Quantum Cryptography based on Grover's Algorithm

Z. Sakhi
Laboratory of Information Technology and Modelisation
Ben M'sik Faculty of Sciences, Hassan II-Mohamedia University, PO box 7955
Casablanca, Marocco
zb.sakhi@yahoo.fr

A. Tragha
Laboratory of Information Technology and Modelisation
Ben M'sik Faculty of Sciences, Hassan II-Mohamedia University, PO box 7955
Casablanca, Marocco
atragha@yahoo.fr

R. Kabil
Laboratory of Information processing,
Ben M'sik Faculty of Sciences, Hassan II-Mohamedia University, PO box 7955
Casablanca, Marocco
relkabil@yahoo.fr

M. Bennai
LPMC, Quantum Information Group,
Ben M'sik Faculty of Sciences, Hassan II-Mohamedia University, PO box 7955
Casablanca, Marocco
mdbennai@yahoo.fr

Abstract— Some cryptographic applications of quantum algorithm on many qubits system are presented. We analyze a basic concept of Grover algorithm and it's implementation in the case of four qubits system. We show specially that Grover algorithm allows as obtaining a maximal probability to get the result. Some features of quantum cryptography and Quantum Secret-Sharing protocol based on Grover's algorithm are also presented.

***Index Terms*— Qubit, quantum cryptography, Grover algorithm**

I. INTRODUCTION

Quantum information processing has emerged recently as a new information science combining physic, informatic and electronic. The mean idea behind quantum information computing is the use of the fundamental laws of quantum physic in information processing [1]. Thus, the information can be encoded in a superposition of states of photons, atoms, or ions which were defined as qubits. On the other hand, the increasing miniaturization of electronic circuits will be certainly limited by quantum effects at nanometer scale.

Recently, a renewed interest in the subject was seen, since the seminal work of Shor [2] and Grover [3]. This make possible to solve many problems which can't be reached in classical computing specially in cryptography. In this perspective, Grover algorithm has showed an increasing capacity to solve many problems and was applied in many contexts in particular in quantum cryptography [4]. Thus, the study of many qubits system has become very important. Recall that four qubits case is very special and entanglement of four qubits systems was studied by many authors and in different context [5].

In this work, we present some cryptographic applications of quantum algorithm in the case of many qubits system. We recall first, in the next section, some basic concept of Grover algorithm. We consider especially the case of four qubits system. Some features of quantum cryptography and Quantum secret-sharing protocol based on Grover's algorithm are presented in section 3. We show specially that Grover algorithm allows as to obtain a maximal probability to get the result.

II. GROVER'S ALGORITHM

II.1. Principe

In order to construct an adequate quantum algorithm, one has to introduce quantum logical gates similar to the classical ones. The most known quantum gates are: Hadamard and CNOT gates. The first one, which is used in the context of Grover algorithm, is a one qubit gate. This gate is very important because it allows as constructing a

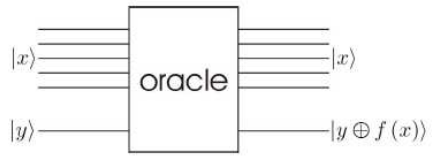
978-1-4673-2679-7/12/$31.00 ©2012 IEEE

superposed states from individual qubits. In matrix representation, the Hadamard gate, is a one-qubit rotation, mapping the qubit-basis states $|0\rangle$ and $|1\rangle$ to two superposition states with equal weight of the computational basis states $|0\rangle$ and $|1\rangle$. This corresponds to the transformation matrix given by:

$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ in $\{|0\rangle, |1\rangle\}$ basis.

In the following, we will recall the essential feature of the Grover algorithm. Suppose we have an unstructured database with N elements which are numbered from 0 to N-1, and the elements are not ordered. Classically, we would test each element at a time, until we get the one searched for. In Grover algorithm, only O($\sqrt{N}$) trials are needed [3]. Grover's algorithm has two registers: n qubits in the first one and one qubit in the second.

The first step is to create a superposition of all 2n computational basis states. This is achieved by initializing the first register in the state and applying the operator H_n, where H is the Hadamard gate. Then we define a function f which recognizes the solution as: $f: \{0,.....,N-1\} \rightarrow \{0,1\}$, f(k) = 1 if k is the searched element, f = 0 otherwise. Note that the function f is also known as an oracle and can be defined as:



Thus, we can resume the Grover algorithm as consisting of the following steps:

1. Consider an initial state: $|0\rangle^{\otimes n}$,
2. We apply the Hadamard gate on the first n qubits to get a uniform superposition of all possible arguments,
3. Apply the oracle f. Note that the information on f are included in the $(n+1)^{th}$ qubit,
4. Apply against the Hadamard gate,
5. Do an observation.

Note that, in this algorithm, we have a succession of a one Grover iteration operator (G) and the states of the first register correspond to the first iteration. In the next section, we show how this algorithm is applied for many qubits system and how it's used in quantum cryptography.

2.2. Example: Four qubits system case

As a realization of the above algorithm, we consider the case of four qubits. To apply the above procedure, we begin by affecting four qubits to the first register and one qubit to the second one. Thus, we initialize the first register to be in state $|0000\rangle$ and the second register in the state $|1\rangle$.

Apply now the Hadamard operator to the first register. We obtain:

$$|\psi\rangle = H|0\rangle^{\otimes 4} = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle$$

Thus

$$|\psi\rangle = \frac{1}{\sqrt{16}}\sum_{i=0}^{15}|i\rangle$$

On the other hand, we apply Hadamard gate to the second register to get the following state

$$H|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Now, to apply the Grover operator G, one must calculate the iteration number given by: $k_0 = round\left(\frac{\pi}{4}\sqrt{N}\right)$. For the present case, where N = 16, we have $k_0 = 3$.

Note that the calculation is done in the following working basis

$$\{|0000\rangle,|0001\rangle,|0010\rangle,|0011\rangle,|0100\rangle,|0101\rangle,|0110\rangle,|0111\rangle,$$
$$|1000\rangle,|1001\rangle,|1010\rangle,|1011\rangle,|1100\rangle,|1101\rangle,|1110\rangle,|1111\rangle\}$$

If we assume that the unknown element is, for example, $|1011\rangle = |11\rangle$, thus one can deduce

$$|\psi\rangle = \frac{1}{\sqrt{16}}\left(\sum_{\substack{i=0 \\ i\neq 11}}^{15}|i\rangle + |1011\rangle\right)$$
$$= \frac{1}{\sqrt{16}}\left(\sqrt{15}|\xi\rangle + |1011\rangle\right)$$

Where: $|\xi\rangle = \frac{1}{\sqrt{15}} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle$

The next steep of Grover algorithm consist of applying the oracle U_f, as:

$$U_f\left(|i\rangle|-\rangle\right) = (-1)^{f(i)}|i\rangle|-\rangle$$

$$|\psi_1\rangle|-\rangle = U_f\left(|\psi\rangle|-\rangle\right)$$

$$= \frac{\sqrt{15}}{4} U_f\left(|\xi\rangle|-\rangle\right) + \frac{1}{4} U_f\left(|1011\rangle|-\rangle\right)$$
$$= \frac{\sqrt{15}}{4}|\xi\rangle|-\rangle - \frac{1}{4}|1011\rangle|-\rangle$$

Introduce

$$|\psi_1\rangle = \frac{\sqrt{15}}{4}|\xi\rangle - \frac{1}{4}|1011\rangle$$
$$|\psi_1\rangle = \frac{1}{4}\sum_{\substack{i=0 \\ i \neq 11}}^{15}|i\rangle - \frac{1}{4}|1011\rangle$$

Now, if we apply the inversion operator about the mean, one can easily obtain

$$|\psi_2\rangle = \left(2|\psi\rangle\langle\psi| - \mathrm{I}\right)|\psi_1\rangle = \frac{3}{4}|\psi\rangle + \frac{1}{2}|1011\rangle$$

$$|\psi_2\rangle = \frac{3}{16}\sum_{\substack{i=0 \\ i \neq 11}}^{15}|i\rangle + \frac{11}{16}|1011\rangle$$

The second iteration (oracle) in Grover algorithm leads to

$$|\psi_3\rangle|-\rangle = U_f\left(|\psi_2\rangle|-\rangle\right)$$

$$|\psi_3\rangle = \frac{3}{4}|\psi\rangle - \frac{7}{8}|1011\rangle$$
$$|\psi_3\rangle = \frac{3}{16}\sum_{\substack{i=0 \\ i \neq 11}}^{15}|i\rangle - \frac{11}{16}|1011\rangle$$

Inversion operator about the mean leads to

$$|\psi_4\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_3\rangle = \frac{5}{64}\sum_{\substack{i=0 \\ i \neq 11}}^{15}|i\rangle + \frac{19}{64}|1011\rangle$$

By applying the 3th iteration, one can obtain easily

$$|\psi_5\rangle|-\rangle = U_f\left(|\psi_4\rangle|-\rangle\right) = \frac{5}{16}|\psi\rangle - \frac{33}{32}|1011\rangle$$

Apply again the inversion operator about the mean, one get

$$|\psi_f\rangle = \left(2|\psi\rangle\langle\psi| - I\right)|\psi_5\rangle$$
$$|\psi_f\rangle = -\frac{13}{256}\sum_{\substack{i=0 \\ i \neq 11}}^{15}|i\rangle + \frac{251}{256}|1011\rangle$$

Finally, to test Grover algorithm, we calculate the probability to find the state (or the searched element) $|1011\rangle$. This probability is around 96%.

III. QUANTUM CRYPTOGRAPHY BASED ON GROVER'S ALGORITHM

3.1. Principe

Quantum cryptography or Quantum Key Distribution (QKD) [6] is a theory for sharing secret keys, whose security is guaranteed based essentially on exploiting the laws of quantum physics. It allows the users to detect eavesdropping easily.

Recall that the current classical cryptographic technologies, such as RSA and others are based on factorization. It was recently shown that this problem could efficiently be solved using Shor's algorithm [2]. This breaking would have very important implications for electronic privacy and security. The only way to overcome this problem is to introduce quantum cryptographic protocols.

Note that the main goal of quantum cryptography is only to produce and distribute a key. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. Quantum key distribution has an important and unique properly; it is the ability of the two communicating users (traditionally referred to as Alice and Bob) to detect the presence of any third party (referred to as Eve) trying to gain knowledge of the key. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By

using quantum entanglement and transmitting information in quantum states over a quantum channel (such as an optical fiber), a communication system can be implemented which detects eavesdropping. More recently, some research has focused on another quantum cryptographic protocols: the quantum secret sharing (QSS) originally considered by Hillery *et al*.[7].

In the present work, we review a particular QSS Hsu [4] protocol, based on Grover's algorithm. An example of quantum secret sharing scheme using Grover's search algorithm for a two qubits system will be considered. The hope is to generalize this work, later, to other entangled states like W-states or EPR-states.

3.2. Quantum secret-sharing protocol based on Grover's algorithm

In this section, we present one of the most interesting quantum cryptographic protocol: the Hsu QSS protocol, especially in two qubits case. For this purpose, we suppose that the searched state is $|w\rangle$, where w can be either 00, 01, 10 or 11. The initial state is a tensor product of each individual state and is noted $|S_i\rangle$. Each qubits in the state $|S_i\rangle$ can be in one of the following states: $1/\sqrt{2}(|0\rangle+|1\rangle)$; $1/\sqrt{2}(|0\rangle-|1\rangle)$; $1/\sqrt{2}(|0\rangle+i|1\rangle)$; $1/\sqrt{2}(|0\rangle-i|1\rangle)$. Thus, we have a 16 possible states (i = 1, 2, … 16). Consider, for example, the state:

$$|S_1\rangle=\left[1/\sqrt{2}(|0\rangle+|1\rangle)\right]^{\otimes 2}$$

The protocol use different states: *carried* state, en*coded* state and *key* state. The carried state is a state randomly chosen from the states $|S_i\rangle$. Encoded state is obtained after applied the unitary transformation on carried state S_1: $|S_1\rangle_w=U_w|S_1\rangle$, where $U_w=I-2|w\rangle\langle w|$ and I is the unit operator and w is the encoded qubits such as 00, 01, 10 and 11.

The key state is obtained after applied the operator of decoding $U_{S_1}=I-2|S_1\rangle\langle S_1|$ on the coded state, the key state is obtained: $-U_{S_1}|S_1\rangle_w=a|w\rangle$; where a is some phase term and w can be 00, 01, 10,or 11.

Suppose now that the message is encoded in the state $|10\rangle$.

Next, we apply the encoding operator on $|S_1\rangle$. We can obtain then the encoded state $|S_1\rangle_{10}$:

$$\begin{aligned}|S_1\rangle_{10}&=U_{10}|S_1\rangle\\&=\left[I-2|10\rangle\langle 10|\right]\left[\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)\right]\\&=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)\end{aligned}$$

To obtain the key, one must then apply the decoding operator:

$$-U_{S1}=2|S_1\rangle\langle S_1|-1$$

on the encoded state $|S_1\rangle_{10}$. This allows as obtaining the key:

$$\begin{aligned}-U_{S_1}|S_1\rangle_{10}&=\left[2|S_1\rangle\langle S_1|-I\right]\left[\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)\right]\\&=|10\rangle\end{aligned}$$

This protocol was first introduced by Hsu [4], and can be represented as:

$$|S_i\rangle\xrightarrow{U_w}|S_i\rangle_w\xrightarrow{-U_{S_i}}|w\rangle$$

where i = 1,……,16.

Finally, we summarize the "Hsu" protocol in the following steps:

Step 1: Alice randomly prepares some carrier state $|S_i\rangle$. Then she applies an encoding operation U_w on $|S_i\rangle$, so as to obtain an encoded state $|S_i\rangle_w=U_w|S_i\rangle$.

Step 2: Alice sends one of the two qubits of the encoded state to Bob and the other qubit to Charlie respectively. After Bob and Charlie receive their qubits, they announce this fact publicly.

Step 3: Alice has to confirm that each agent has actually received the qubit via classical communication.

Step 4: Alice announces her initial state $|S_i\rangle$ in public.

Step 5: Only when Bob and Charlie combine their qubits and perform $-U_{S_i}$ on these two qubits can they both determine the marked state $|w\rangle$ with certainty.

Conclusion:

In this paper, we have presented some applications of quantum algorithm in the quantum information processing system. We have analyzed, in particular, the basic concept of Grover algorithm and its implementation in the case of four qubits system. Some features of quantum cryptography and Quantum secret-sharing protocol based on Grover's algorithm were also presented. In particular QSS Hsu protocol using Grover's search algorithm for a two qubits system was studied. This work is in it's beginning and must be improved to get a more protected protocol for some communication applications.

REFERENCES

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

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser, page 124, Los Alamitos, CA, (1994), IEEE Computer Society.

[3] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," Phys. Rev. Lett. 79 (1997) 325.

[4] Li-Yi-Hsu, "Quantum secret-sharing protocol based on Grover's algorithm,'' Phys. Rev. A 68 (2003) 022306.

[5] Z. Sakhi, A. Tragha, R. Kabil and M. Bennai, "Grover Algorithm Applied to Four Qubits System", Computer and Information Science, Canadian Center of Science and Education Vol. 4, No.3; (2011)

[6] C. Bennett and G. Brassard, cryptography: public key distribution and coin tossing, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India 1984) p.175.

[7] Hillery, M., V. Buzek, and A. Berthiaume, "Quantum secret sharing", Phys. Rev. A 59, (1999) 1829-1834.