Hindawi Publishing Corporation
Advances in High Energy Physics
Volume 2014, Article ID 104325, 5 pages
http://dx.doi.org/10.1155/2014/104325

Research Article

Novel Quantum Encryption Algorithm Based on Multiqubit Quantum Shift Register and Hill Cipher

Rifaat Zaidan Khalaf[1] **and Alharith Abdulkareem Abdullah**[2]

[1] *Department of Mathematics, Eastern Mediterranean University, Gazimağusa, North Cyprus, Mersin 10, Turkey*
[2] *Department of Computer Engineering, Eastern Mediterranean University, Gazimağusa, North Cyprus, Mersin 10, Turkey*

Correspondence should be addressed to Alharith Abdulkareem Abdullah; alharith_alkafije@yahoo.com

Received 17 July 2014; Accepted 3 November 2014; Published 24 November 2014

Academic Editor: Ming Liu

Based on a quantum shift register, a novel quantum block cryptographic algorithm that can be used to encrypt classical messages is proposed. The message is encoded and decoded by using a code generated by the quantum shift register. The security of this algorithm is analysed in detail. It is shown that, in the quantum block cryptographic algorithm, two keys can be used. One of them is the classical key that is used in the Hill cipher algorithm where Alice and Bob use the authenticated Diffie Hellman key exchange algorithm using the concept of digital signature for the authentication of the two communicating parties and so eliminate the man-in-the-middle attack. The other key is generated by the quantum shift register and used for the coding of the encryption message, where Alice and Bob share the key by using the *BB*84 protocol. The novel algorithm can prevent a quantum attack strategy as well as a classical attack strategy. The problem of key management is discussed and circuits for the encryption and the decryption are suggested.

1. Introduction

Cryptography is the science of protection of private information from unauthorized access, ensuring data integrity, authentication, and other related features. In order to succeed in achieving this goal, a cryptography algorithm is employed to produce a cryptogram which includes some additional information that finally determines which key is used. Classical cryptography is divided into two main types depending on the actions of the two conventional parties Alice and Bob. The first type is a symmetrical system with Alice and Bob using the same key. The second type, the asymmetrical system, is so named when Alice and Bob use a different key. The one-time-pad algorithm also belongs to classical cryptography [1]. Quantum cryptography is an emerging technology based on quantum mechanics and the phenomena and the properties of light. Quantum cryptography was developed in 1984 by the physicist Charles Henry Bennett when he developed what he claimed was an unconditionally secure quantum key distribution protocol called BB84 which guaranteed secure communication between parties who had not initially shared secret information [2]. The science is grounded in the uncertainty principle and was proven scientifically in 1992 [3]. Over the following years this science began to evolve rapidly and to have significant effects. Recently, a quantum encryption algorithm has been proposed but it has been noticed that the quantum encryption algorithm is very similar to the classical encryption algorithm with the crucial difference that the quantum algorithm is based on quantum laws whilst the classical algorithms are based on mathematical ones [4–7]. This development in the field of quantum computation may threaten and replace traditional encryption systems by utilizing algorithms such as Shor's quantum factoring algorithms, discrete algorithms, and Grover's algorithm. Thus, we should be looking to design new algorithms to resist the attacks against quantum algorithms whose contribution and progress in this field has become of significant importance and crucial necessity in the protection of information. Unlike classical algorithms, where Eve can be detected easily, the defining characteristics of quantum algorithms provide a much more secure system because the nonorthogonal quantum states protect the information from reliable detection. Unlike classical algorithms, where Eve can be detected easily, the defining characteristics of quantum algorithms provide a much more secure system because the nonorthogonal quantum states protect the information from reliable detection [8]. In other words, in practical terms an unconditionally secure algorithm is of far greater significance and value as a protection system of information than the classical algorithm approach wishing to achieve the same goal. Therefore, the quantum algorithms are the best candidates to provide for these needs. In this paper we will propose a novel and practical quantum block encryption algorithm based on a quantum shift register.

The planning of the paper is as follows. In Section 1, we briefly review classical cryptography and quantum cryptography. Section 2 discusses the quantum shift register and how to generate a matrix code used in the Diffie-Hellman algorithm to match the key between Alice and Bob to be used later in the Hill cipher algorithm [1] and then generate another matrix code used as a one-time pad (OTP). Section 3 is on a quantum encryption algorithm based on the quantum shift register where the encryption, decryption, and transmission of the proposed algorithm are discussed. In Section 4, the security and evaluation of the proposed algorithm are analysed. Finally, we give a brief conclusion in Section 5.

2. Quantum Shift Register

There are many applications of a quantum shift register. The shift registers are mainly used in coding theory, especially in quantum error correction and quantum convolution code [9–12]. This study focuses on the utilization of a quantum shift register to generate a matrix code used in the Diffie-Hellman algorithm to match the key between Alice and Bob in our proposed algorithm and then generate a matrix code used as one-time pad in the encryption of plaintext of our proposed algorithm as well.

2.1. Circuit of the Quantum Shift Register. The quantum shift register circuit is represented by a set of input qubits, memory qubits, a set of output qubits, and updated memory qubits. It feeds the memory back into the application for the next cycle and this concept is similar to the operation of a classical shift register. A quantum shift register circuit consists of swap gates, which can be quantum computationally represented using three CNOT gates as in Figure 1. The properties of CNOT are discussed in [13]. One possible physical realization of the quantum CNOT gate was presented by Linden et al. [14]. The quantum shift register circuit can shift all data qubits to the nearest qubit in a specific direction and apply applications like arithmetic calculation and bitwise operations on two quantum registers where these operations are very useful for quantum computers and quantum computation. The circuit of the quantum shift register is presented and considered in [11] in which shift and rotation operations on qubits are performed by swap gates and controlled swap gates.

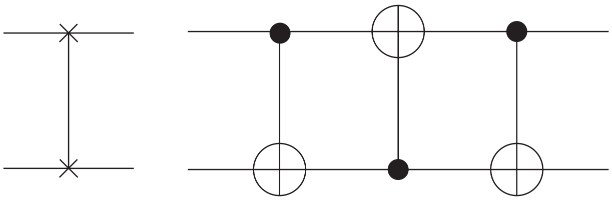


FIGURE 1: SWAP gate using CNOT gates.

2.2. Discussion of the Quantum Shift Register in the Proposed Algorithm. The quantum shift register has a number of positions. Each of these positions contains one qubit. In quantum register all qubits can be shifted one or more positions to the left or to the right. The length of the quantum shift register is determined by the number of qubits (states), the contents of each qubit are shifted to the next qubit in each pulse, and the outputs of the final qubit show a quantum feedback function and the resulting sequence from the quantum shift register is the content of the first qubit. This includes the following steps:

(i) quantum shift register,

(ii) quantum CNOT gate,

(iii) quantum feedback shift register.

The quantum shift register is the shift operation that depends on the swap gate. The shift is done between data and the process continues until the qubit repeats itself. The quantum CNOT gate acts on the connection states in the quantum register and chooses the connect state that achieves the maximum period. The quantum CNOT gate action on two or more qubits,where one or more qubits acts as a control. For instance, the CNOT operation acts on two qubits, and performs the NOT operation on the second qubit only when the first qubit is $|1\rangle$, and otherwise leave it unchanged, so the quantum CNOT of $|10\rangle$ became $|11\rangle$. Clearly the quantum linear feedback shift register is essential in building the quantum stream cipher algorithm. The quantum feedback shift register represents the outputs of the quantum CNOT function and is positioned in the final state (qubit) of quantum register.

In this study this example was taken to understand the mechanism, for instance, if we have a quantum shift register with length three and has initial value are $s_1 = a_1|0\rangle + b_1|1\rangle$, $s_2 = a_2|0\rangle + b_2|1\rangle$, $s_3 = a_3|0\rangle + b_3|1\rangle$, the function linking is between s_1 and s_2. The tensor product between states be:

$$\begin{aligned}|\psi\rangle &= |s_1\rangle \otimes |s_2\rangle \otimes |s_3\rangle \\ \psi &= |0_1 0_2 0_3\rangle + |0_1 0_2 1_3\rangle + |0_1 1_2 0_3\rangle \\ &\quad + |0_1 1_2 1_3\rangle + |1_1 0_2 0_3\rangle + |1_1 0_2 1_3\rangle \\ &\quad + |1_1 1_2 0_3\rangle + |1_1 1_2 1_3\rangle .\end{aligned} \tag{1}$$

The quantum linear feedback shift register was applied on the first state $|\psi\rangle$ and the computation compute as follows:

$$\begin{aligned}
\left|\mathrm{Shift}_1\right\rangle ={}& \mathrm{CNOT}\,(1,2)\left|0_1 0_2 0_3\right\rangle \cdot \mathrm{SWAP}\,(1,2)\left|0_1 0_2 0_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(2,3)\left|0_1 0_2 0_3\right\rangle + \mathrm{CNOT}\,(1,2)\left|0_1 0_2 1_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(1,2)\left|0_1 0_2 1_3\right\rangle \cdot \mathrm{SWAP}\,(2,3)\left|0_1 0_2 1_3\right\rangle \\
& + \mathrm{CNOT}\,(1,2)\left|0_1 1_2 0_3\right\rangle \cdot \mathrm{SWAP}\,(1,2)\left|0_1 1_2 0_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(2,3)\left|0_1 1_2 0_3\right\rangle + \mathrm{CNOT}\,(1,2)\left|0_1 1_2 1_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(1,2)\left|0_1 1_2 1_3\right\rangle \cdot \mathrm{SWAP}\,(2,3)\left|0_1 1_2 1_3\right\rangle \\
& + \mathrm{CNOT}\,(1,2)\left|1_1 0_2 0_3\right\rangle \cdot \mathrm{SWAP}\,(1,2)\left|1_1 0_2 0_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(2,3)\left|1_1 0_2 0_3\right\rangle + \mathrm{CNOT}\,(1,2)\left|1_1 0_2 1_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(1,2)\left|1_1 0_2 1_3\right\rangle \cdot \mathrm{SWAP}\,(2,3)\left|1_1 0_2 1_3\right\rangle \\
& + \mathrm{CNOT}\,(1,2)\left|1_1 1_2 0_3\right\rangle \cdot \mathrm{SWAP}\,(1,2)\left|1_1 1_2 0_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(2,3)\left|1_1 1_2 0_3\right\rangle + \mathrm{CNOT}\,(1,2)\left|1_1 1_2 1_3\right\rangle \\
& \cdot \mathrm{SWAP}\,(1,2)\left|1_1 1_2 1_3\right\rangle \cdot \mathrm{SWAP}\,(2,3)\left|1_1 1_2 1_3\right\rangle .
\end{aligned} \tag{2}$$

This then continues to the second shift using the same procedure and by taking the output of the first shift as input to the second shift. The accumulation at every stage of output proceeds in this way until it reaches the seventh and final shift. Therefore, each stage of the process is conducted and implemented in the same way. It is now possible to select any shift from those completed: for example, if shift $|\mathrm{Shift}_6\rangle$ is chosen, the corresponding matrix to this shift is called matrix A, where the rows for matrix A equal

$$\begin{aligned}
\left|g_0\right\rangle &= |10000000\rangle = 0, \\
\left|g_1\right\rangle &= |00100000\rangle = 1, \\
\left|g_2\right\rangle &= |00001000\rangle = 2, \\
\left|g_3\right\rangle &= |00000010\rangle = 3, \\
\left|g_4\right\rangle &= |00010000\rangle = 4, \\
\left|g_5\right\rangle &= |01000000\rangle = 5, \\
\left|g_6\right\rangle &= |00000001\rangle = 6, \\
\left|g_7\right\rangle &= |00000100\rangle = 7.
\end{aligned} \tag{3}$$

Now, from the above matrix A the matrix code can be generated by using the XOR operation between the rows of matrix A. The matrix code that was used in our proposed algorithm as a code for the matching key in the Diffie-Hellman concept once and one-time-pad matrix used to encode the plaintext once again. For example, if the above matrix A is used for desired $n = 3$ we can generate the matrix code as:

$$\begin{aligned}
\left|g_0\right\rangle &= |10000000\rangle\ , \\
\left|g_1\right\rangle &= |00100000\rangle\ , \\
\left|g_2\right\rangle &= |00001000\rangle\ , \\
\left|g_3\right\rangle &= |00000010\rangle\ ,
\end{aligned} \tag{4}$$

continuing to generate matrix code, where

$$\begin{aligned}
\left|g_0 \oplus g_1\right\rangle &= |10100000\rangle\ , \\
\left|g_0 \oplus g_1 \oplus g_2\right\rangle &= |10101000\rangle\ .
\end{aligned} \tag{5}$$

In similar way we can generate matrix code of any desired order and generate any number of codes from it.

3. Proposed Quantum Encryption Algorithm

The idea of our proposed algorithm is very straightforward. Before proceeding to talk about the algorithm itself, it should be noted that the conventional parties in the cryptography, Alice, Bob, and the meddler Eve, are used. Likewise, the algorithm is divided into the encryption, decryption, and transmission as follows.

3.1. Encryption Part. In the beginning, Alice computes word length from the plaintext and executes modulus 2 operation if she wants to encrypt plaintext with $(2 * 2)$ matrix in accordance with the Hill cipher algorithm [1]. If the result is 0 she sends the word length to Bob or else increments the word length by 1 to make the word length even and then sends it to Bob. Both Alice and Bob compute seven times the word length and generate the matrix A of the desired n depending on the result. For example, if the word length is 4, then $4 \times 7 = 28$. Thus, a matrix A of order 32 is generated which means the length of the quantum shift register is 5 qubits. She encrypts the plaintext by using the Hill cipher algorithm as follows:

$$\mathrm{EncryptPlaintext} = \mathrm{KeyMatrix}\,(2 * 2) \times \mathrm{PlaintextMatrix}. \tag{6}$$

Alice converts each encrypted plaintext character into its equivalent 7-bit ASCII representation. She uses the matrix of the quantum shift register again to generate one-time pad or the key, depending on her route of choice. This one-time pad serves as the symmetric key for the cryptographic process. For example,

$$g_1 \oplus g_{10} \oplus g_{15} \oplus g_{18} \oplus g_{55}. \tag{7}$$

Finally, she performs the XOR operation between the qubits of the encoded message and the one-time pad (key) to produce the quantum ciphertext.

3.2. Transmission Part. In this part, Alice and Bob have two keys they should be sharing. One of them is the classical key that is used in the Hill cipher algorithm where Alice and Bob use the authenticated Diffie-Hellman key exchange algorithm utilizing the idea of a digital signature in order to verify and confirm the identity of the two connecting parties and defend against a man-in-the-middle attack. For example, Alice generates the matrix A where the rows of the matrix are

$$\begin{aligned}
|g_0\rangle &= |10000000\rangle = |000\rangle = 0,\\
|g_1\rangle &= |00010000\rangle = |001\rangle = 1,\\
|g_2\rangle &= |01000000\rangle = |010\rangle = 2,\\
|g_3\rangle &= |00000100\rangle = |011\rangle = 3,\\
|g_4\rangle &= |00100000\rangle = |100\rangle = 4,\\
|g_5\rangle &= |00000010\rangle = |101\rangle = 5,\\
|g_6\rangle &= |00001000\rangle = |110\rangle = 6,\\
|g_7\rangle &= |00000001\rangle = |111\rangle = 7.
\end{aligned} \tag{8}$$

Alice, for instance, selects three random numbers:

$$\begin{aligned}
g_0 &= |10000000\rangle\,,\\
g_1 &= |00010000\rangle\,,\\
g_2 &= |01000000\rangle\,,\\
g_0 + g_1 + g_2 &= |11010000\rangle\,.
\end{aligned} \tag{9}$$

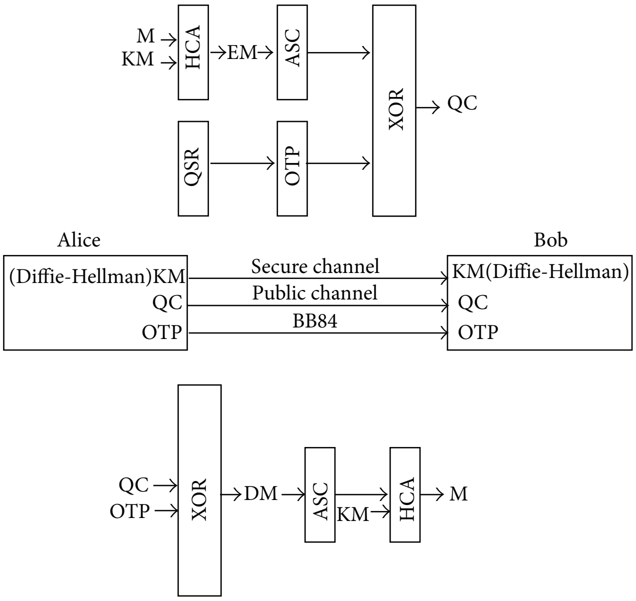
Now Alice has four numbers: $(g_0, g_1, g_2, g_0 + g_1 + g_2)$; Alice send to Bob three numbers and hides, for instance, g_2 number: $(g_0, g_1, g_0 + g_1 + g_2) = (|10000000\rangle, |00010000\rangle, |11010000\rangle)$; Bob selects a number called $g_3 = |00000100\rangle$; then he computes $g_0 + g_1 + g_3 = |10010100\rangle$ leading to $g_0 + g_1 + g_3$ and sends it to Alice.

The key for Alice is $g_0 + g_1 + g_3 + g_2 = |11010100\rangle$, The key for Bob is $g_0 + g_1 + g_2 + g_3 = |11010100\rangle$.

The above example explains the concept of Diffie-Hellman clearly in our approach. Now, suppose they exchange a secret key as 210. Then, both parties perform operation:

$$g_0 \oplus g_1 \oplus g_{10} \oplus g_{16} \oplus g_{56} \oplus g_{60} \oplus g_{210}. \tag{10}$$

The operation is performed by ignoring the values that do not exist in the generated matrix. The g_s represent the corresponding row numbers to be selected for the key creation. After the completion of the operation above, both parties generate the same bit sequence of 1s and 0s. Alice then informs Bob by sending a plaintext message where she indicates her choices, as in 1 as rectilinear and 0 as diagonal and so on. The other key or the one-time pad transmits to Bob by converting the key into binary bit string and again setting up a similar basis at both ends. Then the bits are transmitted across the secure channel where both parties set their basis according to previously generated bit sequences and the agreed-upon pattern for the representation of the bits. In turn, the bits are transmitted securely to Bob. This process is called deterministic one-step quantum key distribution using the *BB84* protocol. The key for the Hill cipher algorithm is again transmitted by Alice in a similar manner by converting the key into a binary bit string and again setting up a similar basis at both ends. After that, the bits are transmitted across the insecure channel securely.



M: message
KM: key matrix
HCA: Hill cipher algorithm
ASC: 7-bit ASCII representation
QSR: quantum shift register
OTP: one-time pad
XOR: exclusive-OR operation
EM: encode message
QC: quantum ciphertext
DM: decode message

Figure 2: Encryption, transmission, and decryption process.

3.3. Decryption Part. After the keys are received by Bob, he uses the one-time pad to decode the message. After that, Bob computes the inverse key of the Hill cipher and recovers the plaintext message in the original form. Figure 2 clarifies the representation of the proposed algorithm.

4. The Security and Evaluation of the Proposed Algorithm

It is known that, based on the algorithm of Bennett and Brassard [2], there are a lot of qubits that acquire distortion during the process of transmission because of the difference in the selection of bases between Alice and Bob. Therefore, in this proposal, Alice and Bob use the same basis during the transmission by reconciling on a common basis before they start transmitting the message which is based on quantum key distribution. This proves that our proposal is deterministic. In addition, this represents an enhancement of the feature of the Bennett and Brassard algorithm.

The scheme used in this study is a quantum linear feedback shift register to generate $2^n - 1$ of shifting. Each shift represents a matrix and this matrix contains binary bits. The Diffie-Hellman key exchange concept was also used between Alice and Bob in such a way that Eve does not possess all the keys between Alice and Bob. As a result, the ciphertext-only attack, the known-plaintext attack, and the chosen-plaintext attack are impossible. In classical cryptography, Eve can duplicate the ciphertext without modifying it through intercepting the channel or illegitimately accessing the ciphertext bank. This allows Eve to attempt to decrypt it time after time. However, using a quantum encryption algorithm, given a quantum ciphertext $|QC\rangle$, Eve cannot derive $|M\rangle$ without the information of the encrypted matrix and one-time pad (key). In addition to that, if Eve manages to obtain the encrypted matrix, she cannot manage to determine the bits message because, for each bit, the probability is bound by $1/2$. Supposing the length of the encrypted message block is n, the probability is bound by $1/2^n$, which is negligible.

Furthermore, if Eve manages to obtain the qubit, she cannot determine the bit M. For example, if she obtains $|0\rangle$ and knows each qubit, she is not able to determine M because there are two preimages, $|0 \oplus 0\rangle$ and $|1 \oplus 1\rangle$.

Likewise, from the encryption process of our algorithm, the known-plaintext and the chosen-plaintext attack are unfeasible because Eve could not know without the key what the ciphertext corresponding to the known-plaintext is. This property results from the uncertainty principle in quantum mechanics.

5. Conclusion

Quantum technology is new and being improved and sophisticated constantly, specifically in the field of quantum cryptography. it is an undisputed fact that the advances made in science and technology are one of the greatest challenges for the future and innovation in the field is advancing at an enormous pace and that, sooner or later, the quantum computers will assume a very significant role in this world. So it is not possible to treat or transfer all of the existing information in the classical form which is familiar to the people in quantum information and preshared classical keys as long as the security cannot be guaranteed. Therefore, it is proposed that a new algorithm encrypts the classical data using a classical encryption algorithm and transfers it by quantum data, where the classical encryption algorithm is represented by the Hill cipher algorithm and the quantum algorithm is represented by the quantum shift register. The security and the physical implementation of the proposed algorithm are analyzed in detail and it is concluded that the new proposed algorithm can prevent a quantum attack as well as a classical attack. Managing to prevent two kinds of attack and protecting the information from a new prying strategy is the goal. It should be mentioned that improvements can be made to the algorithm by future users in order to strengthen its capability and make it more effectively secure.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors would like to express their very great appreciation to Dr. Mustafa Riza for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Custom Computer Science, Prentice Hall, 5th edition, 2010.

[2] H. C. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, pp. 175–179, New York, NY, USA, 1984.

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[4] S. Dutta, A. Kumar, and N. C. Mahanti, "Network security based on quantum cryptography and multi qubit hadamard matrices," *Global Journal of Computer Science and Technology*, vol. 11, no. 12, 2011.

[5] Z. Cao and L. Liu, "Improvement of one quantum encryption scheme," in *Proceedings of the IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS '12)*, vol. 1, pp. 335–339, IEEE, 2012.

[6] R.-G. Zhou, Q. Wu, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," *International Journal of Theoretical Physics*, vol. 52, no. 6, pp. 1802–1817, 2013.

[7] T. Hua, J. Chen, D. Pei, W. Zhang, and N. Zhou, "Quantum image encryption algorithm based on image correlation decomposition," *International Journal of Theoretical Physics*, 2014.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[9] M. M. Wilde, "Quantum-shift-register circuits," *Physical Review A*, vol. 79, no. 6, Article ID 062325, 16 pages, 2009.

[10] J. H. Park, J. H. Kang, T. B. Jung et al., "Low error operation of a 4 stage single flux quantum shift register built with Y-Ba-Cu-O bicrystal Josephson junctions," *IEEE Transactions on Applied Superconductivity*, vol. 11, no. 1, pp. 625–628, 2001.

[11] J.-W. Lee, E. K. Lee, J. Kim, and S. Lee, "Quantum shift register," http://arxiv.org/abs/quant-ph/0112107.

[12] M. Grassl and T. Beth, "Cyclic quantum error-correcting codes and quantum shift registers," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 456, no. 2003, pp. 2689–2706, 2000.

[13] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, "Conditional quantum dynamics and logic gates," *Physical Review Letters*, vol. 74, no. 20, pp. 4083–4086, 1995.

[14] N. Linden, E. Kupče, and R. Freeman, "NMR quantum logic gates for homonuclear spin systems," *Chemical Physics Letters*, vol. 311, no. 3-4, pp. 321–327, 1999.