Noise Deduction using Quantum Check Bits

T. Godhavari
Research Scholar, Sathyabama University,
Associate Professor,ECE Dept,
Dr.M.G.R Educational and Research Institute.

N. R. Alamelu
Principal, Aarupadai Veedu Institute of Technology
Chennai.

ABSTRACT
With the advent of efficient quantum algorithms and technological advances, design of quantum circuits has gained importance. In this paper, Quantum circuit using standard quantum gates is constructed for the transmission of quantum encrypted check bits. The proposed scheme is analogous to the first QKD (quantum key distribution) protocol, (BB84) where the check bits are used to detect the level of noise and evesdropping on the channel. The gates used in this work are easily realizable and the encoding and decoding of classical information bits is extended for multiple bits using dense coding scheme.

Keywords
Quantum algorithms, Hamming code, check bits, encryption

1. INTRODUCTION
Quantum computing is one of the emerging/explored research area at the moment and yields faster solutions for complex problems. However, building quantum circuits is a challenging task. Without the ability to fully build physical quantum computers one must rely on quantum computer simulators and these are therefore at the centre of algorithm design and research. Qubit circuit simulation is at the forefront and qubit gates also have their benefits. Quantum computers evolve a coherent superposition of quantum states so that each of these states follow a distinct computational path until a final measurement is made at the output [11]. It is therefore certainly conceptually possible that at least for some problems, quantum computers could surpass the power of classical computers. The peculiar nature of the quantum de-coherence that leads to quantum errors mandates completion of all the quantum gate operations within a time bound, hence reduction in the gate count and the number of circuit levels leads to lowering the errors and the overall cost in quantum circuits. In this paper, we propose the design of gray code conversion circuits using CNOT gates and extend it for secured transmission of check bits. [6] The commonly used quantum gates along with its transfer matrix, symbol and function performed is described in table 1.

Table 1: Quantum Gates and its Transfer Matrix

Symbol	Name	Transfer Matrix	Symbol	Name	Transfer Matrix
H	Hadamard	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	θ	Rotation	$\begin{pmatrix}0 & 1\\ 1 & e^{i\theta}\end{pmatrix}$
X	Pauli X	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$		Controlled NOT	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$
Y	Pauli Y	$\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$	θ	Controlled Rotation	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{-j\theta}\end{pmatrix}$
Z	Pauli Z	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$		Swap	$\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}$
⊕	NOT	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$			

2. PROPERTIES OF TRANSFER MATRICES OF QUANTUM GATES
Property 1: Any 2x2 matrix can be represented as its linear combination under identity matrix I

$$a = \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix} = k0\ I + k1\sigma x + k2\sigma y + k3\sigma z$$
with ki $\in$ C $\quad \forall$ i = 0 to 3

$$\text{Where} \quad \alpha_x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

$$\alpha_y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$$

$$\alpha_z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

By expansion and equating the terms,

$K_0 = \frac{a11+a22}{2}$; $k_1 = \frac{a12+a21}{2}$; $k_2 = i\frac{a12-a21}{2}$; $k_3 = \frac{a11-a22}{2}$;

Property 2: A unitary operator preserves the distance and the rotation matrices 'R_r' are unitary
By definition:

$$R_x(\theta) = \begin{pmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$$

$$R_y(\theta) = \begin{pmatrix}\cos\frac{\theta}{2} & \sin\frac{\theta}{2}\\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}$$

$$R_y(\theta) = \begin{pmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{pmatrix}$$

It can be easily shown that

$$Rx\ (\theta)RxT(\theta) = Ry(\theta)RyT(\theta) = Rz(\theta)\ RzT\ (\theta) = I$$

Where $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

3. PREVIOUS RESEARCH

Stinson [1] discussed about secure transmission of information using classical bits. [5] It has reported that all quantum computations have to be unitary i.e. all quantum circuits can be evaluated in both directions. The first demonstration that a quantum computer can solve a specific problem more efficiently than a classical computer was provided by [9]. Mehrdaa S. Sharbaf [2] has proposed that Quantum key distribution protocols implementation is based on shifting, Error detection and Correction, Privacy amplification and Authentication processes. Justin Mullins [3] has focused that Satellites to communicate across thousands of kilometers using unbreakable codes whose security is provided by the law of quantum physics. Cederlof .J [4] has discussed that the sender will generate the random number. That is sent as a secret shared key. The unauthorized person cannot understand the random number. The secret key is also called as check bits

4. TYPICAL QUANTUM ENCODING SCHEMES

The bit can be encoded in the polarization state of a photon as given in table 2 and figure 1.

Table 2: Bit encoding in polarization states

BINARY	RECTILINEAR BASE	DIAGONAL BASE
ZERO	0^0 (or) 90^0	45^0 (or) 135^0
ONE	90^0 (or) 0^0	135^0(or)45^0

Alternately two classical bits (basis and data) are encoded to one quantum bit (q bit).The model of quantum computation is as strong as classical computation and more over there exists a small set of quantum gates that are universal [6,7]. An example transmission scheme using the above encoding scheme is illustrated in figure 2. (BB84 Scheme).

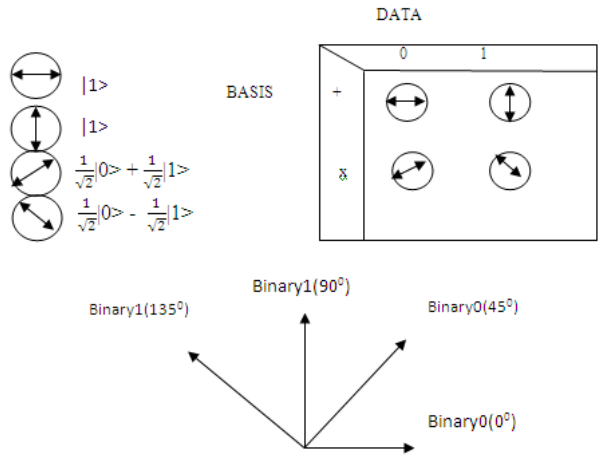
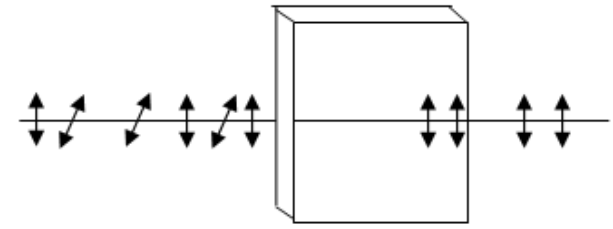


Figure 1 : Qubit encoding rectilinear and diagonal basis.

Quantum key distribution algorithm of Bennett and Brassard involves: (a) Photons prepared by Alice may have vertical/horizontal (VH) or diagonal polarization (DG). The photons with VH polarization may be used to transmit binary information as follows. A photon with vertical polarization may transmit 1 while one with horizontal polarization may transmit 0. Similarly photon with DG polarization may transmit binary information, 1 is encoded as photon with 45^0 polarizations and 0 encoded as a photon with 135^0 polarization. This is shown in figure 2.



Photon #	1	2	3	4	5	6	7	8	....
Alice >>>	VH	VH	DG	VH	VH	DG	DG	VH	....
Bob <<<	VH	DG	DG	VH	DG	VH	DG	DG	....
Match(Y/N)	Y	N	Y	Y	N	N	Y	N	....

Figure 2: BB84 Protocol.

5. STATE DETECTION USING GATES

The average value of an observable Q of quantum system in state $|\Psi>$ is given by

$$< Q \geq < \Psi|Q|\Psi >$$

$$where\ |\Psi> = \frac{|01> - |10>}{\sqrt{2}}$$

quantum system is in the entangled state. Let Z and X represent Quantum gates. Let the first qubit is sent to Alice and the second qubit is sent to Bob. Then the observables Q and R measured Alice on her qubit is Q=Z, and R=X_1 Similarly, the observables S and T measured by Bob is given by

$$S = -\frac{Z_2+X_2}{\sqrt{2}};\quad T = -\frac{-Z_2+X_2}{\sqrt{2}}$$

Where S and T are the output of two circuits, each using a combination of X and Y gates. Then the state detection using the above gates is given by

$$< QS > = < RS > = < RT > = \frac{1}{\sqrt{2}}$$

$$< QT > = -1/\sqrt{2}$$

6. SAMPLE QUANTUM CIRCUITS

6.1 Reversible Gray to Binary Code onverter

A gray code is a code assigning to each of a continuous set of integers, or to each member of a circular list, a word of symbols. These codes are also known as single-distance codes, reflecting

the Hamming distance of 1 between adjacent codes and there can be more than one gray code for a given word length. In modern digital communications, gray codes play an important role in error correction. The implementation of **Gray to Binary** code and **Binary to Gray** converter is shown in Figure 3&4.

6.1.1 Binary to Gray Code Convertor

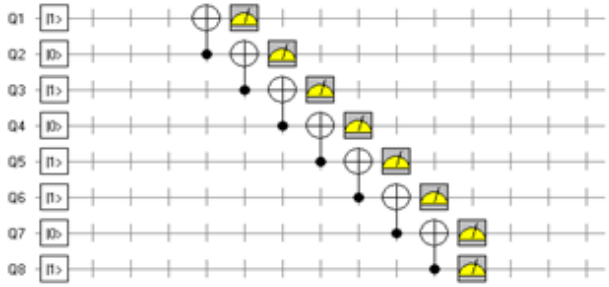


Figure 3a : Binary Value 10110101 given to Input circuit using C-NOT gates

Figure 3b: Gray Output value

6.1.2 Gray To Binary Code Convertor

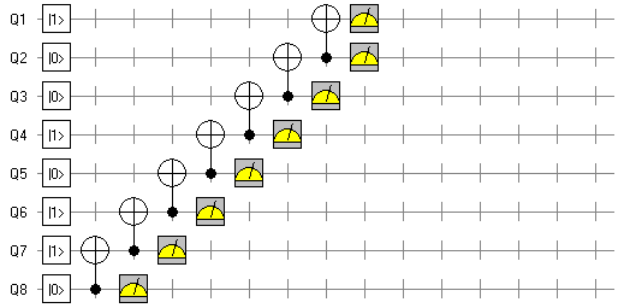


Figure 4a Encoded Gray value 01101001 given to Input of circuit

Figure 4b Decoded Binary Output value

7. QUANTUM ENCRYPTION MODEL

7.1 Information Encoding

Communication between a sender and a receiver involves a mapping called encoding, done at the sender's site and an inverse mapping called decoding, done at the receiver's site. A Check Bit is a binary digit used as part of a unit of information that is intended to indicate whether an error has occurred or not in the transmission or storage of the information. A bit added to an array of information bits at the originating device and used by the receiving device to check for errors that might have occurred during transmission. In communications, error checking refers to the use of Check Bits to check that data has been transmitted accurately. The Check Bit is added to every data unit that is transmitted. The Check Bit for each unit is set so that all bytes have either an odd number or an even number of set bits. For example, that two devices are communicating with even bit. As the transmitting device sends data, it counts the number of set bits in each group of bits. If the number of set bits is even, it sets the bit to 0; if the number of set bits is odd, it sets the bit to 1. In this way, every byte has an even number of set bits. On the receiving side, the device checks each byte to make sure that it has an even number of set bits. If it finds an odd number of set bits, the receiver knows there was an error occurred during transmission. The sender and receiver must both agree to use check bits and to agree on whether bit is to be odd or even. If the two sides are not configured with the same bit sense, communication will be impossible.

7.2 Quantum Encryption and Decryption

7.2.1 4 Bit Encryption circuit

Check bits are the most basic form of error detection in communications. Check bit is used not only in communications but also to test memory storage devices. For example, check bit performs a checking on memory every time a byte of data is read. Likewise, check bits are used in Quantum computing for secure transmission at both sender and receiver side. As classical bits, in this paper the quantum bits or qubits are used for error checking in the encoder and decoder circuits. The first QKD protocol, BB84 was proposed by Bennett and Brassard in 1984[13]. For secure date/key transmission, Alice and Bob perform several tests to determine the level of noise and eavesdropping on the channel. The set of 2n bits is split into two subsets of n bits each. One subset will be the check bits used to estimate the level of noise and eavesdropping, and the other consists of the data bits used for the quantum key. Figure 5.describes a 4bit quantum based check bit encryption circuit. The quantum encrypted check bit is transmitted in an interleaved manner with the key to be distributed.

Input = 0 1 1 0 Decimal number – 6

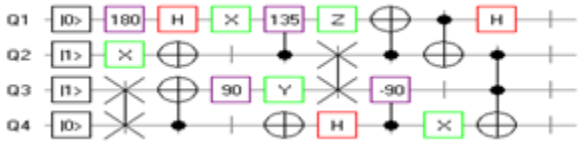


Figure 5a 4 Bit Encryption Circuit

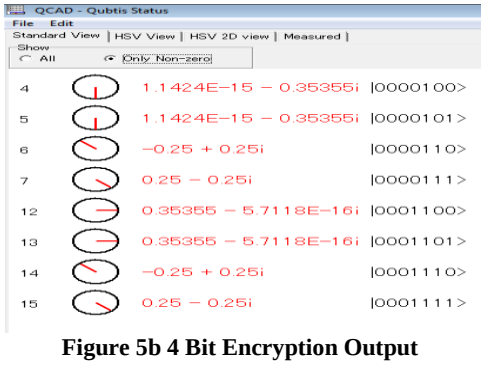


Figure 5b 4 Bit Encryption Output

7.2.2 4 Bit Decryption Circuit

The position of the check bits is known only to the friendly quantum check bits decryption circuit to be used at the receiver as shown in figure 6.

Input = 0 1 0 1 – 5 Output = 0 1 1 0 – 6

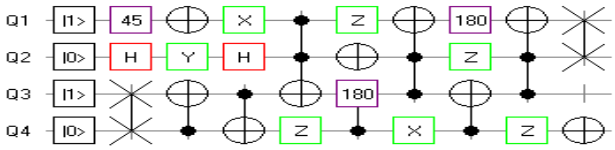


Figure 6a Decryption circuit

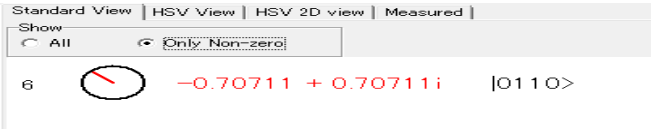


Figure 6b Decryption output (Pre-defined check bits)

7.3 SIMULATION RESULTS

7.3.1 *Eve's Detection*

The proposed circuit encrypts the pre defined check bit interleaved in the data. The size of check qubits is four and is encoded into eight different combinations. For all different four bit combination of input the same eight outputs are obtained but with different polarization. In the receiver side there are eight different software defined decryption circuits. If there is no eves dropping or de coherence due to noise any one of the decryption circuit will result in correct detection of pre defined check bits. The abilty of the proposed quantum circuit to detect one bit and two bit errors due to evesdropping is studied and results are shown in figure 7a to 7d.

7.3.2.1 *One bit error detection*

One bit error occurred due to the Eve's presence, so the output of the software defined decryption circuit is different from the pre defined check bits.

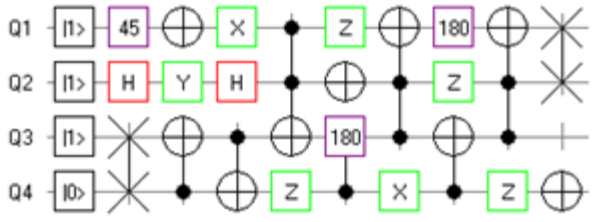


Figure 7a Q_2 Flipped [one bit error]

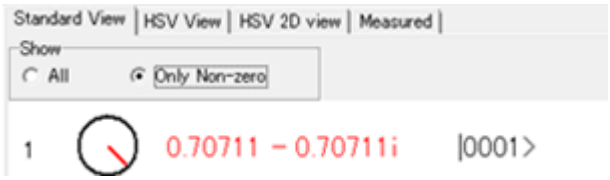


Figure 7b Decrypted output (Differ from Pre-defined check bits)

7.3.2.2. Two bit error detection

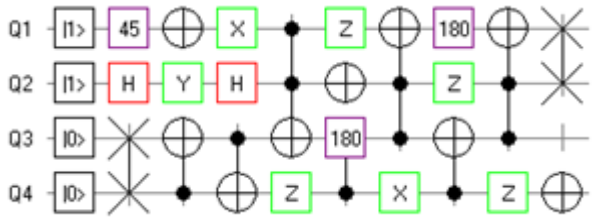


Figure 7c Q_2 & Q_3 – Flipped[Two bit error]

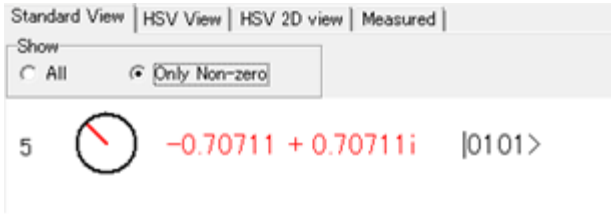


Figure 7d Decrypted output (Differ from Pre-defined check bits)

8. CONCLUSION

Coding is the process of transforming information during a communication process. The sender of a message encodes the message, and then transmits the encoded information over a classical communication channel. The recipient of the message decodes the encoded information. The question we address now is related to the advantage in exchanging quantum information. The peculiar property 'decoherence' of quantum signal / photon is utilized in our novel encoder and decoder to determine the level of noise and eves dropping on the channel.

9. REFERENCES

[1] Stinson, Douglas. R., "*Cryptography : Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

[2] Mehrdaa S.Sharbaf, "Quantum cryptography: A new Generation of Information Technology Security System," IEEE Sixth International Conference on Information Technology, Vol: 3, pp: 1644-1648, 2009.

[3] Justin Mullins, "Breaking Quantum cryptography in 150 kilometer," IEEE Transaction on Spectrum, Vol: 45, Issue: 9, pp: 15-15, September 2008.

[4] Cederlof J, Larson .A, "Security Aspects of the Authentication used in Quantum cryptography," IEEE Transaction on Information Theory, Vol: 54, Issue: 4, pp: 1735-1741, April 2008.

[5] Dan C.Marinesu,Gabrriela M.Marinesu,"*Approching Quantum Computing*" Pearson education,2009.

[6] Vishal Sahani,"*Quantum computing*" Tata McGraw Hill,Delhi.

[7] Vandersypen. L, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", Nature, 414, 883-887, Sep. 2011.

[8] Navleen Kaur, Amardeep Singh, "Enhancement of Network Security Techniques using quantum Cryptography", International Journal on Computer Science and Engineering, vol. 3, No. 5, May 2011

[9] Khalil shihab, " A Back propagation neural network for computer network security", Journal of computer science., 2006

[10] Deutsch, D, "Quantum theory, the church- Turing principle and the universal quantum computer" proceedings of the royal society of London A 400: 97-117, 1985

[11] Simon J. Gay, "Quantum Programming Languages: Survey and Bibliography," Math. struct. in Comp. Science2006.

[12] Tafliovich, A, "Quantum programming", Master's thesis, University Of Toronto, 2004