# HOW TO USE CLASSICAL OPERATION IN DIGITAL BITS TO SIMULATE QUANTUM BITS FOR THE RSA CRYPTOSYSTEM

Jun-Ya Wang[1], Xui-Chengn Chang[2] and Hung-Ju Wang[3]
[1]National Taiwan University of Science and Technology
[2]National Chengchi University
[3]Bureau of Standards, Metrology, and Inspection

## ABSTRACT

*In quantum algorithm, the Shor's algorithm can find prime decomposition of very big numbers easily and break RSA encryption much faster and more efficiently than in the classical case. How to complicant the public key to slow down the speed and efficiency of Shor's algorithm to secure our RSA encryption scheme is main issue in this study. By using classical random simulation to operation as quantum bits to complicate the RSA cryptosystem, even Shor's algorithm can not to find prime decomposition of very big numbers n with qubits random simulation easily.*

## KEYWORDS

*encryption, decryption, key, quantum bits, simulation*

## 1. INTRODUCTION

Shor's algorithm can find prime decomposition of very big numbers in O((logN)^3) time and O(logN) space. Our internet's security relies on the RSA encryption scheme, which involves encryption using an enormous number made of two large prime numbers. Finding large prime numbers is thus very useful to decrypt messages. Shor's algorithm uses quantum mechanics to find such prime numbers, and break RSA encryption much faster and more efficiently than in the classical case [1]. In this study, a methodolody try to use qubit simulator to complicate the public key to slow down the speed and efficiency of Shor's algorithm to secure our RSA encryption scheme.

David C. Wyld et al. (Eds): ICDIPV, CBIoT, ICAIT, WIMO, NC, CRYPIS, ITCSE, NLCA, CAIML -2023
pp. 367-376, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131328

## 2. BASIC OPERATION IN DIGITAL BITS AND QUANTUM BITS IN THE RSA CRYPTOSYSTEM

A bit is a binary unit of information used in classical computation which can take two kind of values, typically taken to be 0 or 1[2]. But quantum bit can be in a state of |0› and |1› with α|0› + β|1› where, α and β are complex numbers, satisfying |α|2 + |β|2 = 1[3]. Hence, the combinational classical bits and quantum bits can be treated as information in classical bits and noise in quantum bits.

In simple unitary transforms, or quantum gates, NOT Gate flips a bit from 0 to 1 and vice versa[4]. This NOT Gate can exchange the bit position easy. NOT=$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

For a linear map, if we set P |0› = |0› and P |1› = 0› then P=$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ [5] is orthogonal projection. This linear map can eliminate noise from quantum bits.

Consider Rivest-Shamir-Adelman (RSA) – Oldest of the public-private key cryptography systems to transmit shared keys for symmetric key cryptography [6], the RSA Cryptosystem generate two large prime numbers p and q and multiply them together to get very large number N [7] as public key and a flow chart illustrating the RSA decryption Algorithm [8] to create an RSA public and private key pair in the following steps as figure 1.

(1) Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = p*q

(2) Select a third number, e, that is relatively prime to the product phi=(p $-1$ )( q $-1$ ) , the number e is the public exponent.

(3) Calculate an integer d from the quotient $\frac{(ed-1)}{(p-1)(q-1)}$ . The number d is the private exponent.

(4) The public key is the number pair (n, e ) . Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough. v. To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation: C= Me Mod n.

(5) The receiver then decrypts the cipher-text with the private key using the equation: M =Cd Mod n.

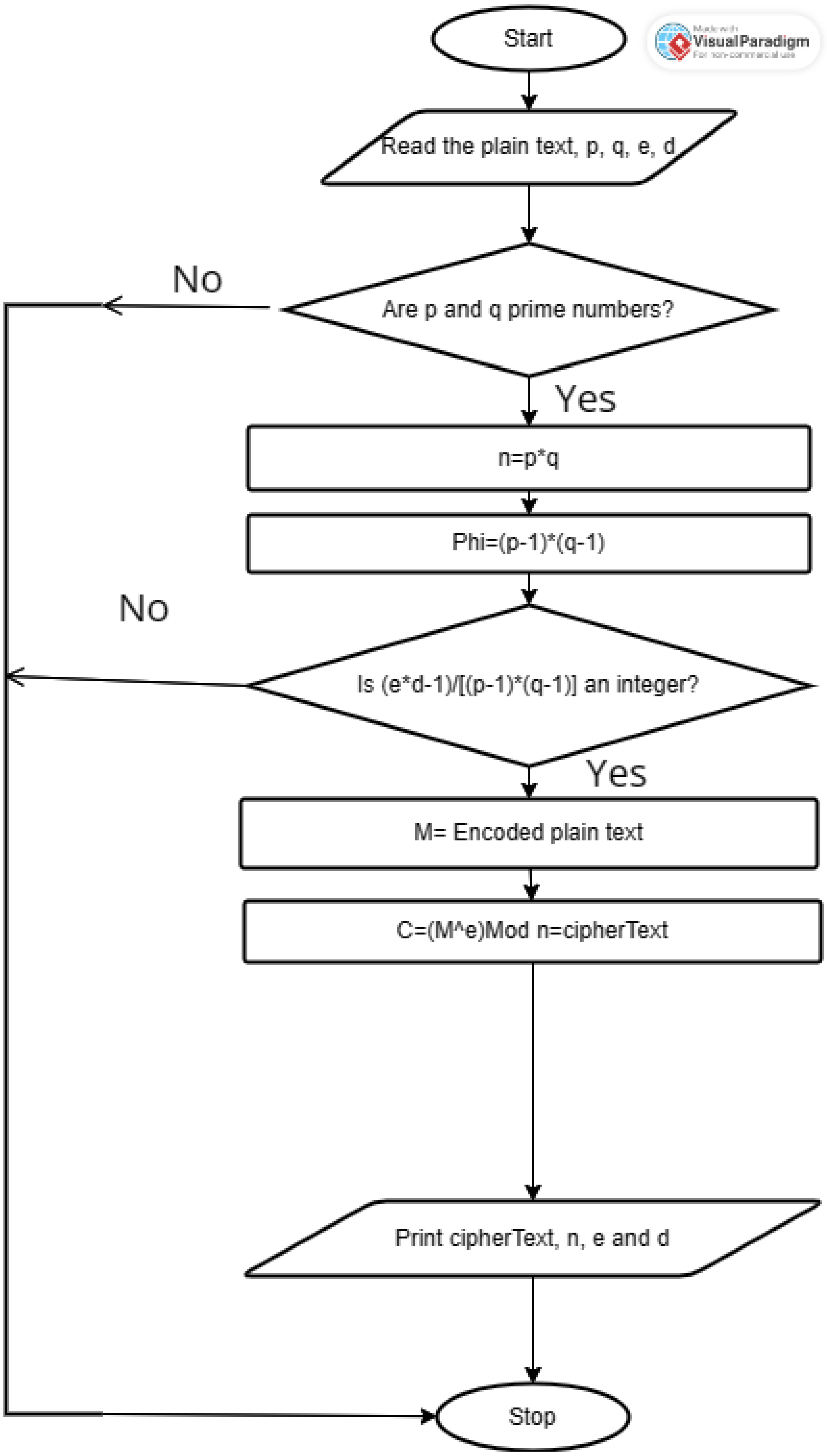

Start
Made with Visual Paradigm For non-commercial use
Read the plain text, p, q, e, d
Are p and q prime numbers?
No
Yes
n=p*q
Phi=(p-1)*(q-1)
Is (e*d-1)/[(p-1)*(q-1)] an integer?
No
Yes
M= Encoded plain text
C=(M^e)Mod n=cipherText
Print cipherText, n, e and d
Stop

Figure 1, A flow chart illustrating the RSA decryption Algorithm

Use the keys for encryption in the following steps as figure 2.

(1) Obtains the recipient B's public key (e,n)

(2) Represents the plaintext message as a positive integer M .

(3) Computes the cipher-text C= Me Mod n.

(4) Send the cipher-text C to B.

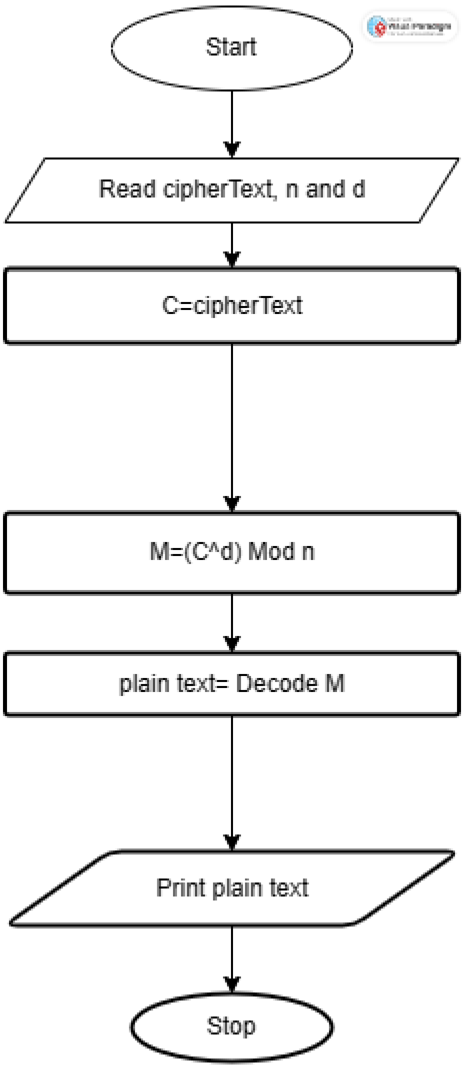
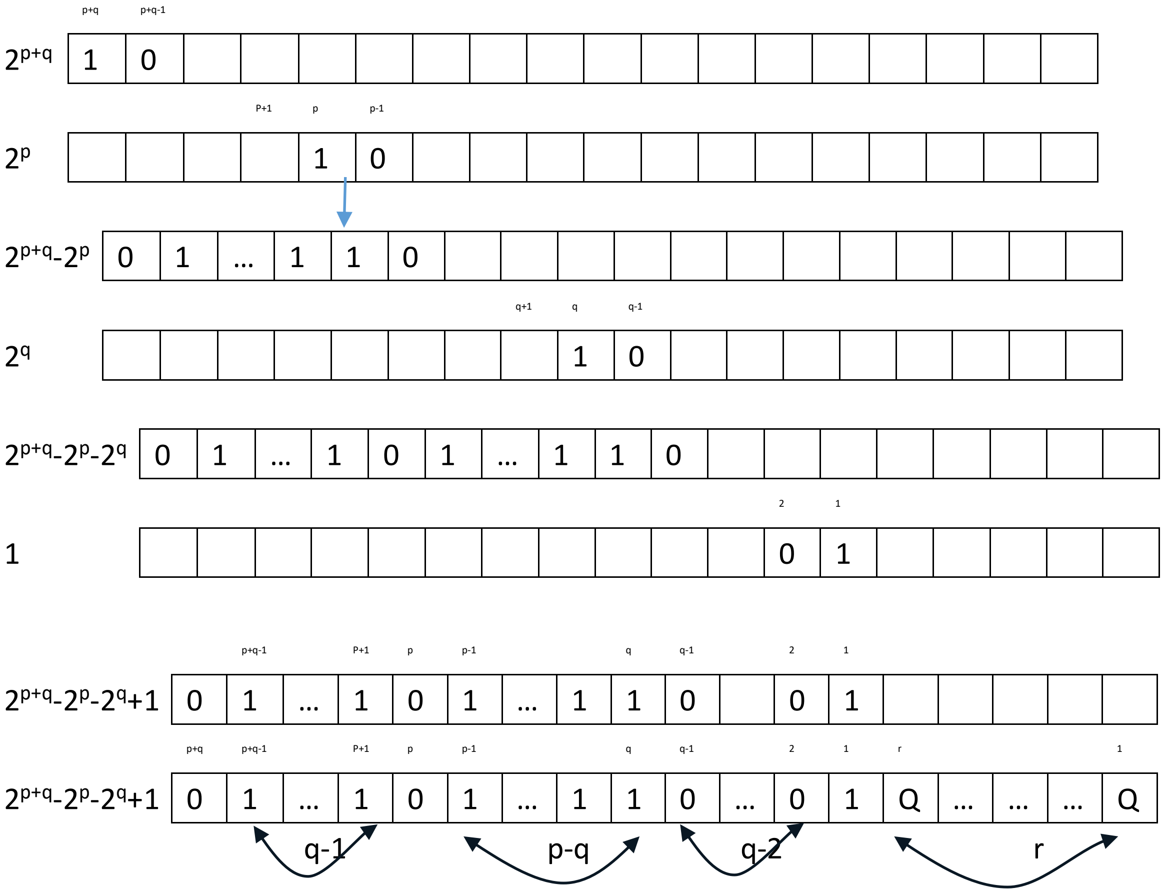


Figure 2, A Flow Chart to Illustrate the Decryption Algorithm

## 3. The RSA Cryptosystem with Combinational Classical Bits and Quantum Bits

According to the Mersenne Numbers, if p was prime, then so was Mx = $2^x$-1.Thus means the public key is two large prime numbers $(2^p-1)*(2^q-1)=2^{p+q}-2^p-2^q+1$. This public key has $2^{p+q}-1$ digits in binary system.



There are p-q+q-1=p-1 replaceable 1 and q-2 replaceable 0 with r qubits. The combination of N* in public key at $(2^p-1)*(2^q-1)$ with r qubits is $\frac{(p+q)!}{(p-1)!(q-2)!(r)!}2^r$

Let the first two largest prime number, p=82589933 and q=77232917 [9], the public key has 82589923+77232917=159822840 digits in binary system. Meanwhile, IBM's condor quantum provides 1121 qubits. Hence, we can combine classical bits 159822840 digits and noise in quantum bits 1121 qubits. In this public key, we generate random signals either 0 or 1 to simulate those qubits. Then those 1121 qubits are noise in these public key digits. We need to eliminate those noise qubits by orthogonal projection with known position. But we can NOT Gate to flip noise qubits position. Therefore, the combinations of this public key are$\frac{(159822840)!}{(82589922)!(77232915)!(1121)!}2^{1121}$. In the same length of 159823961=159822840+1121 digits, if we choose the first largest prime number and the third prime number, p=82589933 and q=77232917 [9], the public key has 82589923+ 74207281=156797204 digits in binary system. Then the random signals to simulate those qubits is in 159823961-156797204 =3026757 qubits. The combinations of this public key are$\frac{(156797204)!}{(82589922)!(74207279)!(3026757)!}2^{3026757}$. The simulation qubits can be increase dramatically from 1121 to 3026747 without the limitation of the capacity of qubits in quantum computer. The reverse flip noise qubits position and eliminate noise qubits can be signal in quantum entanglement [10]to be encryptedand a flow chart illustrating the RSA decryption Algorithm can be modified as figure 3 and 4 respectively.

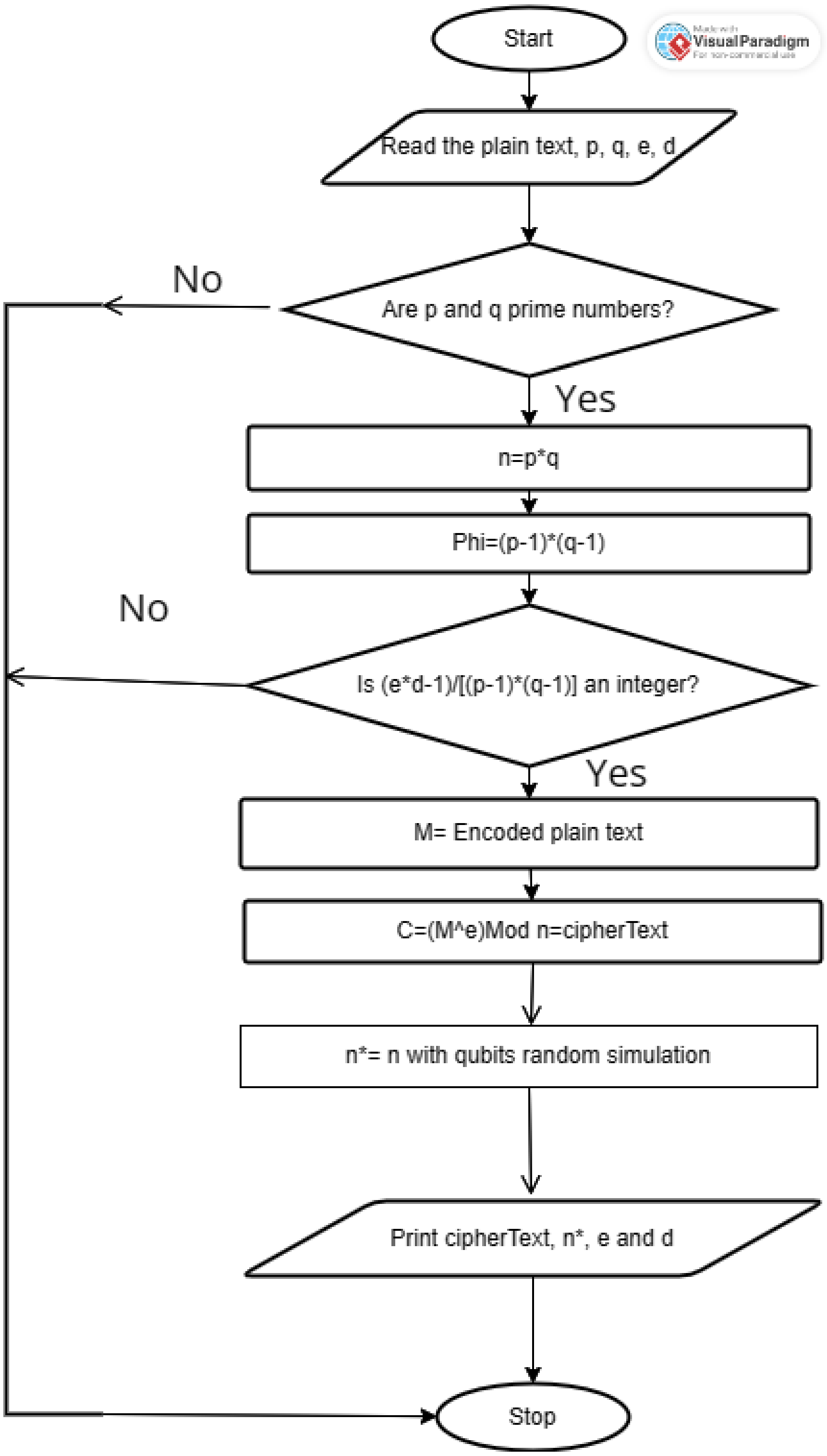

Start
Made with Visual Paradigm For non-commercial use
Read the plain text, p, q, e, d
Are p and q prime numbers?
No
Yes
n=p*q
Phi=(p-1)*(q-1)
Is (e*d-1)/[(p-1)*(q-1)] an integer?
No
Yes
M= Encoded plain text
C=(M^e)Mod n=cipherText
n*= n with qubits random simulation
Print cipherText, n*, e and d
Stop

Figure 3, A flow chart illustrating the RSA decryption Algorithm with qubits random simulation

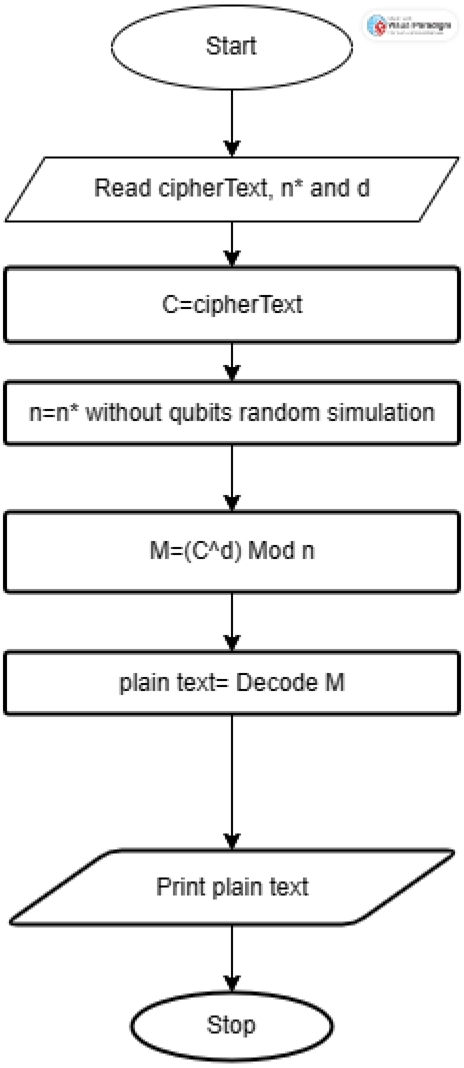


Figure 4, A Flow Chart to Illustrate the Decryption Algorithm with qubits random simulation

## 4. CONCLUSION

In this study, we use classical random simulation to operation as quantum bits to complicate the RSA cryptosystem even Shor's algorithm can not to find prime decomposition of very big numbers n with qubits random simulation. This simulation can increase qubits dramatically without the limitation of the capacity of qubits in quantum computer. That is the way to use the capacity of qubits in quantum computer to reverse flip noise qubits position and eliminate noise qubits can be signal in quantum entanglement encrypted and use qubit simulator to complicate the public key to slow down the speed and efficiency of Shor's algorithm to secure our RSA encryption scheme.

## 5. REFERENCE

[1] Shor's algorithm (Shor's algorithm (qutube.nl))

[2] What is the difference between a qubit and classical bit?(https://quantumcomputing.stackexchange.com/questions/112/what-is-the-difference-between-a-qubit-and-classical-bit)

[3] Anuj Dawar, Quantum Computing Lecture 1 Bits and Qubits(https://www.cl.cam.ac.uk/teaching/0910/QuantComp/notes.pdf)

[4] C/CS/Phys 191 Unitary Evolution, No Cloning Theorem, Superdense Coding 9/4/03 Fall 2003(https://inst.eecs.berkeley.edu/~cs191/sp05/lectures/lecture4.pdf)

[5] Des Johnston, Notes by Bernd J. Schroers, Quantum Mechanics and Quantum Computing: An Introduction, Heriot-Watt University, page 15 (http://www.macs.hw.ac.uk/~des/qcnotesaims17.pdf)

[6] Built by Metropolis, Public – private key pairs & how they work (https://www.preveil.com/blog/public-and-private-key/)

[7] Dr. David Singer (Dept. of Mathematics, CWRU) and Mr Ari Singer (NTRU Cryptosystems) Mr. Ari Singer (NTRU Cryptosystems), Big Numbers: The Role Played by Mathematics in Internet Commerce, page 8 (https://case.edu/affil/sigmaxi/files/CryptoslidesSinger.pdf)

[8] Nentawe Y. Goshwe, Data Encryption and Decryption Using RSA Algorithm in a Network Environment, IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 (Data Encryption and Decryption Using RSA Algorithm in a Network Environment | Semantic Scholar)

[9] The Largest Known prime by Year: A Brief History (https://primes.utm.edu/notes/by_year.html)

[10] Quantum entanglement: A simple explanation (https://www.space.com/31933-quantum-entanglement-action-at-a-distance.html)

## AUTHORS

**Jun-Ya Wang** M.S. of Deaprtment of Computer Science and Information Engineering, National Taiwan University of Science and Technology, B. S. of Department of Information Management, School of Management, National Dong Hwa University

**Xui-Chengn Chang** M.S. of Deaprtment of Computer Science, National Chengchi University, B. S. of Deaprtment of Computer Science, National Chengchi University

**Hung-Ju Wang** M.S. of Deaprtment of Electrical Engineering, UCLA, M.S. of Deaprtment of Acturial Science, UW, Madison