Success Probability Evaluation of Quantum Circuits based on Probabilistic CNOT-Gates

Amor Gueddana, Rihab Chatta and Noureddine Boudriga
Communication Network and Reserach Laboratory (CNAS), Engineering School of Communication of Tunis (SUP'COM), Ghazala Technopark, 2083, Ariana, Tunisia

Keywords: *CNOT*, C^kNOT, Abstract Probabilistic *CNOT*, Quantum *CNOT*-based Circuit.

Abstract: In this paper, we study the effect of non deterministic CNOT gates on the success probability of Quantum CNOT-based circuits. Based on physical implementation, we define an abstract probabilistic model of the CNOT gate that takes into consideration error sources and realizability constraints. Using the proposed model, we simulate a three-qubit quantum adder and show the evolution of the probability of realizing correctly the SUM operation depending on the success probability and errors of the CNOT gates.

1 INTRODUCTION

Controlled-NOT gates associated with single qubits operation are universal for building quantum circuits (Nakahara and Ohmi, 2008). Quantum *CNOT* gates based on linear optics still presents some conceptual and realization problems. It has been shown that the use of linear components doesn't permit to reach deterministic gates. Several works proposed non deterministic *CNOT* gate functioning at least with a success probability of 1/4. Some of these gates were physically realized and the expected result is quite consistent with theoretical modeling, this is due essentially to unexpected errors caused by the imperfection of linear components. We believe that studies concerning errors affecting the functioning of the CNOT gate is missing modeling.

Quantum circuits based on *CNOT* gates were simply treated in the ideal case where the gate works perfectly. All what has been said about the use of non deterministic gates is that the success probability of realizing a function will exponentially decrease depending on the number of gates used. To our knowledge, no detailed study were achieved to show the behavior of quantum circuit against non deterministic gates.

Our contribution in this work is three fold: first, we propose an error control model of an abstract probabilistic *CNOT* gate, while taking into consideration physical implementation constraints. Second, we identify errors affecting the success probability of the gate at the implementation level and we model errors related to the basic quantum linear components. Third, based on physical implementation of the TC.Ralph *CNOT* model, we define a set of *CNOT* gates having the form of an abstract *CNOT* gate that are physically realizable and extend our results to the probabilistic algorithms.

This paper is organized around five sections. Section 2 introduces the universality of *CNOT* gates and illustrates briefly several steps used to get *CNOT* decomposition of C^kNOT gate. In section 3, we present first a model of an abstract probabilistic *CNOT* gate and based on the TC.Ralph model, a subspace of realizable probabilistic gate is presented, second, we study the errors caused by linear components and model their effect at the implementation level. Section 4 presents in a first hand, a scheme for modeling probabilistic CNOT-based quantum circuits and in a second hand, the *CNOT* based three qubit Minimized Quantum Ripple Carry Adder is treated as a case study. Finally some numerical experimentation are illustrated.

2 QUANTUM CNOT-BASED CIRCUITS

2.1 Quantum C^kNOT Gate

In the general form, a single qubit quantum gate has a unitary 2×2 matrix representation denoted by u and having the following expression:

Gueddana A., Chatta R. and Boudriga N..
Success Probability Evaluation of Quantum Circuits based on Probabilistic CNOT-Gates.
DOI: 10.5220/0004058503780387
In *Proceedings of the International Conference on Data Communication Networking, e-Business and Optical Communication Systems* (OPTICS-2012), pages 378-387
ISBN: 978-989-8565-23-5

$$u = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \quad (1)$$

where u_{00}, u_{01}, u_{10} and $u_{11} \in \mathbb{C}$ and describing the amplitude probability of being in a specific quantum state (Figure 1a).

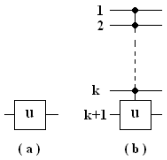


Figure 1: General form of a quantum gate.

We consider two major single qubit operations for building quantum circuits:

$$I_2 = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (2)$$

$$U_{NOT} = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (3)$$

A $C^k u$ gate, where $k \in \mathbb{N}_+^*$, is a gate acting on $(k+1)$ qubits. It inverts the state of the last qubit if all of the k qubits are set to $|1\rangle$, the k qubits left unchanged are the control qubits.

The matrix representation of $C^k u$ (Figure 1b) is denoted by $U_{C^k u}$ and obtained as follows:

$$U_{C^k u} = \begin{pmatrix} I_{2^{k+1}-2} & O \\ O & u \end{pmatrix} \quad (4)$$

Where $I_{2^{k+1}-2}$ is a $\left(2^{k+1}-2\right) \times \left(2^{k+1}-2\right)$ identity matrix.

For $u = NOT$, $C^k NOT$ gates are universal for building quantum circuits. For $k = 1$, the $C^1 NOT$ is called $controlled - NOT$ gate and denoted simply $CNOT$.

2.2 *CNOT* based Implementation of $C^k NOT$ Gate

In this paragraph, we focus our study on a detailed decomposition of the $C^2 NOT$ gates, since $k = 2$ is the highest k value among all gates constituting the adder circuit to be studied later.

Decomposition of $C^2 NOT$ is obtained across the following steps:

Step 1: We determine a first decomposition of the $C^2 NOT$ gate (Figure 2a) to a circuit composed of $CNOT$, ν and $\nu^\dagger$ gates as depicted by Figure 2b.

Where ν and $\nu^\dagger$ are determined such that $\nu^2 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\nu^\dagger$ is the transpose conjugate of ν. Transfer matrix of ν and $\nu^\dagger$ are given as follows:

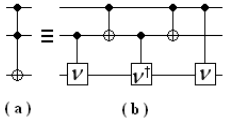


Figure 2: First decomposition of the $C^2 NOT$ gate.

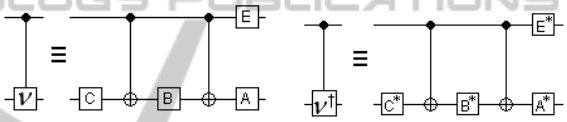
$$\nu = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix};\ \nu^\dagger = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix} \quad (5)$$

Step 2: Apply a control qubit to ν ($c\nu$) and $\nu^\dagger$ ($c\nu^\dagger$). Equation 5 becomes:

$$c\nu = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1+i}{2} & \frac{1-i}{2} \\ 0 & 0 & \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \quad (6)$$

$c\nu^\dagger$ is the transpose conjugate of $c\nu$.

Determine equivalent decomposition of $c\nu$ and $c\nu^\dagger$ to a set of single qubit and $CNOT$ gates as depicted by Figure 3(a) and Figure 3(b), respectively.



(a) Decomposition of $c\nu$. (b) Decomposition of $c\nu^\dagger$.

Figure 3: Decomposition of $c\nu$ and $c\nu^\dagger$.

Where A, B, C and D are given as follows:

$$A = \frac{\sqrt{2}}{2}\begin{pmatrix} cos\left(\frac{\pi}{8}\right)(1-i) & sin\left(\frac{\pi}{8}\right)(1-i) \\ -sin\left(\frac{\pi}{8}\right)(1+i) & cos\left(\frac{\pi}{8}\right)(1+i) \end{pmatrix}$$

$$B = \begin{pmatrix} cos\left(\frac{\pi}{8}\right) & sin\left(-\frac{\pi}{8}\right) \\ -sin\left(-\frac{\pi}{8}\right) & cos\left(\frac{\pi}{8}\right) \end{pmatrix}$$

$$C = \frac{\sqrt{2}}{2}\begin{pmatrix} (1+i) & 0 \\ 0 & (1-i) \end{pmatrix}$$

$$E = \begin{pmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2}(1+i) \end{pmatrix}$$

A^*, B^*, $C^*$and $E^*$are the conjugate matrix of A, B, C and E, respectively.

Step 3: Reassemble the equivalent parts of the circuit to obtain a final equivalent implementation as depicted by Figure 4.

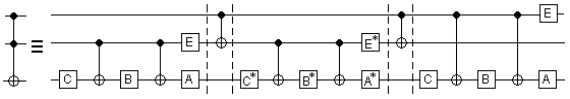


Figure 4: Final decomposition of the $C^2 NOT$.

According to (Nakahara and Ohmi, 2008; Barenco et al., 1995), for $k \geq 3$, the decomposition of $C^k NOT$

follows the same steps and all what differs from the C^2NOT decomposition is that ν and $\nu^\dagger$ transforms changes.

2.3 Modeling and Implementing *CNOT* Gate

During the last decade, large set of works have been addressed modeling and implementing *CNOT* gate. We consider in the following those based on linear optical components.

Early model have been proposed since 2001 by T.B.Pittman et al (Pittman et al., 2001), the construction for a probabilistic *CNOT* gate, using linear optics and auxiliary photon pair, was achieved by the combining of quantum encoder and a destructive *CNOT*. The desired *CNOT* gate was defined to work with a success probability of 1/16. This model has been optimized and the success probability raised to 1/4. T.B.Pittman presented an improvement of this model in 2003 (Pittman et al., 2003) and instead of using auxiliary entangled photon pair, a single auxiliary photon was used. The success probability remained equal to 1/4 and a physical realization including unexpected errors was presented.

A third model developed during 2002 is related to T.C.Ralph et al (Ralph et al., 2002), the model showed that the *CNOT* gate operates in the coincidence basis and the success probability is 1/9. This model presented some weaknesses related to path interference, to avoid this problem, a fourth model comes with the use of three Partially Polarizing Beam Splitter (PPBS). This model, known under the name "compact *CNOT* gate", was proposed by Ryo Okamoto et al (Okamoto et al., 2005) and kept same success probability value (1/9).

Another experimentation related to the third cited model was proposed by J.L.O.Brien et al in 2003 (Brien et al., 2003). The success probability obtained presented some errors comparing to the model.

Based on the TC.Ralph model theoretically proposed in (Ralph et al., 2002) and implemented in (Brien et al., 2003), we aim in this paper to model errors affecting the success probability of the gate at the experimentation level.

3 QUANTUM PROBABILISTIC GATE

3.1 Abstract Probabilistic *CNOT* Transform

Let $|c\rangle$ and $|t\rangle$, be vectors from a two dimensional real vector space spanned by the basis $\{|0\rangle,|1\rangle\}$, representing control and target qubits of a *CNOT* gate. The system's quantum state is a vector in the four dimensional real vector space spanned by the basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, representing the column vectors $\begin{pmatrix}1&0&0&0\end{pmatrix}^t$, $\begin{pmatrix}0&1&0&0\end{pmatrix}^t$, $\begin{pmatrix}0&0&1&0\end{pmatrix}^t$ and $\begin{pmatrix}0&0&0&1\end{pmatrix}^t$, respectively.

A probabilistic *CNOT* gate realizes the function $f_{CNOT} : |c,t\rangle \rightarrow |c,t\oplus c\rangle$ in a non deterministic way. In the sens that, for $i, j, k \in \mathbb{N}^*$:

$$\begin{aligned} \exists p &= (p_i)_{i\leq 4} \in [-1,1]^4 \\ \exists \varepsilon &= (\varepsilon_j)_{j\leq 4} \in [-1,1]^{12} \\ \exists \chi &= (\chi_k)_{k\leq 4} \in [-1,1]^4 \end{aligned} \quad (7)$$

Satisfying:

$$\begin{aligned} |p_1|^2+|\varepsilon_1|^2+|\varepsilon_2|^2+|\varepsilon_3|^2+|\chi_1|^2 &= 1 \\ |p_2|^2+|\varepsilon_4|^2+|\varepsilon_5|^2+|\varepsilon_6|^2+|\chi_2|^2 &= 1 \\ |p_3|^2+|\varepsilon_7|^2+|\varepsilon_8|^2+|\varepsilon_9|^2+|\chi_3|^2 &= 1 \\ |p_4|^2+|\varepsilon_{10}|^2+|\varepsilon_{11}|^2+|\varepsilon_{12}|^2+|\chi_4|^2 &= 1 \end{aligned} \quad (8)$$

Such that:

$$f_{CNOT}: \begin{cases} |00\rangle \rightarrow p_1|00\rangle+\varepsilon_1|01\rangle+\varepsilon_2|10\rangle \\ \quad +\varepsilon_3|11\rangle+\chi_1|\psi_{00}\rangle \\ |01\rangle \rightarrow \varepsilon_4|00\rangle+p_2|01\rangle+\varepsilon_5|10\rangle \\ \quad +\varepsilon_6|11\rangle+\chi_2|\psi_{01}\rangle \\ |10\rangle \rightarrow \varepsilon_7|00\rangle+\varepsilon_8|01\rangle+\varepsilon_9|10\rangle \\ \quad +p_3|11\rangle+\chi_3|\psi_{10}\rangle \\ |11\rangle \rightarrow \varepsilon_{10}|00\rangle+\varepsilon_{11}|01\rangle+p_4|10\rangle \\ \quad +\varepsilon_{12}|11\rangle+\chi_4|\psi_{11}\rangle \end{cases} \quad (9)$$

When the input of the *CNOT* is the basis state $|00\rangle$, p_1 represents the amplitude probability of realizing correctly the function f_{CNOT}, yielding to the correct output $|00\rangle$. ε_1, ε_2 and ε_3 are the amplitude probabilities of ending in the erroneous output basis state $|01\rangle$, $|10\rangle$ and $|11\rangle$, respectively, χ_1 is an amplitude probability that appears, when auxiliary qubits are used by the *CNOT* gate, and assigned to all states $|\psi_{00}\rangle$ that takes the system out of the basis states.

Following the same considerations for the rest of *CNOT* input states $|01\rangle$, $|10\rangle$ and $|11\rangle$, $|\psi_{01}\rangle$, $|\psi_{10}\rangle$

and $|\psi_{11}\rangle$ denotes the states out of the system basis, respectively.

We call probabilistic *CNOT* transform the matrix associated to the *CNOT* function given by equation 9 and denoted by U_{CNOT}.

We define P_{CNOT} to be the probability matrix describing theoretical probability of ending in a basis state after measure. P_{CNOT} components are obtained directly from the module of U_{CNOT} components squared.

Implementation of the quantum probabilistic *CNOT* gate gives a circuit that should be able to produce after measure P_{CNOT} or something close. However, implementation and measuring errors will only allow the determination of an estimated matrix denoted by P^{Imp}_{CNOT}.

Definition.

An abstract probabilistic transform is denoted by $A^{p,\varepsilon}$, satisfying properties of equations 7 and 8, and has the following form:

$$A^{p,\varepsilon} = \begin{pmatrix} p_1 & \varepsilon_4 & \varepsilon_7 & \varepsilon_{10} \\ \varepsilon_1 & p_2 & \varepsilon_8 & \varepsilon_{11} \\ \varepsilon_2 & \varepsilon_5 & \varepsilon_9 & p_4 \\ \varepsilon_3 & \varepsilon_6 & p_3 & \varepsilon_{12} \end{pmatrix} \quad (10)$$

Where $p = (p_i)_{1\leq i\leq 4}$ and $\varepsilon = (\varepsilon_j)_{1\leq j\leq 12}$ for $i, j \in \mathbb{N}^*$.

It's worth to notice that a probabilistic *CNOT* transform is an abstract probabilistic transform, but reciprocal way is not necessary checked. Therefore, there must be a technique capable of implementing the abstract probabilistic transform. We assign to the feasibility of implementation the concept of realizability.

$A^{p,\varepsilon}$ is a realizable matrix if there exist a quantum *CNOT* circuit whose physical parametrization permits to compute theoretically it's transfer matrix U_{CNOT} and verifying the equality $U_{CNOT} = A^{p,\varepsilon}$.

$A^{p,\varepsilon}$ is α-realizable, for $\alpha \in \mathbb{R}_+$, $\alpha \geqslant 1$, if $A^{p,\varepsilon}$ is realizable and the following condition is satisfied:

$$|p_i| \geqslant \alpha |\varepsilon_j| \quad (11)$$

Under condition of equation 11, we don't know at which level it's possible to determine p and ε to get U_{CNOT} having the form of $A^{p,\varepsilon}$. For this purpose, we study in the following the Ralph *CNOT* model (Ralph et al., 2002).

3.2 Realizable Abstract Probabilistic *CNOT* Transform based on the Ralph Model

A generalization of the Ralph *CNOT* model is the central component illustrated by stage 3 of Figure 5. It includes five Beam Splitters (BS), denoted BS_1, BS_2 , BS_3 BS_4 and BS_5, characterized by five reflectivity coefficients η_1, η_2, η_3, η_4 and η_5, respectively. We denote the generalized *CNOT* Ralph model by $CR(H)$, where $H = (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5) \in]-1,1[^5$. The associated *CNOT* transfer matrix obtained from the circuit is denoted by $U_{CR(H)}$.

The encoding and decoding modules contains four Polarizing Beam Splitter (PBS) and four Half Wave Plate (HWP).

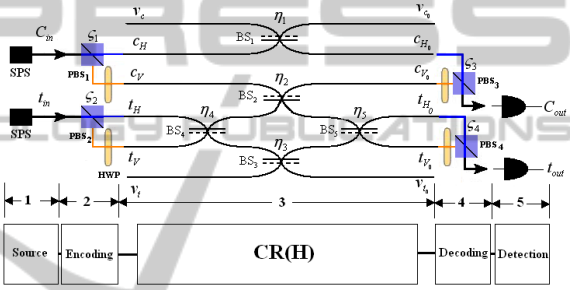


Figure 5: Generalization of the *CNOT* gate of TC.Ralph.

$CR(H)$operates on the dual rail coding to realize the *CNOT* function.

Recall that in their work, TC.Ralph et al (Ralph et al., 2002) used reflectivity coefficient $\eta = \eta_1 = \eta_2 = \eta_3 = 1/3$ and $\eta' = \eta_4 = \eta_5 = 1/2$ and showed that the *CNOT* gate operates with a success probability of $1/9$.

In the reality, BS imperfection of realization can't produce the values $\eta = 1/3$, $\eta' = 1/2$ but only values that are closed to them. Since $(1/3, 1/2)$ are supposed to be the ideal values, $CR(H)$ is proposed.

Proposition.

$A^{p,\varepsilon}$ is realizable by $CR(H)$, for $H = (\eta_1, \eta_2, \eta_3, \eta_4, \eta_5) \in]0,1[^5$, if the following equalities are satisfied:

$$p_1 = \sqrt{\eta_1\eta_2\eta_4\eta_5} + \sqrt{\eta_1\eta_3(1-\eta_4)(1-\eta_5)}$$
$$p_2 = \sqrt{\eta_1\eta_3\eta_4\eta_5} + \sqrt{\eta_1\eta_2(1-\eta_4)(1-\eta_5)}$$
$$p_3 = (1-2\eta_2)\sqrt{(1-\eta_4)\eta_5} + \sqrt{\eta_2\eta_3\eta_4(1-\eta_5)}$$
$$p_4 = (1-2\eta_2)\sqrt{\eta_4(1-\eta_5)} + \sqrt{\eta_2\eta_3(1-\eta_4)\eta_5}$$
$$\varepsilon_1 = \sqrt{\eta_1\eta_2(1-\eta_4)\eta_5} - \sqrt{\eta_1\eta_3\eta_4(1-\eta_5)}$$
$$\varepsilon_4 = \sqrt{\eta_1\eta_2\eta_4(1-\eta_5)} - \sqrt{\eta_1\eta_3(1-\eta_4)\eta_5}$$

$$\varepsilon_9 = (1-2\eta_2)\sqrt{\eta_4\eta_5} - \sqrt{\eta_2\eta_3(1-\eta_4)(1-\eta_5)}$$
$$\varepsilon_{12} = (1-2\eta_2)\sqrt{(1-\eta_4)(1-\eta_5)} - \sqrt{\eta_2\eta_3\eta_4\eta_5}$$
$$p_1 = \sqrt{\eta_1\eta_2\eta_4\eta_5} + \sqrt{\eta_1\eta_3(1-\eta_4)(1-\eta_5)}$$

$$(\varepsilon_j)_{1\le j\le 12,\, j\neq\{1,4,9,12\}} = 0 \qquad (12)$$

Moreover, $A^{p,\varepsilon}$ is α-realizable $\forall\alpha \geq 1$ by $CR(H)$, where $H = (\eta,\ \eta,\ \eta,\ \eta',\ \eta') \in]0,1[^5$, if $\eta = 1/3$ and $\eta' = 1/2$.

Proof.

We consider $\eta_{BS} \in]0,1[$ the reflectivity coefficient of a BS. Let a_{in}^{BS}, b_{in}^{BS} be the two incoming photons of the BS and a_{out}^{BS}, b_{out}^{BS} the outgoing photons. The Heisenberg equation relating outputs-inputs are illustrated by Figure 6 (reflection upon dashed lines introduces a π phase shift).

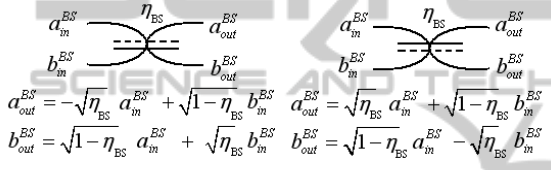


Figure 6: Heisenberg equation of the BS.

We consider the Heisenberg equations relating the control (c_H, c_V) and target (t_H, t_V) inputs photons to their corresponding outputs, depending on η_1, η_2, η_3, η_4 and η_5 (Figure 5). After excluding auxiliary inputs ν_c, ν_t and outputs ν_{c_0}, ν_{t_0}, these equations are given by the following:

$$c_{H_0} = \sqrt{\eta_1}c_H + \sqrt{(1-\eta_1)}\nu_c$$

$$\begin{aligned} c_{V_0} &= -\sqrt{\eta_2}c_V + \sqrt{(1-\eta_2)\eta_4}t_H \\ &\quad + \sqrt{(1-\eta_2)(1-\eta_4)}t_V \end{aligned}$$

$$\begin{aligned} t_{H_0} &= \left[\sqrt{\eta_2\eta_4\eta_5} + \sqrt{\eta_3(1-\eta_4)(1-\eta_5)}\right]t_H \\ &\quad + \left[\sqrt{\eta_2(1-\eta_4)\eta_5} - \sqrt{\eta_3\eta_4(1-\eta_5)}\right]t_V \\ &\quad + \sqrt{(1-\eta_2)\eta_5}c_V + \sqrt{(1-\eta_3)(1-\eta_5)}\nu_t \\ t_{V_0} &= \left[\sqrt{\eta_2\eta_4(1-\eta_5)} - \sqrt{\eta_3(1-\eta_4)\eta_5}\right]t_H \\ &\quad + \left[\sqrt{\eta_3\eta_4\eta_5} + \sqrt{\eta_2(1-\eta_4)(1-\eta_5)}\right]t_V \\ &\quad + \sqrt{(1-\eta_2)(1-\eta_5)}c_V - \sqrt{(1-\eta_3)\eta_5}\nu_t \end{aligned} \qquad (13)$$

For $H = (\eta_1,\ \eta_2,\ \eta_3,\ \eta_4,\ \eta_5)$ and $s,\ t \in \mathbb{N}^*$, these equations permits to determine the transfer matrix $U_{CR(H)} = (u_{s,t})_{s,t\le 4}$ as follows:

The input state $|00\rangle$ is represented by a presence of a photon in $|c_H\rangle$ and $|t_H\rangle$, the amplitude probability of having the correct output $|00\rangle$, meaning a simultaneous detection (coincidence basis) in $|c_{H_0}\rangle$ and $|t_{H_0}\rangle$, is given by the product of amplitude probabilities of having a photon in $|c_{H_0}\rangle$ and $|t_{H_0}\rangle$, when $|c_H\rangle = |1\rangle$ and $|t_H\rangle = |1\rangle$. Therefore, the resulting probability amplitude $u_{1,1}$ is expressed as:

$$u_{1,1} = \sqrt{\eta_1\eta_2\eta_4\eta_5} + \sqrt{\eta_1\eta_3(1-\eta_4)(1-\eta_5)}$$

The amplitude probability of having the erroneous output $|01\rangle$, $|10\rangle$ and $|11\rangle$, meaning a simultaneous detection on $|c_{H_0}\rangle$ and $|t_{V_0}\rangle$, $|c_{V_0}\rangle$ and $|t_{H_0}\rangle$, $|c_{V_0}\rangle$ and $|t_{V_0}\rangle$, are $u_{2,1}$, $u_{3,1}$ and $u_{4,1}$, respectively, expressed as:

$$\begin{aligned} u_{2,1} &= \sqrt{\eta_1\eta_2(1-\eta_4)\eta_5} - \sqrt{\eta_1\eta_3\eta_4(1-\eta_5)} \\ u_{3,1} &= 0,\ u_{4,1} = 0 \end{aligned}$$

Following the same manner, the input state $|01\rangle$ gives $u_{2,2} = p_2$, $u_{1,2} = \varepsilon_4$, $u_{3,2} = \varepsilon_5$, $u_{4,2} = \varepsilon_6$, the input state $|10\rangle$ gives $u_{4,3} = p_3$, $u_{1,3} = \varepsilon_7$, $u_{2,3} = \varepsilon_8$, $u_{3,3} = \varepsilon_9$ and the input states $|11\rangle$ gives $u_{3,4} = p_4$, $u_{1,4} = \varepsilon_{10}$, $u_{2,4} = \varepsilon_{11}$, $u_{4,4} = \varepsilon_{12}$, where $(p_i)_{1\le i\le 4}$ and $(\varepsilon_j)_{1\le j\le 12}$ are expressed by equation 12.

We consider $p = (p_1, p_2, p_3, p_4)$ and $\varepsilon = (\varepsilon_1, 0, 0, \varepsilon_4, 0, 0, \varepsilon_9, 0, 0, \varepsilon_{12})$ a set of amplitude probabilities depending on η_1, η_2, η_3, η_4 and η_5. $U_{CR(H)}$ defines a set of abstract probabilistic *CNOT* matrix having the following form:

$$A^{p,\varepsilon} = \begin{pmatrix} p_1 & \varepsilon_4 & 0 & 0 \\ \varepsilon_1 & p_2 & 0 & 0 \\ 0 & 0 & \varepsilon_9 & p_4 \\ 0 & 0 & p_3 & \varepsilon_{12} \end{pmatrix} \qquad (14)$$

Where $A^{p,\varepsilon} = U_{CR(H)}$.

We suppose that $A^{p,\varepsilon}$ is α-realizable $\forall\alpha \geq 1$ and as requested by Ralph, η=η_1=η_2=η_3, η'=η_4=η_5. Encoding and decoding parts are supposed to operate perfectly. According to these considerations, $U_{CR(H)}$ becomes:

$$U_{CR(H)} = \begin{pmatrix} \eta & 0 & 0 & 0 \\ 0 & \eta & 0 & 0 \\ 0 & 0 & -\eta+\eta'(1-\eta) & (1-\eta)\sqrt{(1-\eta')\eta'} \\ 0 & 0 & (1-\eta)\sqrt{(1-\eta')\eta'} & -\eta+(1-\eta)(1-\eta') \end{pmatrix} \qquad (15)$$

Moreover, by substituting these considerations into equation 12, we deduce that p and ε becomes:

$$\begin{aligned} p_1 &= p_2 = \eta \\ p_3 &= p_4 = (1-\eta)\sqrt{(1-\eta')\eta'} \\ \varepsilon_9 &= \varepsilon_{12} - \eta + \eta'(1-\eta);\ \varepsilon_{12} = -\eta + (1-\eta)(1-\eta') \\ &\quad (\varepsilon_j)_{1\le j\le 11,\, j\neq 9} = 0 \end{aligned} \qquad (16)$$

$\forall \alpha \geq 1$, $A^{p,\varepsilon}$ of equation 16 is α-realizable if $\varepsilon_9 = 0$ and $\varepsilon_{12} = 0$. Under these conditions, we deduce that $\eta = 1/3$ and $\eta' = 1/2$.

4 ERRORS OF THE CNOT RALPH MODEL

4.1 Internal Errors

We consider in the following errors affecting all BSs composing stage 3 of figure 5.

BS reflectivity coefficient presents some uncertainties with current BS technology. Work presented in (Ralph et al., 2002) predicted an error of about 0.007 on BS reflectivity coefficient and it concluded that errors below 0.01 are realistic. In the sequel, we assume this error lower than 0.05.

We study in the following the influence of the BSs errors on the α-realizability of $A^{p,\varepsilon}$.

First Case:
For the ideal Ralph model, meaning $\eta = \eta_1 = \eta_2 = \eta_3 = 1/3$ and $\eta' = \eta_4 = \eta_5 = 1/2$, we suppose that common error $\xi \in [-0.05, 0.05]$ affects BS1, BS2 and BS3 and $\xi' \in [-0.05, 0.05]$ affects BS4 and BS5, meaning that $\eta = 1/3 + \xi$ and $\eta' = 1/2 + \xi'$. Under these suppositions, p and ε of equation 16 changes as follows:

$$p_1 = 1/3 + \xi$$
$$p_3 = (2/3 - \xi)\sqrt{(1/2 - \xi')(1/2 + \xi')}$$
$$\varepsilon_9 = -\tfrac{3}{2}\xi + \tfrac{2}{3}\xi' - \xi\xi'; \varepsilon_{12} = -\tfrac{3}{2}\xi - \tfrac{2}{3}\xi' + \xi\xi'$$

$$(\varepsilon_j)_{1 \leq j \leq 11,\, j \neq 9} = 0 \qquad (17)$$

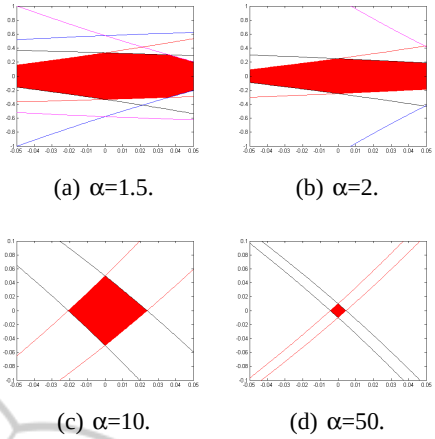
According to equations 17, a set of α-realizable $A^{p,\varepsilon}$ transforms is defined for $|p_1| \geqslant \alpha|\varepsilon_9|$, $|p_1| \geqslant \alpha|\varepsilon_{12}|$, $|p_2| \geqslant \alpha|\varepsilon_9|$ and $|p_2| \geqslant \alpha|\varepsilon_{12}|$.

We vary ξ in $[-0.05, 0.05]$ and α in $\{1.5, 2, 10, 50\}$. The delimited area illustrated by Figure 7(a), 7(b), 7(c) and 7(d), gives a representation of the parameters p and ε, for which $A^{p,\varepsilon}$ is α-realizable by $CR_{(H)}$.

According to Figure 7, α-realizability of $A^{p,\varepsilon}$ is defined by the ranges of ξ and ξ' inside the intersection. Table 1 shows the range of the smallest rectangle containing the surfaces of interest that allows α-realizability.

Second Case:

Even in the case where same technology is used to construct BS1, BS2, BS3, BS4 and BS5, different errors occurs independently on η_1, η_2, η_3, η_4 and η_5, respectively.



(a) α=1.5. (b) α=2. (c) α=10. (d) α=50.

Figure 7: α-realizability of $A^{p,\varepsilon}$ depending on BSs errors.

Table 1: ξ and ξ' ranges defining α-realizable $A^{p,\varepsilon}$.

α	ξ	ξ'
1.5	$[-0.05, 0.05]$	$[-0.05, 0.05]$
2	$[-0.05, 0.05]$	$[-0.05, 0.05]$
10	$[-0.021, 0.023]$	$[-0.05, 0.05]$
50	$[-0.005, 0.005]$	$[-0.01, 0.01]$

We consider $(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5) \in]-0.05, 0.05[^5$ the errors affecting optimal values $(1/3, 1/2)$ as:

$$(\eta_i = 1/3 + \xi_i)_{1 \leq i \leq 3}; (\eta_j = 1/2 + \xi_j)_{1 \leq j \leq 2} \qquad (18)$$

By substituting equations 18 into equations 12, we obtain a set of $A^{p,\varepsilon}$ that are α-realizable and has the form of equation 14.

Similarly to the process applied to common errors (ξ and ξ'), one can use numerical simulation to build Table 2 that illustrates the ranges of ξ_1, ξ_2, ξ_3, ξ_4 and ξ_5, yielding to the smallest area permitting to get a set of α-realizable $A^{p,\varepsilon}$.

It's worth to notice from this study that if we want that $A^{p,\varepsilon}$ be α-realizable for high α values, then errors should be minimal.

4.2 Input-output Errors

Encoding module in Figure 5 is composed of two PBSs and two HWPs, this permits to move from polarization to dual rail encoding where the presence of the single photon on the upper or the lower arms defines the $|0\rangle$ and $|1\rangle$ states, respectively. The transfer matrix of the encoding part is denoted by U_{end}.

Decoding module of Figure 5 realizes the inverted process and has a transfer matrix denoted by U_{dec}.

Table 2: ξ_1, ξ_2, ξ_3, ξ_4 and ξ_5 ranges defining α-realizable $A^{p,\varepsilon}$ transform.

α	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
1.5	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$
2	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$
10	$[-0.05, 0.05]$	$[-0.03, 0.03]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$	$[-0.05, 0.05]$
50	$[-0.05, 0.05]$	$[-0.001, 0.001]$	$[-0.02, 0.02]$	$[-0.01, 0.01]$	$[-0.01, 0.01]$

The encoding and decoding parts associated with $CR(H)$ previously studied, constitutes a polarization encoding $CNOT$ gate that is used to construct probabilistic $CNOT$-based circuits.

The total transform of the $CNOT$ gate, including encoding and decoding part, is denoted by $U_{CR(H)}^{enc,dec}$ and obtained as follows:

$$U_{CR(H)}^{enc,dec} = U_{dec}.U_{CR(H)}.U_{enc} \tag{19}$$

$CR_{(H)}$ of Figure 5 uses encoding-decoding modules, these latter may introduce errors due to imperfect PBS (Tyan et al., 1996). In our study, we neglect errors that may be introduced by HWP since it does not affect the logic function of the gate but rather it's second one, which is entangled photons state generation.

We denote a_{in}^{PBS} the incoming photon of the PBS (Figure 8) and a_{out}^{PBS}, b_{out}^{PBS} the outgoing photons.

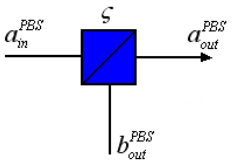


Figure 8: Polarizing Beam Splitter with error.

The error introduced by the PBS is modeled by $\varsigma \in [0,1]$, the PBS acts on the incident Horizontal (H) and vertical (V) photons as follows:

$$\begin{aligned} a_{in,H}^{PBS} &\rightarrow \sqrt{1-\varsigma}\,a_{out,H}^{PBS} + \sqrt{\varsigma}\,b_{out,H}^{PBS} \\ a_{in,V}^{PBS} &\rightarrow \sqrt{\varsigma}\,a_{out,V}^{PBS} + \sqrt{1-\varsigma}\,b_{out,V}^{PBS} \end{aligned} \tag{20}$$

In the two dimensional real vector space spanned by the basis $\{|0\rangle, |1\rangle\}$ with components $|0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$ and $|1\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix}^t$, the function of the PBS is given as:

$$f_{PBS} : \begin{cases} |0\rangle \rightarrow \sqrt{1-\varsigma}|0\rangle + \sqrt{\varsigma}|1\rangle \\ |1\rangle \rightarrow \sqrt{\varsigma}|0\rangle + \sqrt{1-\varsigma}|1\rangle \end{cases} \tag{21}$$

The matrix transform describing the PBS function with error $\varsigma \in [0,1]$, for $\langle 0|$ and $\langle 1|$ representing the bras vectors and having matrix expression $(1\,0)$ and $(0\,1)$, respectively, is denoted by U_{PBS}^{ς} and given as:

$$\begin{aligned} U_{PBS}^{\varsigma} &= \left(\sqrt{1-\varsigma}|0\rangle + \sqrt{\varsigma}|1\rangle\right)\langle 0| \\ &\quad + \left(\sqrt{\varsigma}|0\rangle + \sqrt{1-\varsigma}|1\rangle\right)\langle 1| \\ &= \begin{pmatrix} \sqrt{1-\varsigma} & \sqrt{\varsigma} \\ \sqrt{\varsigma} & \sqrt{1-\varsigma} \end{pmatrix} \end{aligned} \tag{22}$$

We consider ς_1, ς_2, ς_3 and ς_4, the error introduced by PBS1, PBS2, PBS3 and PBS4, respectively. By considering parallel combining of PBS1 and PBS2, parallel combining of PBS3 and PBS4, U_{enc} and U_{dec} are obtained as:

$$U_{enc} = U_{PBS1}^{\varsigma_1} \otimes U_{PBS2}^{\varsigma_2};\; U_{dec} = U_{PBS3}^{\varsigma_3} \otimes U_{PBS4}^{\varsigma_4}$$

Using the expression of U_{enc} and U_{dec}, one can deduce $U_{CR(H)}^{enc,dec}$ by simple computation.

Let us show know that the transfer matrix provided experimentally by J.L.O.Brein (Brien et al., 2003) can be computed with $U_{CR(H)}^{enc,dec}$ using specific values for the errors. Since the values are hardly complicated to obtain, we only show that we can approximate closely the matrix P_{CNOT}^{Imp} by selecting a series of values. For example, if we take $\eta_1 = 1/3 - 0.005$, $\eta_2 = 1/3 + 0.015$, $\eta_3 = 1/3 - 0.02$, $\eta_4 = 1/2 + 0.04$, $\eta_5 = 1/2 + 0.05$, $\varsigma_1 = 10^{-3.2}$, $\varsigma_2 = 10^{-2}$, $\varsigma_3 = 10^{-2}$ and $\varsigma_4 = 10^{-2}$, then a direct computation of $U_{CR(H)}^{enc,dec}$ is obtained and the associated probability matrix, denoted by $P_{CR(H)}^{enc,dec}$ is given as:

$$P_{CR(H)}^{enc,dec} = \begin{pmatrix} 0.1091 & 0.0051 & 0.0003 & 0.0011 \\ 0.0061 & 0.1080 & 0.0011 & 0.0001 \\ 0.0012 & 0.0002 & 0.0060 & 0.0970 \\ 0.002 & 0.0011 & 0.0969 & 0.0005 \end{pmatrix}$$

Knowing the expression of P_{CNOT}^{Imp} (Brien et al., 2003) which is equal to:

$$P_{CNOT}^{Imp} = \begin{pmatrix} 0.1056 & 0.0034 & 0.0006 & 0.0012 \\ 0.0026 & 0.1044 & 0.0012 & 0.0001 \\ 0.0027 & 0.0002 & 0.0256 & 0.08 \\ 0.0001 & 0.0024 & 0.0833 & 0.0289 \end{pmatrix}$$

One can deduce that the approximation is in the order of 10^{-2}. A similar computation for other errors values could show that $P_{CR(H)}^{enc,dec}$ is close to P_{CNOT}^{Imp} in lower order.

It's worth to mention that in their implementation, J.L.O.Brein et al (Brien et al., 2003)used as a Single Photon Source (SPS) a pairs of energy degenerate photons generated through beam-like spontaneous parametric down-conversion and collected into single-mode optical fibers (stage 1 of Figure 5), at the output level (stage 5 of Figure 5), C_{out} and t_{out} are analyzed by a system ending with a single photon counting module (SPCM).

Let us finally notice that SPS and SPCM, according to (Brida et al., 2006; Eiseman et al., 2011), do introduce some extra errors that are not under investigation in this work.

5 TOWARDS QUANTUM ALGORITHM SIMULATION

5.1 Computation Scheme

A quantum algorithm whose circuit is acting on a set of n qubits is a collection of binary functions $f_j : \{0,1\}^n \to \{0,1\}^n$, $j = [1..x]$ where $x \in \mathbb{N}^*_+$. The quantum circuit realizing the algorithm which we denote by Qc_{alg}, is composed by serial and parallel combining of circuits realizing f_j, denoted by Qc_{f_j}. We assume that Qc_{f_j} is based on C^kNOT gates.

Using the techniques developed in section 2.2, an equivalent single qubit and $CNOT$ gate based circuit denoted by QC_{CNOT} may be obtained. QC_{alg} and QC_{CNOT} compute the same transfer matrix U_{alg}. We describe briefly in the following, several techniques used to determine U_{alg}.

An abstract probabilistic $CNOT$ gate, acting on two qubits is represented by Figure 9a. Study of probabilistic $CNOT$-based quantum circuits requires description of the abstract probabilistic $CNOT$ transform in multiple qubits system (Figure 9b) composed of $m+2$ qubits, where $m \in \mathbb{N}$. To this end, $A^{p,\varepsilon}$ will have the equivalent block matrix representation:

$$A^{p,\varepsilon} \equiv \begin{pmatrix} A_{(1,1)} & A_{(1,2)} \\ A_{(2,1)} & A_{(2,2)} \end{pmatrix} \quad (23)$$

$$A_{(1,1)} = \begin{pmatrix} p_1 & \varepsilon_4 \\ \varepsilon_1 & p_2 \end{pmatrix}, \quad A_{(1,2)} = \begin{pmatrix} \varepsilon_7 & \varepsilon_{10} \\ \varepsilon_8 & \varepsilon_{11} \end{pmatrix},$$

$$A_{(2,1)} = \begin{pmatrix} \varepsilon_2 & \varepsilon_5 \\ \varepsilon_3 & \varepsilon_6 \end{pmatrix} \text{ and } A_{(2,2)} = \begin{pmatrix} \varepsilon_9 & p_4 \\ p_3 & \varepsilon_{12} \end{pmatrix}.$$

For m qubits between the control and the target , the effect on the final transform, depending on m, is denoted by $A^{p,\varepsilon}(m)$ and obtained as:

$$A^{p,\varepsilon}(m) = \begin{pmatrix} I_2^{\otimes m} \otimes A_{(1,1)} & I_2^{\otimes m} \otimes A_{(1,2)} \\ I_2^{\otimes m} \otimes A_{(2,1)} & I_2^{\otimes m} \otimes A_{(2,2)} \end{pmatrix} \quad (24)$$

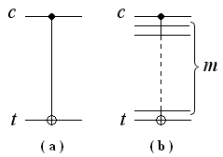


Figure 9: $CNOT$ gate used with $m+2$ qubits.

Using equation 24 and methods presented in (Chakrabarti and Kolay, 2008; Shende et al., 2003), we can use serial and parallel combining to determine U_{alg} by using identical $CR(H)$ in all the circuit.

U_{alg} is a function of nine errors, they are ξ_1, ξ_2, ξ_3, ξ_4, ξ_5 affecting BSs and ς_1, ς_2, ς_3, ς_4 affecting PBSs. A control of the errors may provide a better approximation of the algorithm function. We consider this in more details in the next paragraph.

5.2 Case Study

Several proposal of Quantum adder circuits were proposed in (Nakahara and Ohmi, 2008; Bannerjee and Pathak, 2009; Kaye, 2004; Florio and Picca, 2004; Vedral et al., 1996).The system used for our study is the three qubits Minimized Quantum Ripple Carry Adder (MQRCA) (Chakrabarti and Kolay, 2008). The 3-qubits MQRCA circuit is presented by Figure 10, it computes the SUM of two numbers A and B, represented by three qubits each as $|a_3,a_2,a_1\rangle$ and $|b_3,b_2,b_1\rangle$, respectively.

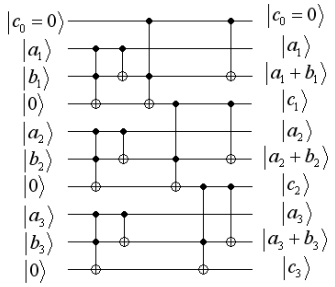


Figure 10: 3-qubits $CNOT$ based MQRCA.

The total number of $CNOT$ gates composing the MQRCA is $9\times 8+3=75$. The result of MQRCA is given by $|c_3, a_3+b_3, a_2+b_2, a_1+b_1\rangle$.

We present simulation results describing the errors effect on the success probability when realizing the SUM of $|A\rangle = |4\rangle$ and $|B\rangle = |7\rangle$.

Deterministic $CNOT$ gate realizes the addition with certainty as illustrated by Figure 11(a).

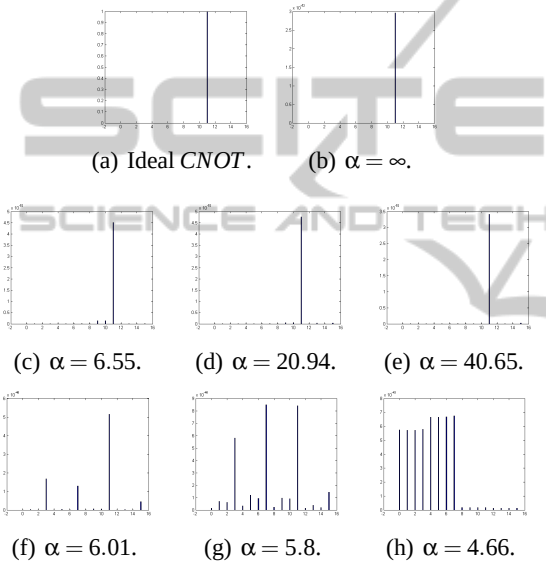
When using $CR(H)$, in one hand, we vary only BSs errors for fixed $(\varsigma_1,\varsigma_2,\varsigma_3,\varsigma_4) = (0,0,0,0)$ as illustrated by Table 3, in the other hand, we vary PBSs errors for fixed values $(\xi_1,\xi_2,\xi_3,\xi_4,\xi_5) =$

Table 3: Varying BSs errors.

α	η	η'	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ς_1	ς_2	ς_3	ς_4	P_{11}
6.55	1/3	1/2	0.05	-0.05	0.04	0.01	-0.01	0	0	0	0	4.45×10^{-48}
20.94	1/3	1/2	0.03	-0.01	-0.02	0.015	0.01	0	0	0	0	4.51×10^{-52}
40.65	1/3	1/2	-0.01	0.001	-0.02	-0.001	0.007	0	0	0	0	4.76×10^{-52}
∞	1/3	1/2	0	0	0	0	0	0	0	0	0	2.96×10^{-52}

Table 4: Varying PBSs errors.

α	η	η'	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5	ς_1	ς_2	ς_3	ς_4	P_{11}
6.01	1/3	1/2	0.05	-0.05	0.04	0.01	-0.01	$10^{-4.1}$	10^{-4}	$10^{-4.5}$	$10^{-3.8}$	5.15×10^{-48}
5.8	1/3	1/2	0.05	-0.05	0.04	0.01	-0.01	10^{-3}	$10^{-3.2}$	$10^{-3.4}$	$10^{-3.5}$	8.41×10^{-48}
4.66	1/3	1/2	0.05	-0.05	0.04	0.01	-0.01	10^{-2}	$10^{-2.2}$	$10^{-2.4}$	$10^{-2.5}$	1.8×10^{-44}



(a) Ideal *CNOT*. (b) $\alpha=\infty$. (c) $\alpha=6.55$. (d) $\alpha=20.94$. (e) $\alpha=40.65$. (f) $\alpha=6.01$. (g) $\alpha=5.8$. (h) $\alpha=4.66$.

Figure 11: Success probability of $(4+7)$.

$(0.05,-0.05,0.04,0.01,-0.01)$ as illustrated by Table 4.

$U_{CR(H)}$ associated to (ξ_1, ξ_2, ξ_3, ξ_4, ξ_5)=(0.05, -0.05, 0.04, 0.01, -0.01) and (ς_1, ς_2, ς_3, ς_4)=(0, 0, 0, 0) is given as follows:

$$U_{CR(H)} = U_{CR(H)}^{enc,dec}$$

$$= \begin{pmatrix} 0.3539 & -0.0173 & 0 & 0 \\ -0.0314 & 0.3539 & 0 & 0 \\ 0 & 0 & 0.054 & 0.3804 \\ 0 & 0 & 0.3782 & 0.054 \end{pmatrix} \quad (25)$$

According to equation 25, $\alpha = {}^{0.3539}/_{0.054}$ =6.55. For different α values, the resulting success probability of realizing correctly the SUM 4+7, denoted by P_{11}, is illustrated by Figure 11.

The correct output is obtained for probability P_{11} around 10^{-52}, which is significant comparing to the other outputs $\left(10^{-54}\right)$, but non interesting for realizing arithmetic operations.

We notice that this probability is very low since the success probability of the used model is around 1/9, the success probability decreases exponentially depending on the number of probabilistic *CNOT* gates used (=75).

Figures 11(b), 11(c), 11(d) and 11(e) shows the result of the SUM for $\alpha=[\infty,6.55,20.94,40,65]$. This figure shows that the higher the α value, the higher is the GAP between P_{11} and non significant results, but the lower is P_{11}.

Figure 11(f), 11(g) and 11(h) illustrate the impact of the encoding and decoding parts. ς_1, ς_2, ς_3 and ς_4 contribute to decrease α value and push non significant results to be closer to P_{11}. An upper bound to keep detection possible in our case is approximated to a PBS error around $\zeta=10^{-3}$.

6 CONCLUSIONS

In this work, we have defined an abstract probabilistic *CNOT* model, we identified and modeled errors occurring in the success probability in the case of T.C.Ralph *CNOT* based implementation. We also studied the effect of the errors occurring in the implementation of quantum algorithm when it uses identical *CNOT* called generalized Ralph *CNOT* model and abbreviated $CR(H)$. The work we have performed here, for $CR(H)$ based technology can be used with other technologies. We omitted in this paper to discuss the other technologies because of the lack of space and the redundancy of results. We believe that the study of implementations based on linear components will highlight a large range of α-realizable abstract probabilistic *CNOT*. Our future work address this issue.

REFERENCES

Bannerjee, A. and Pathak, A. (2009). An analysis of reversible multiplier circuits. *arXiv:0907.3357*, pages 1–10.

Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., and Weinfurter, H. (1995). Elementary gates for quantum computation. *Phys. Rev. A*, vol.52:pp.3457–3467.

Brida, G., Genovese, M., and Gramegna, M. (2006). Twin photon techniques for photo-detector calibration. *Laser.Phys.Lett*, vol.3, no.3:115–123.

Brien, J. L. O., Pryde, G. J., White, A. G., Ralph, T. C., and Branning, D. (2003). Demonstration of an all-optical quantum controlled-not gate. *Nature*, vol.426:pp.264–267.

Chakrabarti, A. and Kolay, S. S. (2008). Designing quantum adder circuits and evaluating their error performance. In *International conference on Electronic design ICED2008*, pages 1–6.

Eiseman, M. D., Fan, J., Migdall, A., and Polyavok, S. s. (2011). Single photon sources and detectors. *Rev.Sci.Instrum*, vol.82:p.071101.

Florio, G. and Picca, D. (2004). Quantum implementation of elementary arithmetic operations. *arXiv: quant-ph/0403048*.

Kaye, P. (2004). Reversible addition circuit using one ancillary bit with application to quantum computing. *arXiv: quant-ph/0408173v2*.

Nakahara, M. and Ohmi, T. (2008). *"Quantum computing from linear algebra to physical realizations"*. CRC Press, Taylor & Fancis Group, 6000 Broken sound parkway NW, suite 300, Boca Raton, FL 33487-2742.

Okamoto, R., Hofmann, H. F., Takeuchi, S., and Sasaki, K. (2005). Demonstration of an optical quantum controlled not gate without path interference. *Phys. Rev. Lett.95*, 210506:4 pages.

Pittman, T. B., Fitch, M. J., Jacobs, B. C., and Franson, J. D. (2003). Experimental controlled not logic gate for single photons in the coincidence basis. *Phys.Rev.A*, vol.68:p.032316.

Pittman, T. B., Jacobs, B. C., and Franson, J. D. (2001). Probabilistic quantum logic operations using polarizing beam splitters. *Phys.Rev.A*, vol.64:p.062311.

Ralph, T. C., Langford, N. K., Bell, T. B., and White, A. G. (2002). Linear optical controlled not gate in the coincidence basis. *Phys. Rev. A.65*, 062324:5 pages.

Shende, V. V., Prasad, A. K., Markov, I. L., and Hayes, J. P. (2003). synthesis of reversible logic circuits. *IEEE transaction on computer-aided design of integrated circuits and systems*, VOL 22, NO 6.

Tyan, R. C., Sun, P. C., and Tyan, Y. F. R.-C. (1996). Polarizing beam splitters constructed of form-birefringent multilayer gratings. *Proc. SPIE 2689, 82*.

Vedral, V., Barenco, A., and Ekert, A. (1996). Quantum networks for elementary arithmetic operations. *Phys. Rev. A.*, vol.54:pp.147–153.