Int J Theor Phys (2009) 48: 3262–3267
DOI 10.1007/s10773-009-0115-x

Quantum Mechanical Algorithm for Solving Quadratic Residue Equation

Hong-Fu Wang · Shou Zhang · Yong-Fang Zhao · Kyu-Hwang Yeon

Received: 31 May 2009 / Accepted: 27 July 2009 / Published online: 4 August 2009

Abstract We propose a quantum mechanical algorithm for solving quadratic residue equation $z^2 = b \pmod{M}$ based on Grover quantum search. The quantum algorithm will take $O(\sqrt{M})$ steps for finding the solutions to the equation by exploiting the properties of quantum superposition and interference effect, while classical algorithm to the same problem will take $O(M)$ steps. The success probability of the algorithm approaches to unity and the cost of the algorithm mainly depends on the calculations of quadratic residue modulo M and the number of iterations. Furthermore, we show that the algorithm can be used to solve the prime factorization problem, and the computing complexity is $O(\sqrt{N})$.

Keywords Quadratic residue equation · Grover quantum search · Factorization

Over the past few years, quantum computers based on fundamental quantum mechanical superposition principle have attracted a great deal of attention because it can provide exponential or quadratic speed-up for certain computational tasks which are not feasible on a classical computer, such as factoring problem [1], search problem [2–4], counting solution problem [5], phase estimation problem [6], hidden subgroup problem [7, 8], and so on. The existence of quantum algorithms shows that quantum computers can in principle outperform classical computers in many aspects. In early 1994 Shor [1] proposed a quantum mechanical algorithm showing that factorization problem and discrete logarithm problem which were

H.-F. Wang · S. Zhang (✉) · Y.-F. Zhao
Center for the Condensed-Matter Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, People's Republic of China
e-mail: szhang@ybu.edu.cn

S. Zhang
Department of Physics, College of Science, Yanbian University, Yanji, Jilin 133002, People's Republic of China

K.-H. Yeon
Department of Physics & BK21 Program for Device Physics, College of Natural Science, Chungbuk National University, Cheongju, Chungbuk 361-763, Republic of Korea

and still are widely believed to have no efficient solution on a classical computer could be solved efficiently on a quantum computer. However, Shor's algorithm had two shortcomings, that is, the order r must be even and the output might be a trivial factor. After the pioneering work of Shor, Grover [2–4] proposed another quantum mechanical algorithm for finding an unique marked element from an unordered database of size N by using $O(\sqrt{N})$ calls to the oracle. In contrast, the best classical algorithm requires $O(N/2)$ calls on average, and $O(N)$ calls in the worst case. The Grover quantum search could achieve this task quadratically faster than any classical algorithm, and more importantly, it did not depend for the impact on the unproven difficulty of the factorization problem. The power of quantum computation is based on the fact that the quantum state of a quantum computer can be a superposition of basis states and we can perform the unitary operations on multiple quantum states simultaneously.

The quadratic residue problem, which is thought to be a very difficult question in number theory, is the basis of modern cryptosystems and plays an important role. In 1979, Rabin [9] first designed a secure cryptosystem based on quadratic residue problem, called Rabin cryptogram. Rabin cryptogram was a special case of Rivest-Shamir-Adleman (RSA) cryptosystem [10] and had several characters comparing with RSA cryptosystem. Subsequently, Harn and Kiesler [11] proposed an improved Rabin public key cryptosystem and digital signature protocol, called H-K public key cryptosystem and H-K digital signature protocol, respectively. Nyang and Song [12] designed a fast digital signature protocol, i.e., N-S digital signature protocol. The security of N-S protocol was ensured by the difficulty of solving quadratic residue problem efficiently. In this paper, we propose a quantum mechanical algorithm for solving the quadratic residue equation $z^2 = b \pmod{M}$ (here M is very large), which is considered to be as hard as factorization problem and has no efficient polynomial time algorithms for this problem on a classical computer. The proposed quantum algorithm is not a polynomial time algorithm, only a quadratic speed-up algorithm. Furthermore, we apply the method to factorize a large number N that is the product of two odd prime numbers p and q, and the computing complexity is $O(\sqrt{N})$. The implementation of the algorithm would be an important evidence that quantum computer algorithm is more powerful than classical algorithm, serving to illustrate the strong power of quantum computer.

Let $\gcd(b, M) = 1$, $M > 0$. b is a quadratic residue modulo N if the quadratic equation $z^2 = b \pmod{M}$ has a solution. Otherwise, b is a quadratic non-residue modulo N. Here $\gcd(x,\ y)$ is the largest common divisor of x and y, that is, the largest integer that divides both x and y.

Theorem 1 *Suppose both c and d are odd prime numbers, and $M = c \cdot d$. Let $b \in Z_M^*$, Z_M^* denotes reduced set of residues modulo M. If b is a quadratic residue modulo M, then the equation $z^2 = b \pmod{M}$ has two sets of solutions in Z_M^*, that is, $\{z_1, M - z_1\}$ and $\{z_2, M - z_2\}$, and any two solutions of the two sets are not equal.*

In Theorem 1, it can be easily proved that if we let $z_i < M - z_i$ $(i = 1, 2)$, then $z_i \leq \frac{M-1}{2} < M - z_i$. Therefore, in the range $0 < z \leq \frac{M-1}{2}$, there are two solutions z_1 and z_2 to the equation $z^2 = b \pmod{M}$. And the other two solutions $M - z_1$ and $M - z_2$ are in the range $\frac{M-1}{2} \leq z < M$. We now give a quantum algorithm for finding the solutions z_1 and z_2 to the quadratic residue equation $z^2 = b \pmod{M}$. Here we have assumed that the quadratic residue equation has solutions. Suppose M is L bits long. The algorithm consists of the following steps.

Step (i) Initialize the first and the second registers in the state

$$|\psi\rangle = |0\rangle_1^{\otimes L-1} \otimes |0\rangle_2^{\otimes L}. \tag{1}$$

Step (ii) Apply the Walsh-Hadamard transform defined as $\mathcal{W} = \frac{1}{\sqrt{2}} \sum_{i,j=0}^{1} (-1)^{ij} |i\rangle\langle j|$ to each of the qubits in the first register, obtaining

$$|\psi\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} |z\rangle_1 \otimes |\mathbf{0}\rangle_2, \tag{2}$$

where $q = 2^{L-1}$ and $|\mathbf{0}\rangle = |0^{\otimes L}\rangle$.

Step (iii) Repeat the following unitary operations $O(\sqrt{q/2})$ times.

Step (iii)-(a) apply the unitary operator $\mathcal{U}_z^{\oplus}$ to the first and the second registers, where $\mathcal{U}_x^{\oplus} : |x\rangle \otimes |y\rangle \longrightarrow |x\rangle \otimes |y \oplus_n x^2 (\mathrm{mod}\ M)\rangle$, giving

$$|\psi\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} |z\rangle_1 \otimes \left|\mathbf{0} \oplus_L z^2 \ (\mathrm{mod}\ M)\right\rangle_2, \tag{3}$$

where $\oplus$ is XOR operation, which is the addition modulo 2.

Step (iii)-(b) rotate the state $|b\rangle_2$ in the second register by a phase of π radians.

Step (iii)-(c) apply the $\mathcal{U}_z^{\oplus}$ to the first and the second registers again, giving

$$|\psi\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} (-1)^{\delta_{b,z^2(\mathrm{mod}M)}} |z\rangle_1 \otimes |\mathbf{0}\rangle_2, \tag{4}$$

Step (iii)-(d) apply the $\mathcal{W}^{\otimes L-1}$ transform to the first register.

Step (iii)-(e) rotate all the states $|z\rangle_1$ except state $|0\rangle_1$ in the first register by a phase of π radians, namely, $|z\rangle_1 \longrightarrow -(-1)^{\delta_{0,z}} |z\rangle_1$.

Step (iii)-(f) apply the $\mathcal{W}^{\otimes L-1}$ transform to the first register again.

Step (iv) Measure the resulting state in the first register and thus get the solution z_1 (z_2) to the equation $z^2 = b \ (\mathrm{mod}\ M)$ with a probability greater than 0.5. Repeat the algorithm again, we can obtain the other solution z_2 (z_1) to the equation $z^2 = b \ (\mathrm{mod}\ M)$.

So far we have proposed a quantum mechanical algorithm for solving quadratic residue equation. The main cost of the algorithm depends on the calculations of quadratic residue modulo M and the number of iterations. Mathematically, $z^2 \ (\mathrm{mod}\ M)$ can be computed by a reversible gate array [13, 14]. Asymptotically, the best result for gate arrays for multiplication is the Schönhage-Strassen algorithm [15], which needs $O(k \log k \log\log k)$ gates to multiply two k-bit numbers for integer multiplication. However, Schönhage-Strassen algorithm operates well only for large k, while for small k, it does not scale well. For small numbers, the best gate arrays for multiplication essentially use elementary-school longhand multiplication in binary, requiring $O(k^2)$ time to multiply two k-bit numbers. Thus the implementation of $z^2 \ (\mathrm{mod}\ M)$ in the present algorithm requires $O((L-1)^2)$ time with this method.

The success probability of the present algorithm depends on the number of iterations. Chen et al. [16] have proved that the upper bound on the required time of iterations is

$$R \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{N'}{M'}} \right\rceil, \tag{5}$$

where N' is the total number of the initial states and M' is the number of the marked states. That is, $R = O(\sqrt{M/4})$ iterations must be performed for obtaining the solutions to the equation $z^2 = b \ (\mathrm{mod}\ M)$ with high probability. In addition, in the present algorithm, multi-qubit

controlled phase gate operations are required to be performed during the iteration process. Up to now many schemes have be presented to generate multi-qubit controlled phase gate using different physical systems, such as cavity QED system [17–25], linear optical system [26], NMR system [27], Josephson charge qubits in superconducting circuit [28], ion trap system [29, 30], and so on. Therefore, the iteration process can be efficiently implemented. The computing complexity of the present algorithm is $O(\sqrt{M})$.

We now use this quantum algorithm to solve another problem—prime factorization problem. To factor an integer N, we shall use quantum computation to solve an equivalent problem.

Theorem 2 *Suppose N is an L bit composite number ($N = p \cdot q$, both p and q are odd prime numbers), and z is a non-trivial solution to the equation $z^2 = 1 \pmod N$ in the range $1 \le z \le N$, that is, neither $z = 1 \pmod N$ nor $z = N - 1 = -1 \pmod N$. Then $\gcd(z \pm 1, N)$ are nontrivial factors of N that can be computed using $O(L^3)$ operations.*

Proof For the quadratic equation $z^2 = 1 \pmod N$, let $N = p \cdot q$ with $\gcd(p,\ q) = 1$, we have

$$(a)\quad \begin{cases} z_1 = 1 \pmod p, \\ z_1 = 1 \pmod q, \end{cases} \qquad (b)\quad \begin{cases} z_2 = -1 \pmod p, \\ z_2 = -1 \pmod q, \end{cases}$$
$$(c)\quad \begin{cases} z_3 = 1 \pmod p, \\ z_3 = -1 \pmod q, \end{cases} \qquad (d)\quad \begin{cases} z_4 = -1 \pmod p, \\ z_4 = 1 \pmod q. \end{cases} \tag{6}$$

In each case $z_i^2 = 1 \pmod p$ and $\pmod q$; so each z_i satisfies $z^2 = 1 \pmod N$. By the *Chinese remainder theorem*, each set has a unique solution $\pmod N$. From (a) and (b) we obtain

$$z_1 = 1 \quad \text{and} \quad z_2 = N - 1 \pmod N \quad \longrightarrow \quad \text{trivial solutions}, \tag{7}$$

and from (c) and (d) we obtain

$$z_3 = a \quad \text{and} \quad z_4 = N - a \pmod N \quad \longrightarrow \quad \text{nontrivial solutions}. \tag{8}$$

Therefore, we have

$$(a + 1)(a - 1) = 0 \pmod N, \tag{9}$$

obtaining

$$\begin{cases} \gcd(a - 1, N) = p, \\ \gcd(a + 1, N) = q. \end{cases} \tag{10}$$

By virtue of Euclid's algorithm [31] we may compute $\gcd(a - 1,\ N)$ and $\gcd(a + 1,\ N)$. Thus we obtain the nontrivial factors p and q of N, using $O(L^3)$ operations. □

As mentioned above, we can compute a factor of N if we can find a nontrivial solution $z' \neq \pm 1 \pmod N$ to the equation $z^2 = 1 \pmod N$. The whole algorithm for factorizing is described as below.

Step (i) Initialize the first and the second registers in the state

$$|\psi'\rangle = |0\rangle_1^{\otimes L-1} \otimes |\mathbf{0}\rangle_2. \tag{11}$$

Step (ii) Apply the $\mathcal{W}^{\otimes L-1}$ transform to the first register, obtaining

$$|\psi'\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} |z\rangle_1 \otimes |\mathbf{0}\rangle_2. \tag{12}$$

Step (iii) Repeat the following unitary operations $O(\sqrt{q})$ times.

Step (iii)-(a′) apply the unitary operator $\mathcal{U}_z^{\oplus}$ to the first and the second registers, giving

$$|\psi'\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} |z\rangle_1 \otimes \left|\mathbf{0} \oplus_L z^2 \pmod N\right\rangle_2. \tag{13}$$

Step (iii)-(b′) rotate the state $|1\rangle_2$ in the second register by a phase of π radians.

Step (iii)-(c′) rotate the state $|1\rangle_1$ in the first register by a phase of π radians.

Step (iii)-(d′) apply the $\mathcal{U}_z^{\oplus}$ to the first and second registers again, giving

$$|\psi'\rangle \longrightarrow \frac{1}{q^{1/2}} \sum_{z=0}^{q-1} (-1)^{\delta_{1,z}} (-1)^{\delta_{1,z^2 (\mathrm{mod} N)}} |z\rangle_1 \otimes |\mathbf{0}\rangle_2. \tag{14}$$

Step (iii)-(e′) apply the $\mathcal{W}^{\otimes L-1}$ transform to the first register.

Step (iii)-(f′) rotate all the states $|z\rangle_1$ except state $|0\rangle_1$ in the first register by a phase of π radians.

Step (iii)-(g′) apply the $\mathcal{W}^{\otimes L-1}$ transform to the first register again.

Step (iv) Measure the first register. Therefore, we can obtain the nontrivial solution z' to the equation $z^2 = 1 \pmod N$ according to the measurement result.

Finally, we compute $\gcd(z' \pm 1, N)$ and thus get the two nontrivial factors of N. Here we should point out that the proposed algorithm for factoring is not a polynomial time algorithm, such as Shor's factorization algorithm [1], it is only a quadratic speed-up algorithm compared with classical algorithm.

In summary, we have proposed a quantum mechanical algorithm for solving quadratic residue equation $z^2 = b \pmod M$. The classical algorithm to this problem requires $O(M)$ calculations for finding the solutions to the quadratic residue equation $z^2 = b \pmod M$, while the present quantum algorithm only needs $O(\sqrt{M})$ calculations, proving a quadratic speed-up. As an application of this algorithm, we show that the prime factorization problem could be solved by using the proposed quantum algorithm. The essential idea of factorization is to find a non-trivial solution z' to the equation $z^2 = 1 \pmod N$. By computing $\gcd(z' \pm 1, N)$ based on Euclid's algorithm, we can get two non-trivial factors of N. The implementation of the algorithm would be an important step toward showing the strong power of quantum computer.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grant No 60667001.

References

1. Shor, P.W.: In: Proceedings of the Symposium on the Foundations of Computer Science, pp. 124–134. IEEE Computer Society Press, Los Alamitos (1994)

2. Grover, L.K.: Phys. Rev. Lett. **79**, 325 (1997)
3. Grover, L.K.: Phys. Rev. Lett. **79**, 4709 (1997)
4. Grover, L.K.: Phys. Rev. Lett. **80**, 4329 (1998)
5. Boyer, M., Brassard, G., Hoyer, P., Tapp, A.: Fortschr. Phys. **46**, 493 (1998)
6. Kitaev, A.Y.: quant-ph/9511026
7. Simon, D.: In: Proceedings of the Symposium on the Foundations of Computer Science, pp. 116–123. IEEE Computer Society Press, Los Alamitos (1994)
8. Jozsa, R.: quant-ph/9707033
9. Rabin, M.V.: Technical Report TR212 (1979)
10. Rivest, R.L., Shamir, A., Adleman, L.: Commun. Assoc. Comput. Mach. **21**, 120 (1978)
11. Harn, L., Kiesler, T.: Electron. Lett. **25**, 726 (1989)
12. Nyang, D.H., Song, J.S.: Electron. Lett. **33**, 205 (1997)
13. Lecerf, Y.: C. R. Acad. Fr. Sci. **257**, 2597 (1963)
14. Bennett, C.H.: IBM J. Res. Dev. **17**, 525 (1973)
15. Schönhage, A., Strassen, V.: Computing **7**, 281 (1971)
16. Chen, G., Fulling, S.A., Chen, J.: quant-ph/0007123
17. Xiao, Y.F., Zou, X.B., Guo, G.C.: Phys. Rev. A **75**, 054303 (2007)
18. Wang, H.F., Zhang, S.: Chin. Phys. B **17**, 1165 (2008)
19. Yang, C.P., Han, S.: Phys. Rev. A **72**, 032311 (2005)
20. Wang, H.F., Zhang, S., Yeon, K.H.: J. Korean Phys. Soc. **53**, 1787 (2008)
21. Gabris, A., Agarwal, G.S.: Phys. Rev. A **71**, 052316 (2005)
22. Wang, H.F., Zhang, S., Yeon, K.H.: J. Korean Phys. Soc. **53**, 3144 (2008)
23. Xiao, Y.F., Zou, X.B., Guo, G.C.: Phys. Rev. A **75**, 014302 (2007)
24. Zhang, Y.Q., Zhang, S., Jin, X.R., Yeon, K.H.: J. Korean Phys. Soc. **51**, 1626 (2007)
25. Zhu, A.D., Zhang, S., Yeon, K.H., Um, C.I.: J. Korean Phys. Soc. **52**, 1 (2008)
26. Zou, X.B., Li, K., Guo, G.C.: Phys. Rev. A **74**, 044305 (2006)
27. Chen, C.Y., Feng, M., Gao, K.L.: Phys. Rev. A **73**, 064304 (2006)
28. Niskanen, A.O., Vartiainen, J.J., Salomaa, M.M.: Phys. Rev. Lett. **90**, 197901 (2003)
29. Cirac, J.I., Zoller, P.: Phys. Rev. Lett. **74**, 4091 (1995)
30. Šašura, M., Bužck, V.: Phys. Rev. A **64**, 012305 (2001)
31. Knuth, D.E.: The Art of Computer Programming, vol. 2. Addison-Wesley, Reading (1997)