Enhancing Fidelity of Quantum Cryptography using Maximally Entangled Qubits

Saiful Islam Salim*, Adnan Quaium†, Sriram Chellappan‡ and A. B. M. Alim Al Islam§
*†§Department of CSE, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
†Department of EEE, Ahsanullah University of Science and Technology, Dhaka, Bangladesh
‡Department of CSE, University of South Florida, Florida, USA
Email: *1018052067@grad.cse.buet.ac.bd, †adnan.eee@aust.edu, ‡sriramc@usf.edu, §alim_razi@cse.buet.ac.bd

Abstract—**Securing information transmission is critical today. However, with rapidly developing powerful quantum technologies, conventional cryptography techniques are becoming more prone to attacks each day. New techniques in the realm of quantum cryptography to preserve security against powerful attacks are slowly emerging. What is important though now is the fidelity of the cryptography, because security with massive processing power is not worth much if it is not correct. Focusing on this issue, we propose a method to enhance the fidelity of quantum cryptography using maximally entangled qubit pairs. For doing so, we created a graph state along a path consisting of all the qubits of *ibmqx4* and *ibmq_16_melbourne* respectively and we measure the strength of the entanglement using negativity measurement of the qubit pairs. Then, using the qubits with maximal entanglement, we send the modified encryption key to the receiver. The key is modified by permutation and superdense coding before transmission. The receiver reverts the process and gets the actual key. We carried out the complete experiment in the IBM Quantum Experience project. Our result shows a 15% to 20% higher fidelity of encryption and decryption than a random selection of qubits.**

Index Terms—**security, quantum cryptography, entanglement, fidelity**

I. Introduction

Information security has always been a critical component of digital communications, and the need for security is only increasing. Recent advances, such as quantum computers, threaten many existing public-key cryptography systems (RSA [1], [2], ElGamal [3], ECC [4], and so on). To resist the threats of quantum computing, new cryptosystems based on quantum technology, i.e., quantum cryptography, are already being explored. Quantum cryptography, a combination of quantum mechanics and classical cryptography, is an important branch of cryptography today. Although quantum cryptography is still in its infancy, its challenges to the security of conventional cryptosystems cannot be ignored. A more important concern in this regard is that the current state of quantum cryptography still falls behind in achieving high fidelity.

Therefore, in this paper, we focus on enhancing the fidelity of quantum cryptography using the maximally entangled qubits. Here, we create graph states consisting of all the qubits of *ibmqx4* and *ibmq_16_melbourne* and perform full quantum state tomography on all groups of 4 connected qubits on the path to produce highly entangled states. Then, we use the maximally entangled qubit pairs to transmit the encryption key to the receiver. The encrypted message is sent through a conventional communication channel. As a result, we are able to demonstrate higher fidelity of quantum cryptography than the classical approach of a random selection of qubits.

Based on our work, we make the following set of contributions in this paper:

- We propose a new technique of quantum encryption where the encryption key is transmitted to the receiver through the quantum channel, whereas, the encrypted message is transmitted through the conventional communication channel.
- We simulate the proposed technique in IBM Quantum Experience.
- We measure the fidelity of our proposed technique, which is 15% to 20% higher than the classical process of a random selection of qubits.

The rest of this paper is organized as follows. Section 2 introduces some related research studies about the fidelity of quantum cryptography. Section 3 discusses the background of quantum physics and quantum communication. Section 4 presents our proposed mechanism. Section 5 discusses the experimental setup of our research. Section 6 presents the results of our experiment. Finally, Section 7 concludes our paper.

II. Related Work

Researchers are actively investigating the design of components and systems involved in quantum cryptography today. A notable secure communication method, that implements a cryptographic protocol involving components of quantum mechanics, is Quantum Key Distribution (QKD) [5]. Mirhosseini et al., [6] investigated that relying on the polarization of light for encoding, QKD limits the amount of information that can be sent per photon as well as confined the error rates. They also showed that multilevel QKD systems based on spatial-mode encoding can be more resilient against eavesdropping attacks in addition to having an increased information capacity. Milicevic et al., [7] introduced a quasi-cyclic code construction for multi-edge codes, that is highly suitable for hardware-accelerated decoding on a graphics processing unit (GPU). Pirandola et al., [8] designed a coherent-state network protocol to achieve remarkably high key rates at metropolitan distances.

Cryptographers have been working on quantum-resistant algorithms and lattice-based cryptography [9]. However, the high computational complexity of these algorithms makes it challenging to implement lattice-based protocols on resource-constrained IoT devices. To address this challenge, Banerjee et al., [10] presented a lattice cryptography processor with configurable parameters, which results in a 124K-gate reduction in the system area. Liu et al., [11] efficiently implemented crypto-systems for 8 and 32-bit micro-controllers. Apart from that, Ottaviani et al., [12] have shown that super-additivity of two-way Gaussian quantum cryptography enhances security performance. Kabir et al. [13] proposed a new technique of encryption, called Supercrypt, which enhances the security level by a significant margin with the help of quantum computing as well as enhances data transmission rate through exploiting the notion of Superdense Coding.

Fidelity measures in various types of quantum states and operators are also explored by researchers. Gutoski et al., [14] introduced a definition of the fidelity function for multi-round quantum strategies, which is a generalization of the fidelity function for quantum states. They illustrate an operational interpretation of the strategy fidelity in the spirit of Uhlmann's Theorem and discuss its application to the security analysis of quantum protocols for interactive cryptographic tasks, such as bit-commitment and oblivious string transfer. Gyongyosi et al., [15] showed an effective method to compute the fidelity of quantum cloning based attacks in quantum cryptography using Delaunay tessellation.

As we see existing studies have focused on quantum cryptography and fidelity. However, enhancing the fidelity of quantum cryptography and related analysis is still in its infancy, and yet to be focused in the literature. This paper designs a solution to enhance the fidelity of quantum cryptography using maximally entangled qubit pairs.

III. Background of Quantum Cryptography

Quantum computing uses the principles of quantum physics to perform operations on data. In our proposed technique, a very important step is creating a full quantum entangled state. Therefore, we discuss a few necessary basics of quantum entanglement along with the quantum cryptography and fidelity in this section.

A. Quantum Computing

Quantum computing is based on quantum bit or qubit, an analogous concept of the bit. The computation mainly deals with quantum information. A qubit is different from a classical bit, which has a state of either 0 or 1. On the contrary, a qubit has a quantum state that can be a superposition of both the classical states (0 and 1) at the same time. This quantum state, also known as superposition state, is a linear combination of the classical states.

The quantum state can be expressed as: $|\psi\rangle = \alpha|0\rangle + \beta|0\rangle$, where α and β are probability amplitudes and both can be complex numbers in general. The two states $\alpha|0\rangle$ and $\alpha|1\rangle$ are called computational basis states and they form an orthonormal basis for computation in a vector space [16]. Utilizing the superposition states, the quantum computation can deal with a huge number of calculations simultaneously.

A quantum computer is a device that performs quantum computing. A quantum computer with 400 basic units (qubits) could, for example, simultaneously process more bits of information than the number of atoms in the universe [17]. Therefore large-scale quantum computers are theoretically able to rapidly solve certain problems than any classical computer.

As of 2020, the development of actual quantum computers is still in its infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. A small 20-qubit quantum computer has been developed and is available for experiments via the IBM Quantum Experience project [18]. D-Wave Systems has been developing its own version of a quantum computer that uses quantum annealing [19]. Our experiment was carried out in the IBM Quantum Experience.

B. Quantum Entanglement

Quantum entanglement of particles is a quantum mechanical phenomenon, that describes a relationship between their fundamental properties that cannot happen by chance even though the individual objects may be spatially separated [20]. Quantum entanglement occurs when particles such as photons, electrons, molecules, etc interact physically and then become separated. This interaction properly describes each resulting member of a pair by the same quantum mechanical state. This could refer to states, such as their momentum, position, or polarisation.

In the case of two entangled particles, if one is observed to be spin-up, the other one will always be observed to be spin down and vice versa. However, according to quantum mechanics, it is impossible to predict, which set of measurements will be observed.

For example, let Alice and Bob be two observers for system A and system B respectively. In the entangled state, if Alice measures the eigenbasis of A, there are two possible equally probable outcomes:

1) Alice measures 0, and the state of the system collapses to $|0\rangle_A \otimes |1\rangle_B$. So, any subsequent measurement performed by Bob will always return 1.
2) Alice measures 1, and the state of the system collapses to $|1\rangle_A \otimes |0\rangle_B$ and Bob's measurement will return 0 with certainty.

Thus, system B is altered depending on Alice's measurement on system A. This remains true, even if the systems A and B are spatially separated.

C. Quantum Cryptography

Quantum cryptography exploits quantum mechanical properties to perform cryptographic tasks. Quantum cryptography allows the completion of various cryptographic tasks, that are proven or conjectured to be impossible using only classical (i.e., non-quantum) computation [21]. It is a special method of securely communicating a private key, from one party to another for use in one-time pad encryption [22].

The correct selection of bases for measurement of qubits is fundamental to quantum cryptography. A sender encodes the one-time pads in strings of qubits by performing some quantum operations using particular bases and then sends it over a public quantum channel. Only the sender knows the actual bases of the performed quantum operations. Therefore the receiver cannot distinguish all original states of the qubits.

D. *Fidelity*

Fidelity is a measure of the distance between two quantum states. Fidelity can be explained by assessing how good the source or quantum state preparation is. This can be done by comparing the state of the measured value with the ideal value. Fidelity, denoted by F, is by definition $F \in [0, 1]$. Here, $F = 1$ means that two states are identical and $F = 0$ means they are as different as physically distinct possible.

If the objective is to create pairs of perfectly entangled particles, and if there are extra stray (non-entangled) photons that were measured in an ensemble of prepared bi-photons, then the ensemble average state will be different from the expected perfectly entangled bi-photon pairs. In this case, how close the result is to the perfectly entangled bi-photon pairs is given by fidelity F.

In quantum cryptography, fidelity measures the correctness of the information. Higher fidelity indicates more correctness of the information. Therefore, achieving high fidelity is of critical importance in quantum cryptography.

IV. Proposed Mechanism

Our proposed mechanism involves, creating a full field entangled state of qubits [23]. Then highly entangled states, namely the graph states [24] are produced using optimized low-depth circuits that are tailored to the universal gate set. We detect full entanglement of all the qubits, using an entanglement criterion based on reduced density matrices. Qubits are fully entangled in the sense that, the state involves all physical qubits and is inseparable to any fixed partition.

For a set of vertices V and a set of edges E, the graph state that corresponds to $G(V, E)$ is the unique common eigenvector (of eigenvalue 1) of the set of independent commuting operators,

$$K_a = X^a Z^{N_a} = X^a \prod_{b \in N_a} Z^b \tag{1}$$

where, X and Z denote the Pauli operators, the eigenvalues to K_a are $+1$ for all $a \in V$, and N_a denotes the set of neighbor vertices of a in G [25]. A n-qubit graph state can be prepared by the following steps:

1) Initialize the state to $|+\rangle^{\otimes n}$ by applying n Hadamard gates to $|0\rangle^{\otimes n}$
2) For every $(a, b) \in E$, apply a control-Z gate on qubits a and b; the order can be arbitrary

According to one of the most widely used criteria, partial transpose criterion [26]–[28], a bipartite state ρ_{AB} on the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is said to be separable if ρ_{AB} can be written as,

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \tag{2}$$

where, ρ_A^i and ρ_B^i are quantum states of the system A and B, respectively, with the positive weights p to be $p_i \geq 0$ and $\sum_i p_i = 1$. Otherwise ρ_{AB} is entangled. For a state ρ of a many-body system, for any fixed bipartition AB of the system, if ρ is entangled to the partition AB, then the entanglement of the many-body state ρ can also be examined via its subsystems. That is, if the subsystems are all entangled, the whole system must be also entangled.

To be more specific, consider a 4-qubit subsystem $\rho_{A,B,C,D}$ in an n qubit system -

$$\rho_{A,B,C,D} = \frac{1}{4}(I + Z_A X_B Z_C)(I + Z_B X_C Z_D). \tag{3}$$

Due to Eq. 3, for a ring graph state, each 4-qubit density matrix of neighboring four qubits, as illustrated in Fig. 1 is given by [23]

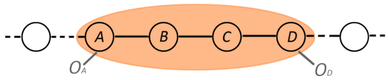


Fig. 1: A four-qubit subsystem that forms a chain [23]

Now, to calculate the negativity of the resulting 2-qubit subsystem, local operations of $O_A = \frac{Z_A+I}{2}$ and $O_D = \frac{Z_D+I}{2}$ need to be applied for each 4-qubit density matrix. For example, if (q_5, q_6, q_7, q_8) is chosen as our subsystem; after applying O_A and O_D to q_5 and q_8 respectively, q_5 and q_8 will be traced out, and the negativity of the remaining subsystem, (q_6, q_7) will be measured. The reason to choose $O_A = \frac{Z_A+I}{2}$ and $O_D = \frac{Z_D+I}{2}$ is discussed below.

If ρ is graph state, and the 4-qubit subsystem corresponds to 4 vertices that form a chain in the graph, then the resulting 2-qubit state is a maximally entangled state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|+\rangle + |1\rangle|-\rangle). \tag{4}$$

Now, two local operations O_A and O_D will be performed on qubit A and D respectively, and then, the reduced density matrix of qubit B and C is obtained by tracing out qubit A and D. The reduced density matrix for qubits B and C will be as follows [23]

$$\rho'_{B,C} = tr_{A,D}\left(\frac{O_A O_D \rho_{A,B,C,D} O_D^\dagger O_A^\dagger}{tr\left(O_A O_D \rho_{A,B,C,D} O_D^\dagger O_A^\dagger\right)}\right). \tag{5}$$

From this, the entanglement of $\rho'_{B,C}$ can be determined by using entanglement monotones such as negativity, which has non-zero values in the 2 qubit case, if and only if the system is entangled [26], [28]. Therefore if $\rho'_{B,C}$ is entangled, there is no separation with qubit B and C on different sides in the original system. This means, the qubit B and C must be on the same side for the original system to be biseparable concerning a fixed partition. The pair with maximum negativity is thus maximally entangled.

After measuring the negativity (entanglement), we perform the encryption and decryption, which is adopted from the Supercrypt protocol [13]. Fig. 2 depicts the whole process of Supercrypt protocol. The protocol improves both security and data transmission rate simultaneously as demonstrated in [13] through comparing with other available classical alternatives, and confirms significant performance improvements in terms of both the network performance and average throughput of the network.

The encryption process consists of the following steps,

- Alice (the sender) encodes the message with the key.
- She modifies the key using permutation.
- She applies the superdense coding for the key.
- She sends the encoded message through the *classical channel* and the superdense coded key through the *quantum channel*.

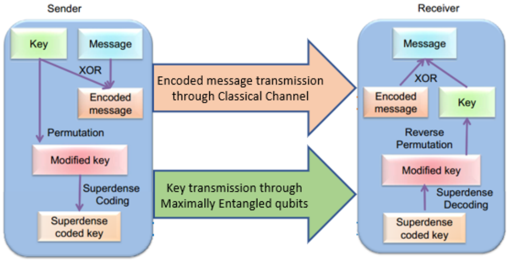
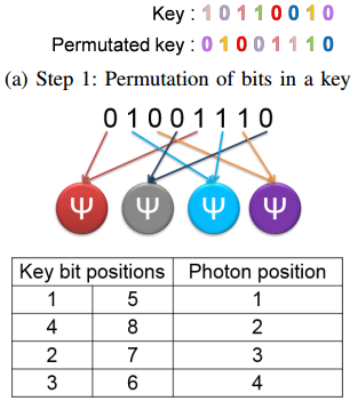


Fig. 2: Block diagram of Encryption-Decryption using Maximally Entangled Qubit pairs [13]



(a) Step 1: Permutation of bits in a key

Key bit positions		Photon position
1	5	1
4	8	2
2	7	3
3	6	4

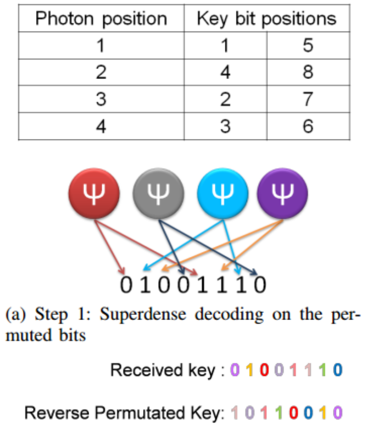
(b) Step 2: Superdense Coding on the permuted bits

Fig. 3: Encoding process in sender device [13]

In our proposed method, a sender needs to perform two operations to enhance the security of the transmitted key. First, a permutation operation is required on the bit sequence of the key. Second, the sender takes a pair of bits from the modified bit sequence and performs Superdense Coding on those. As a result, an n bit key is encoded in $n/2$ qubits. This encoding process is elaborated in Fig. 3.

The decryption process consists of the following steps,

- Bob (the receiver) receives the encoded message from the *classical channel* and the superdense coded key from the *quantum channel*.



Photon position	Key bit positions	
1	1	5
2	4	8
3	2	7
4	3	6

(a) Step 1: Superdense decoding on the permuted bits

Received key : 0 1 0 0 1 1 1 0
Reverse Permutated Key: 1 0 1 1 0 0 1 0

(b) Step 2: Re-permutation of bits in a key

Fig. 4: Decoding process in receiver device [13]

- He applies superdense decoding to the received key.
- He retrieves the modified key by applying reverse permutation.
- Finally he decodes the message using the key.

The decoding process confirms providing receiver an n bit key from $n = 2$ qubits. Subsequently, the sender performs the permutation as decided earlier and gets the original bit sequence. At the end of this phase, the sender gets the exact key or one-time pad to decrypt the message. This decoding process is elaborated in the Fig. 4.

V. Experimental Setup

The IBM Quantum experience is a quantum cloud service released by IBM, which has several quantum computing devices in the backend. A full field entangled state of 5 qubits and 14 qubits in two machines, named *ibmqx4* and *ibmq_16_melbourne* is created respectively. Then the graph states, that correspond to 2 rings involving 5 qubits from *ibmqx4* and 14 qubits from *ibmq_16_melbourne* is generated using optimized low-depth circuits that are tailored to the universal gate set. The qubit connectivity is given below,

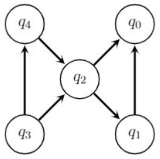


Fig. 5: Qubit topology of *ibmqx4* (5 qubits)

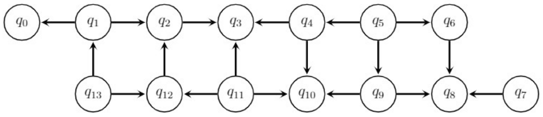
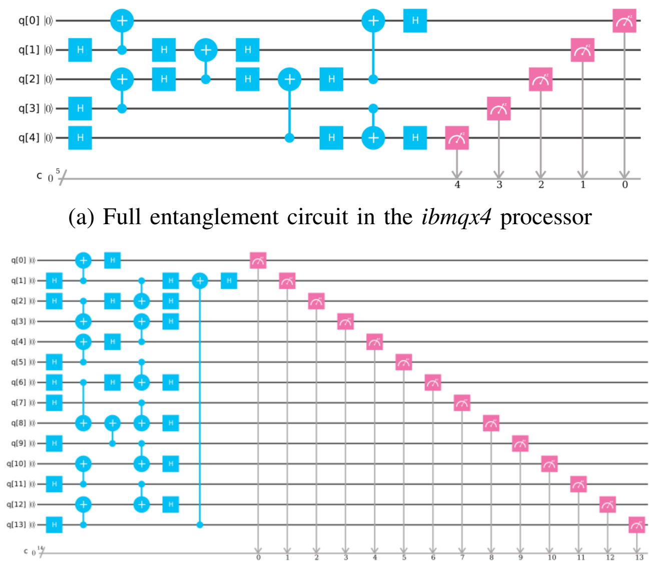


Fig. 6: Qubit topology of *ibmq_16_melbourne* (14 qubits)

Here, Fig. 7a and Fig. 7b show the circuit of the full entanglement that is implemented in *ibmqx4* and *ibmq_16_melbourne*.

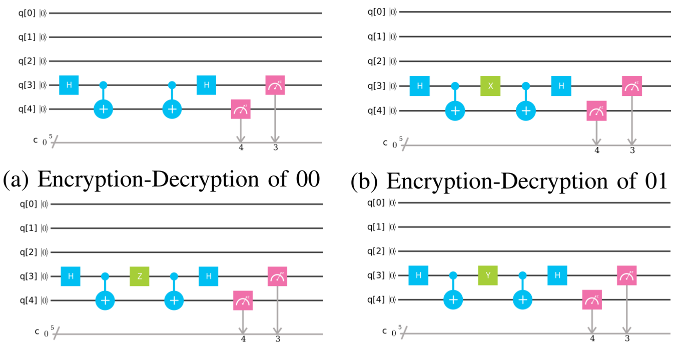


(a) Full entanglement circuit in the *ibmqx4* processor

(b) Full entanglement circuit in the *ibmq_16_melbourne* processor

Fig. 7: Full entanglement circuits used in our experiment

After measuring the entanglement for all the qubit pairs, the encryption and decryption process is implemented. In our experiment, two different devices to communicate with each other using encryption and decryption is not available. Therefore, an assumption is made that there is no information loss in data communication, and the encryption and decryption processes are implemented on the same device. And then, the fidelity for each predefined qubit pairs is checked. Implementation of the encryption and decryption of key in *ibmqx4* for qubit pair $(q3, q4)$ is shown in Fig. 8.



(a) Encryption-Decryption of 00

(b) Encryption-Decryption of 01

(c) Encryption-Decryption of 10

(d) Encryption-Decryption of 11

Fig. 8: Encryption and decryption for qubit pair $(q3, q4)$

VI. Experimental Results

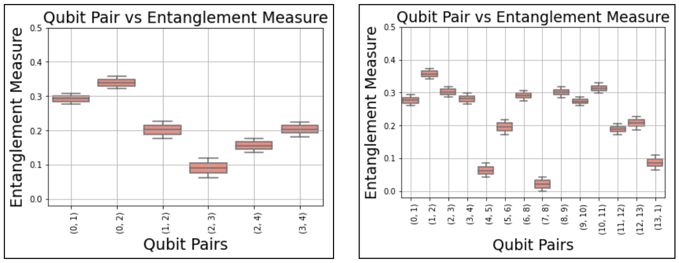
For *ibmqx4*, the measured qubit pairs were (q_0, q_1), (q_0, q_2), (q_1, q_2), (q_2, q_3), (q_2, q_4), (q_3, q_4) and for *ibmq_16_melbourne*, the measured qubit pairs were (q_0, q_1), (q_1, q_2), (q_2, q_3), (q_3, q_4), (q_4, q_5), (q_5, q_6), (q_6, q_8), (q_7, q_8), (q_8, q_9), (q_9, q_{10}), (q_{10}, q_{11}), (q_{11}, q_{12}), (q_{12}, q_{13}), (q_{13}, q_1).

In both quantum processors, the entanglement measure for each pair of qubits is calculated and the results are plotted in Fig. 9. The entanglement measure, i.e., Negativity, ranges between 0, and 0.5, where 0 indicates no entanglement and larger values indicate more entanglement [23], [29]. We found that, the magnitude of entanglement between pairs of qubits in the *ibmq_16_melbourne* processor surpasses the *ibmqx4* processor.

The fidelity for each pair of qubits for encryption and decryption in both quantum computers is measured. To determine the fidelity, total 20 measurements are conducted, where a total of 8192 shots were used for each measurement. The average fidelity of all the measurements is calculated, which are shown in Fig. 10. The fidelity ranges between 0 and 1.0, where 0 indicates the states of the qubits are completely different and 1.0 indicates the states are identical.

Now, Fig. 9a and Fig. 10a clearly indicate that, qubits with the higher entanglement show higher fidelity. The same is true for Fig. 9b and Fig. 10b. It is worth mentioning that, if the entanglement was not considered in this experiment, the average fidelity for a random selection of qubits would not be better.

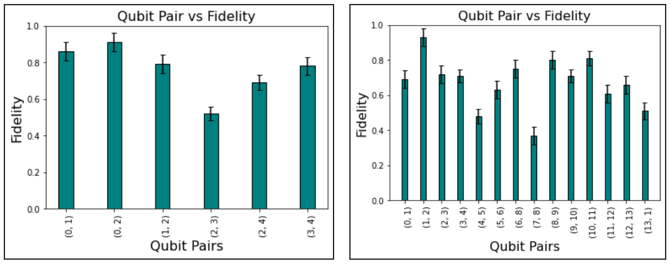
Considering the maximally entangled qubit pairs, we found the fidelity of the encryption and decryption process approximately 15% to 20% higher than the random selection of qubits. This result is shown in Fig. 11. It can also be observed from Fig. 11 that, the standard error of the fidelity is lower in case of the maximally entangled qubits, especially, in the *ibmqx4* processor. The maximally entangled fidelity of *ibmq_16_melbourne* processor is slightly higher than the *ibmqx4* processor.



(a) Entanglement measure in *ibmqx4* processor

(b) Entanglement measure in *ibmq_16_melbourne* processor

Fig. 9: Entanglement measure for each qubit pairs



(a) Qubit vs Fidelity in *ibmqx4* processor

(b) Qubit vs Fidelity in *ibmq_16_melbourne* processor

Fig. 10: Fidelity for each qubit pairs

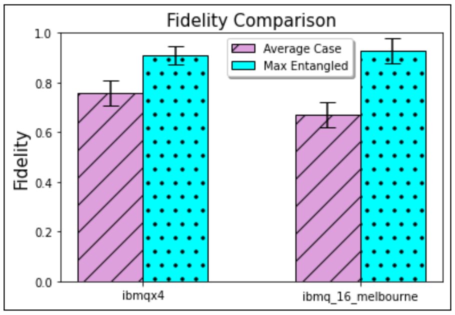


Fig. 11: Fidelity comparison between randomly selected qubits (average case) and maximally entangled qubits

VII. Conclusion and Future Work

Recent advancements in quantum computers pose significant risks to both conventional public-key and symmetric key algorithms. As a result, new encryption techniques that could offer more security becomes necessary. Here, the fidelity of resulting cryptography techniques is important to ensure correctness, and the current state here has room for improvement. In this paper, we enhanced the fidelity of quantum cryptography using the notion of maximally entangled qubit pairs to transmit the super dense key to the receiver. Our experiment shows that using maximally entangled qubits, the fidelity of cryptography significantly improves by up to 20% compared to the classical method of a random selection of qubits. We plan to implement our work for a higher number of qubits in two separate devices for encryption and decryption in the near future. Furthermore, we plan to conduct a detailed correctness analysis of our proposed methodology also.

Acknowledgment

This work was supported in part by US National Science Foundation (Grant # 1718071). Findings and conclusions are those of the authors alone, and do not reflect views of NSF.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, p. 120–126, 1978.

[2] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, “Anonymous and traceable group data sharing in cloud computing,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, p. 912–925, 2018.

[3] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, p. 469–472, 1985.

[4] Y.-M. Tseng, “An efficient two-party identity-based key exchange protocol,” *Informatica*, vol. 18, no. 1, p. 125–136, 2007.

[5] A. Broadbent and C. Schaffner, “Quantum cryptography beyond quantum key distribution,” *Designs Codes and Cryptography*, vol. 78, no. 1, p. 351–382, 2016. [Online]. Available: https://dx.doi.org/10.1007/s10623-015-0157-4

[6] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O’Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, “High-dimensional quantum cryptography with twisted light,” *New Journal of Physics*, vol. 17, no. 3, p. 33033, 2015. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/17/3/033033

[7] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, “Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography,” *npj Quantum Information*, vol. 4, no. 1, 2018. [Online]. Available: https://dx.doi.org/10.1038/s41534-018-0070-6

[8] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, “High-rate measurement-device-independent quantum cryptography,” *Nature Photonics*, vol. 9, no. 6, p. 397–402, 2015. [Online]. Available: https://dx.doi.org/10.1038/nphoton.2015.83

[9] I. Verbauwhede, J. Balasch, S. S. Roy, and A. Van Herrewege, “24.1 circuit challenges from cryptography,” in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, 2015, pp. 1–2.

[10] U. Banerjee, A. Pathak, and A. P. Chandrakasan, *2.3 An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things*, 2019.

[11] Z. Liu, K. R. Choo, and J. Grossschadl, “Securing edge devices in the post-quantum internet of things using lattice-based cryptography,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 158–162, 2018.

[12] C. Ottaviani and S. Pirandola, “General immunity and superadditivity of two-way gaussian quantum cryptography,” *Scientific Reports*, vol. 6, no. 1, p. 22225, 2016. [Online]. Available: https://dx.doi.org/10.1038/srep22225

[13] K. S. Kabir, T. Chakraborty, and A. B. M. Alim Al Islam, “Supercrypt: a technique for quantum cryptography through simultaneously improving both security level and data rate,” in *2016 International Conference on Networking Systems and Security (NSysS)*, 2016, pp. 1–9.

[14] G. Gutoski, A. Rosmanis, and J. Sikora, “Fidelity of quantum strategies with applications to cryptography,” *Quantum*, vol. 2, p. 89, 2018.

[15] L. Gyongyosi and S. Imre, “Fidelity analysis of quantum cloning based attacks in quantum cryptography,” in *2009 10th International Conference on Telecommunications*, 2009, pp. 221–227.

[16] G. P. Berman, R. Mainieri, V. I. Tsifrinovich, and G. D. Doolen, *Introduction to Quantum Computers*, ser. Introduction to Quantum Computers. World Scientific, 1998. [Online]. Available: https://books.google.com.bd/books?id=S5QJtSYW5LgC

[17] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and et al., “Heralded entanglement between solid-state qubits separated by three metres,” *Nature*, vol. 497, no. 7447, p. 86–90, 2013. [Online]. Available: https://dx.doi.org/10.1038/nature12016

[18] “IBM Quantum Experience,” https://quantum-computing.ibm.com/, [Online] [Accessed: 10-May-2020].

[19] “D-Wave Systems,” https://www.dwavesys.com/quantum-computing/, [Online] [Accessed: 10-May-2020].

[20] J. Wang, M. Landman, T. Sutter, and Z. Seblini, “Entanglement evolution in a heisenberg spin dimer,” *IEEE Transactions on Magnetics*, vol. 55, no. 12, pp. 1–3, 2019.

[21] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, p. 7–11, 2014. [Online]. Available: https://dx.doi.org/10.1016/j.tcs.2014.05.025

[22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. USA: Cambridge University Press, 2011.

[23] Y. Wang, Y. Li, Z.-q. Yin, and B. Zeng, “16-qubit ibm universal quantum computer can be fully entangled,” *npj Quantum Information*, vol. 4, no. 1, Sep 2018. [Online]. Available: http://dx.doi.org/10.1038/s41534-018-0095-x

[24] M. Hein, J. Eisert, and H. Briegel, “Multiparty entanglement in graph states,” *Phys. Rev. A*, vol. 69, p. 062311, 06 2004.

[25] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, “Entanglement in graph states and its applications,” 2006.

[26] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Rev. Mod. Phys.*, vol. 81, pp. 865–942, Jun 2009. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.81.865

[27] A. Peres, “Separability criterion for density matrices,” *Physical Review Letters*, vol. 77, no. 8, p. 1413–1415, Aug 1996. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.77.1413

[28] M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed states: necessary and sufficient conditions,” *Physics Letters A*, vol. 223, no. 1, pp. 1 – 8, 1996. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0375960196007062

[29] G. J. Mooney, C. D. Hill, and L. C. L. Hollenberg, “Entanglement in a 20-qubit superconducting quantum computer,” *Scientific Reports*, vol. 9, no. 1, 2019. [Online]. Available: https://dx.doi.org/10.1038/s41598-019-49805-7