE. https://doi.org/10.1109/ICQNM.2007.18

Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, *81*(14), 3018. https://doi.org/10.1103/PhysRevLett.81.3018

Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S., & Bianchi, G. (2019). Quantum internet: Networking challenges in distributed quantum computing. *IEEE Network*, *34*(1), 137-143. https://doi.org/10.1109/MNET.001.1900092

Chang, D. C. (2017). Physical interpretation of Planck's constant based on the Maxwell theory. *Chinese Physics B*, *26*(4), 040301. https://doi.org/10.1088/1674-1056/26/4/040301

Chou, Y. H., Zeng, G. J., Lin, F. J., Chen, C. Y., & Chao, H. C. (2014). Quantum secure communication network protocol with entangled photons for mobile communications. *Mobile Networks and Applications*, *19*, 121-130. https://doi.org/10.1007/s11036-013-0454-y

Deng, F. G., Long, G. L., & Liu, X. S. (2003). Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A*, *68*(4), 042317. https://doi.org/10.1103/Phys RevA.68.042317

Dong, L., Dong, H. K., Xiu, X. M., Gao, Y. J., & Chi, F. (2009). Quantum secure direct communication using a six-qubit maximally entangled state with dense coding. *International Journal of Quantum Information*, *7*(03), 645-651. https://doi.org/10.1142/S021974990900533X

Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Physical Review Letters*, *67*(6), 661.https://doi.org/10.1103/PhysRevLett.67.661

Guo, Y., Xie, J., Li, J., & Lee, M. H. (2013). An arbitrated quantum signature scheme based on chaotic quantum encryption algorithm. *Journal of Modern Physics*, *4*(05), 83. https://www.scirp.org/html/34236.html

Hillery, M., Bužek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Physical Review A*, *59*(3), 1829.https://doi.org/10.1103/PhysRevA.59.1829

IBM Quantum. (2021). https://quantum-computing.ibm.com/

Ji, Z., Fan, P., & Zhang, H. (2022). Entanglement swapping for bell states and Greenberger Horne Zeilinger states in qubit systems. *Physica A: Statistical Mechanics and its Applications*, *585*, 126400. https://doi.org 10.1016/ j.physa.2021.126400

Li, J., Li, H., Wang, N., Li, C., Hou, Y., Chen, X., & Yang, Y. (2021). A quantum key distribution protocol based on the EPR Pairs and its simulation. *Mobile Networks and Applications*, *26*, 620-628. https://doi.org/10.1007/s11036-019-01408-2

Li, J., Li, N., Li, L. L., & Wang, T. (2018). Corrigendum: One Step Quantum Key Distribution Based on EPR Entanglement. *Scientific Reports*, *8*. https://doi.org/10.1038/srep47004

Lin, C. Y., Yang, C. W., & Hwang, T. (2015). Authenticated quantum dialogue based on bell states. *International Journal of Theoretical Physics*, *54*, 780-786.https://doi.org/10.1007/s10773-014-2269-4

Lu, Y., Hong-Yang, M., Chao, Z., Xiao-Lan, D., Jian-Cun, G., & Gui-Lu, L. (2017). Quantum communication scheme based on quantum teleportation. *Acta Physica Sinica*, *66*(19).

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge University Press. ISBN: 10-1139495488.

Sarvaghad-Moghaddam, M. (2019). Efficient controlled bidirectional quantum secure direct communication using entanglement swapping in a network. *arXiv preprint arXiv:1902.11188*. https://doi.org/10.48550/arXiv.1902.11188

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332. https://doi.org/10.1137/S0036144598347011

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, *85*(2), 441. https://doi.org/10.1103/PhysRevLett.85.441

Sierra-Sosa, D., Telahun, M., & Elmaghraby, A. (2020). TensorFlow quantum: Impacts of quantum state preparation on quantum machine learning performance. *IEEE Access*, *8*, 215246-215255. https://doi.org/10.1109/ACCESS. 2020.3040798

Stipčević, M., & Koç, Ç. K. (2014). True random number generators. In *Open Problems in Mathematics and Computational Science* (pp. 275-315). Cham: Springer International Publishing. https://doi.org/10.1007/ 978-3-319-10683-0_12

Stucki, D., Brunner, N., Gisin, N., Scarani, V., & Zbinden, H. (2005). Fast and simple one-way quantum key distribution. *Applied Physics Letters*, *87*(19). https://doi.org/10.1063/1.2126792

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802-803. https://doi.org/10.1038/299802a0

Wu, W., Zhang, H., Wang, H., Mao, S., Jia, J., & Liu, J. (2015). A public key cryptosystem based on data complexity under quantum environment. *Science China Information Sciences*, *58*, 1-11. https://doi.org/10.1007/s11432-015-5408-5

Xu, F., Curty, M., Qi, B., & Lo, H. K. (2014). Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, *21*(3), 148-158. https://doi.org/10.1109/JSTQE.2014.238146

Yang, Y. G., & Wen, Q. Y. (2009). An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *Journal of Physics A: Mathematical and Theoretical*, *42*(5), 055305. https://doi.org/10.1088/1751-8113/42/5/055305