International Journal of Theoretical Physics
https://doi.org/10.1007/s10773-021-04789-x

# Practical Security of RSA Against NTC-Architecture Quantum Computing Attacks

Kai Li[1,2] · Qing-yu Cai[1,3]

Received: 29 December 2020 / Accepted: 17 March 2021 / Published online: 19 June 2021

**Abstract**
Quantum algorithms can greatly speed up computation in solving some classical problems, while the computational power of quantum computers should also be restricted by laws of physics. Due to quantum time-energy uncertainty relation, there is a lower limit of the evolution time for a given quantum operation, and therefore the time complexity must be considered when the number of serial quantum operations is particularly large. When the key length is about at the level of KB (encryption and decryption can be completed in a few minutes by using standard programs), it will take at least 50-100 years for NTC (Neighbor-only, Two-qubit gate, Concurrent) architecture ion-trap quantum computers to execute Shor's algorithm. For NTC architecture superconducting quantum computers with a code distance 27 for error-correcting, when the key length increased to 16 KB, the cracking time will also increase to 100 years that far exceeds the coherence time. This shows the robustness of the updated RSA against practical quantum computing attacks.

**Keywords** Quantum computing · RSA · Shor's algorithm

## 1 Introduction

In the early 1980s, Benioff described the first quantum mechanical model of a computer [1], and Feynman pointed out that the exact simulation of quantum physical systems can be ideally achieved with computers governed by quantum mechanics [2]. The groundbreaking was that Shor discovered a polynomial time algorithm for calculating prime number decomposition and discrete logarithm [3, 4], which threatened the security of RSA public key cryptosystem. On account of the wide use of the RSA algorithm in modern electronic commerce for information encryption, the cracking of RSA public key cryptosystem

✉ Qing-yu Cai
qycai@wipm.ac.cn

[1] State Key Laboratory of Magnetic Resonances and Atomic and Molecular Physics, Innovation Academy for Precision Measurement Science and Technology, Chinese Academy of Sciences, Wuhan, 430071, China

[2] University of Chinese Academy of Sciences, Beijing, 100049, China

[3] School of Information and Communication Engineering, Hainan University, Haikou, 570228, China

by quantum algorithm will pose a serious threat to everyone's information and property security. After that, Shor's quantum algorithm become a widely concerned subject that needs to be studied urgently due to the rapid development of quantum computing. In experiment, there are many applicable candidate for quantum computation, including ion trap systems [5–7], linear optics systems [8, 9], semiconductor quantum dot systems [10, 11] and superconducting systems [12]. Recently, the superconducting systems advanced rapidly because the circuit chips can be processed with traditional semiconductor technology. Google lately realized a 53-qubits quantum processor by using a superconducting system [13]. Another notable candidate for quantum computing is trapped ion systems that has advantages in ultrashort operation time $\tau_{op}$ and high-fidelity. In 2018, IonQ achieved the trapped ion quantum computation of 160-bit storage qubits and 79-bit single-qubit operations, and built an 11-qubit quantum processor to calculate the ground-state energy of water molecules [14, 15].

Although quantum algorithms can speed up the calculation, it still takes a certain amount of time to complete a quantum algorithm in practice. If the cracking time exceeds a set time, the results obtained are overdue and therefore useless, which is especially true in the field of cryptography. For example, when the time required to crack a ciphertext exceeds its confidentiality period, the cracking is obviously unsuccessful. On the security of RSA, it has been discussed by Bernstein et al. that it needs $2^{44}$ multiplication modulo $n$ operations to solve the 4096-bit 1 TB key length PQRSA protocol with the Shor's algorithm [16]. Under this huge-scale inputs, a total of $2^{100}$ qubit operations were finally estimated. On the one hand, 1 TB key length input may be too large for the public key cryptosystem, since it will greatly reduce the efficiency of the actual information transmission due to the too long decryption time. On the other hand, $2^{100}$ qubit operations may cause the time overhead actually far exceeding the security requirement. Therefore, finding a key length that can both quickly encrypt and decrypt and ensure security under quantum algorithm attacks is an interesting matter in the field of RSA public key cryptography and even public key cryptography.

Quantum algorithms are accelerated by the support of physical principles, but the computational speed of quantum computers will also be restricted by laws of physics. For example, there is a minimum time to complete a quantum operation due to the time-energy uncertainty relation, based on which one can theoretically estimate the time cost of Shor's algorithm, and obtain the minimum number of bits required for the RSA public key cryptosystem. When the number of key bits is gradually increased, the time overhead of the quantum computing attacks will become gradually unbearable since quantum computing has a computational speed limit that is restricted by laws of physics. The key is safe if practical quantum computers take longer time to crack the key than the key needs to be kept secret. In theory, there are two different architecture for practical quantum computers, the AC (Abstract, Current) architecture, and the NTC (Neighbor-only, Two-qubit gate, Concurrent) architecture. Since the AC architecture leads to possible unwanted couplings that will significantly reduce of the coherence time of the qubits, the NTC architecture is more adopted in experiments. In this paper, we theoretically show that, if the key length is about at the level of tens KB, the time required for NTC architecture ion trap quantum computers to successfully crack the key will be more than 50 years, which can meet the confidentiality requirements of most commercial secrets. This paper is organized as follows. The algorithm complexity of RSA public key system and Shor's algorithm are reviewed in Section 2. In Section 3, the energy-time uncertainty relation and quantum operation time limit are described first, and then we enumerate the ion trap system for quantum operation to estimate the specific time overhead. Finally, we discuss and conclude.

## 2 RSA Public Key and Shor's Algorithm

Let us briefly review the RSA public key cryptosystem and Shor's algorithm in this section.

### 2.1 RSA Public Key

As an asymmetric public key cryptosystem, the security of RSA is based on the difficulty of integer modular exponentiation and large integer factorization. The key generation steps are as follows:

1. Generate two large prime numbers $p, q$, let $N = pq$ be the modulus of the public key system.
2. Select the public key exponent $e$, $e$ is co-prime with the Euler function of $N$, $\varphi(n) = (p-1)(q-1)$.
3. The private key $d$ is obtained by the relationship $ed = 1 \pmod{\varphi(n)}$, and then $(N, e)$, $(N, d)$ are packaged as the public key and the private key respectively.

The RSA key size $n = log\ N$ currently used is generally 1024 bits, or 2048 bits. The public key exponent $e$ can be selected manually, but it should not be too small to achieve relative security, and also not be too large to reduce encryption time. It is common in the industry to use $e = 65537(2^{16} + 1$ in binary system), which is the smallest prime number in the form of $2^{2^k} + 1$ except for 2, 3, 5, 17, 257.

The length of plaintext $M$ requires $0 < M \leqslant N$ ($M$ can be grouped when $M > N$, so that each group of plaintext $M_i \leqslant N$). Then $C = M^e \pmod N$ is calculated to obtain ciphertext, and recover the plaintext by obtain $M = C^d \pmod N$. In this way, the encryption algorithm only needs to perform a few times multiplication modular exponentiations (for the specific $e = 65537$) with a relatively long private key, and the decryption time is also acceptable.

### 2.2 Shor's Algorithm

The keypoint to Shor's algorithm is to turn the factoring problem into the problem of finding the period of a function [3, 4]. Take an arbitrary positive integer $a$, which satisfies $\{a \in Z | a < N, \gcd(a, N) = 1\}$, and $r$ is the order of $a$ (it requires $r$ to be an even number to execute the subsequent algorithm), i.e., $a^r = 1 \pmod N$. One can get

$$(a^{r/2} - 1)(a^{r/2} + 1) = 0 \pmod N. \tag{1}$$

Then use Euclidean algorithm to find $\gcd(a^{r/2} - 1, N)$, $\gcd(a^{r/2} + 1, N)$, and get the nontrivial factors of $N$.

From $a^r = 1 \pmod N$, $a^x = a^{x+jr} \pmod N$ can be obtained. Thus, finding the order $r$ of $a$ can be transformed into solving a periodic problem of the function $f(x) = a^x \pmod N$. The time overhead of running Shor's algorithm depends on the complexity of the quantum circuits (Actually the overhead of the classical part of the algorithm is the same as or even smaller than the quantum part, including the continued fraction expansion and the Euclidean algorithm. See Section 5.3.1 in [17]). The QFT can get the integers which are the closest to the integer multiples of $N/r$ with the probability of $\Omega(1)$. The execution time complexity of the standard QFT circuits is $O(n^2)$. If parallelism is adopted, QFT circuit complexity will be smaller [18]. However, the total complexity of the algorithm mainly depends on the modular exponentiation. So we will not discuss the complexity of QFT further here. The most time-consuming part is to calculate $a^x \pmod N$, which is the modular exponentiation with the complexity $O(n^3)$ [17] (See more in Appendix). It's worth noting that $O(n^3)$ is the complexity of modular exponentiation in a serial NTC (neighbor-only, two-qubit-gate, concurrent) structure. There are also parallel schemes, which make the time complexity of modular exponentiation reach to the order of $O(log^3 n)$ [19]. The reduction of time is always accompanied by the increase of qubits. In addition to the increase of qubits required, the parallel architecture has a limitation on long distance multi-qubit gates. Detailed analysis will be discussed in Section 4. We use the order $O(n^3)$ complexity for estimation in the following.

Therefore, the complexity of the overall quantum circuit is $O(n^3)$, and the probability of successful calculation of $r$ is at the $O(1)$ level. The success probability determines the repeat times of algorithm when considering the time overhead. As the key length $n = \log N$ increases, the time overhead of Shor's algorithm increase at a rate of $O(n^3)$. If one increases the key length $\log N$ appropriately in practice, the time overhead of running Shor's algorithm will be too huge to crack the key timely. On the other side, the key length cannot be too long to perform the encryption and decryption, which makes it important to find out an appropriate $\log N$ for RSA against quantum computing attacks.

The difference between some Shor's algorithm variants is the coefficients before $n^3$, which has no effect on the complexity function, but a greater impact on the specific time overhead. For example, if the coefficient is in the range of $0.1 \sim 100$, it can produce a multiple of $10^3$. This has an influence on our estimation of the specific tolerable time cost, and therefore on the estimation of RSA key length. In the following, we default the coefficient as 1 to estimate the secure key length, and discuss the secure key length $n$ against optimized Shor's algorithms.

## 3 Speed Limit and Time Overhead

With the time-consuming for each quantum operation, we can estimate the time overhead of running Shor's algorithm step by step.

### 3.1 Time-energy Uncertainty Relation and Speed Limit

Every step of the quantum computer changes the state of the system and consumes a certain amount of time. This time is actually the evolution time of a quantum state in one operation. Whether it is a single-qubit gate or a multiple, one can record the evolution time of the controlled qubit as the shortest time of an operation. So the total time is the sum of the time of all operations.

The concept of quantum speed limit is gradually formed [20–23], after Aharonov and Bohm [24] explained the energy-time uncertainty relationship as the relationship of time interval $\Delta t$ of the quantum state change rate and the dispersion $\Delta E$ of its energy. If the Hamiltonian is independent of time, the quantum speed limit can be written as followed,

$$t_{QSL} \geqslant \frac{\hbar}{\Delta E_0} \arccos |\langle \psi_0 | \psi_t \rangle|, \tag{2}$$

where $\Delta E_0 = \sqrt{\langle H_0^2 \rangle - \langle H_0 \rangle^2}$ is the energy standard deviation of initial Hamiltonian in initial state, and $|\psi_0\rangle$ and $|\psi_t\rangle$ are the initial state and the final state of the evolution respectively [22]. This states that the evolution time of a quantum system has a minimum lower bound restricted by physical principles.

The basic network to realize modular exponentiation is modular addition. The ordinary addition network can be composed of two controlled-not gates to complete the addition operation, two Toffolli gates and a controlled-not gate to complete the carry operation. And the modular addition network can also be composed of several above adders [25]. So if one takes the two-qubit gate as the basic operation, such a chain structure makes the circuit time complexity of modular addition proportional to the input $n$.

Next we just need to estimate the operation time of each basic operation. Considering that all universal quantum gates can be composed of single qubit gates and two-qubit gates [17], and the two-qubit gates commonly used in adders are the controlled-not gates, we take the operation time of single-bit gate instead of two-bit gate in the following calculation as the basic operation time. The reasons are as follows: the operation time of a single qubit gate is less than that of a two-qubit gate (as can be seen from the trapped ion model we will use), and what we are estimating is the lower bound of time, so our model is feasible and reasonable.

It is worth noting that in classic computers, the operation speed is limited by the clock speed. The similar concept in quantum computing is that, the clock frequency can be understood as the time required to evolve between two distinguishable states, that is, the time to transform between $|0\rangle$ and $|1\rangle$. In the following section, whether the evolution time between orthogonal states can be used as the operation time of the quantum gates will be discussed in detail in the following section. Finally, we will find that the actual quantum gate operation time can indeed be estimated by Eq. (2), and the deviation will not affect the magnitude of the key length estimation presented at the end of this article.

### 3.2 Time Overhead for NTC Architecture Trapped-ion Quantum Computing

Trapped ion quantum computer system is one of the most promising architectures for a scalable universal quantum computer. There are currently two schemes for applying trapped ions as qubits. (a) Using the electronic ground state and metastable excited state as qubits, such as $^{40}\mathrm{Ca}^{+}$ ground state $\mathrm{S}_{1/2}$ and the excited state $\mathrm{D}_{5/2}$ [26]. (b) Using the Zeeman effect energy levels or hyperfine structure energy levels of the electronic ground state as the two-level system of the qubit [27], which has a considerable advantage in terms of lifetime.

Take the trapped $^{40}\mathrm{Ca}^{+}$ to illustrate our point. The eigenstates in the $S_z$ direction of the ground state $\mathrm{S}_{1/2}$ and the excited state $\mathrm{D}_{5/2}$ are taken as the qubits $|0\rangle$ and $|1\rangle$. The interaction Hamiltonian between the spin magnetic moment and the magnetic field is $H_I = -\vec{\mu}\cdot B$. Here, the electron's spin magnetic moment $\mu = \mu_m \cdot \frac{\vec{\sigma}}{2}$, the magnetic field $B$ is selected from the $x$-axis $B = B_0 x \cos\left(k_z z - \omega t + \varphi\right)$, $z = z_0\left(a^{\dagger} + a\right)$ describes the creation and annihilation of a phonon, $z_0 = \sqrt{\hbar/\left(2m\omega_t\right)}$ is the spatial extension of ion's ground state wave function in the harmonic oscillator, $\eta = k_z z_0$ is the Lamb-Dicke parameter, and Rabi oscillation frequency $\Omega = -\mu_m B_0/2\hbar$. Then the interaction Hamiltonian can be reduced to the following form [17],

$$
\begin{aligned}
H_I &= -\mu_m \frac{\vec{\sigma}}{2} \cdot B_0 \hat{x} \cdot \cos\left[k_z z_0\left(a^{\dagger}+a\right) - \omega t + \varphi\right] \\
&= \frac{\Omega\hbar}{2} \cdot \left(\sigma_+ + \sigma_-\right)\left\{\cos\left[\eta\left(a^{\dagger}+a\right)\right]\cos(\omega t-\varphi) + \sin\left[\eta\left(a^{\dagger}+a\right)\right]\sin(\omega t-\varphi)\right\}. \quad (3)
\end{aligned}
$$

Using the Lamb-Dicke approximation $\eta\sqrt{\left\langle\left(a^\dagger + a\right)^2\right\rangle} \ll 1$, then keeping the first order of Taylor expansion of the sine and cosine function, and taking the rotation wave approximation, one can obtain

$$H_I \approx \frac{\Omega\hbar}{4}\cdot\left[\sigma_+ e^{i(\varphi-\omega t)} + \sigma_- e^{i(\omega t-\varphi)}\right] + \frac{i\eta\Omega\hbar}{4}\left(\sigma_+ + \sigma_-\right)\left(a^\dagger + a\right)\left[e^{i(-\omega t+\varphi)} - e^{i(\omega t-\varphi)}\right]. \quad (4)$$

The first polynomial describes the change of the spin state, and the spin isn't entangled with the harmonic oscillator. The second polynomial is a coupling term of spin and harmonic oscillator, describes the mode of the sideband transition. One can find that the first term corresponds to a single qubit operation, and the second term related to a two-qubit operation. The difference between these two are the coefficient $\eta$, and the different Rabi frequencies of sideband transition and the carrier transition(the former is smaller than the latter). Therefore, it is easy to find that the time limit of a two-qubit gate is longer than that of a single-qubit gate when the same calculation is carried out.

For simplicity, let us consider the Hamiltonian of a single qubit operation in the following. In the interaction picture, this item can be simplified when the free Hamiltonian $H_0$ is set as the reference system, but also can be ignored when considering single-qubit operation. By setting the external magnetic field oscillation frequency $\omega$ be the spin frequency $\omega_0$, detuning between spin and harmonic oscillator becomes 0, only the spin energy level changes. In this way, the Hamiltonian can be rewritten as

$$H_I = \frac{\Omega\hbar}{4}\cdot\left(\sigma_+ e^{i\varphi} + \sigma_- e^{-i\varphi}\right). \quad (5)$$

According to $H_I$, one can get the standard deviation of energy in the initial state

$$\Delta E_0 = \sqrt{\left\langle 0\left|(H_I)^2\right|0\right\rangle - \left(\langle 0\,|H_I|\,0\rangle\right)^2}. \quad (6)$$

Recall that $\sigma_x|0\rangle = |1\rangle$, $\sigma_x|1\rangle = |0\rangle$, $\sigma_y|0\rangle = i|1\rangle$ and $\sigma_y|1\rangle = -i|0\rangle$, and one can get

$$\Delta E_0 = \sqrt{\left\langle 0\left|\frac{\Omega\hbar}{2}\left(\cos\varphi\cdot\sigma_x - \sin\varphi\cdot\sigma_y\right)^2\right|0\right\rangle - \left[\left\langle 0\left|\frac{\Omega\hbar}{2}\left(\cos\varphi\cdot\sigma_x - \sin\varphi\cdot\sigma_y\right)\right|0\right\rangle\right]^2} \quad (7)$$

Combining the Eqs. (2) and (7), one can obtain the time limit $\tau_{\text{ort}}$ for the initial state to evolve to its orthogonal state through a single-qubit operation in the trapped ion system,

$$\tau_{ort} = \frac{\hbar}{\Delta E_0}\cdot\arccos(\langle 0|1\rangle) = \frac{\pi}{\Omega} = \frac{1}{2}T_{\text{Rabi}}. \quad (8)$$

It can be seen that the time boundary in Eq. (8) is inversely proportional to the Rabi frequency. The Rabi oscillation period between the $\text{S}_{1/2} - \text{D}_{5/2}$ of $^{40}\text{Ca}^+$ is about 11 $\mu s$ [28], so we can know that the theoretical time for a single-qubit operation of the quantum computing of the trapped $^{40}\text{Ca}^+$ system is $\frac{1}{2}T_{Rabi}$, which is about 5.5 $\mu s$. The Rabi oscillation period of IonQ's $^{171}\text{Yb}^+$ system is 12.0 $\mu s$, which is about equivalent to that of $^{40}\text{Ca}^+$ [27].

Normally, the operation speed of a single-qubit gate is about 10 times faster than that of a two-qubit gate [28]. We just assume that the completion of the algorithm is all built by single-qubit gates, so the estimated time is lower than that needed. The single-qubit flippng time calculated from the time evolution limit is consistent with the half Rabi oscillation period needed to control the bit flipping in experiments, which is corroborative evidence with each other. With single operation time, we can now list the time cost of different numbers of operations.

Table 1 shows the change in the total time consumed as the number of quantum operations increases. We can see that at $2^{50}$ times, the shortest time for serial operation is about

**Table 1** The number of operations and the corresponding time overhead

| Number of operations | Total duration T |
|---|---|
| $2^{10}$ | $5.632 \times 10^{-3} s$ |
| $2^{20}$ | $5.767 s$ |
| $2^{30}$ | $5.905 \times 10^{3} s$ $(1.64 h)$ |
| $2^{40}$ | $6.047 \times 10^{6} s$ $(69.98 days)$ |
| $2^{50}$ | $6.192 \times 10^{9} s$ $(196.342 years)$ |

200 years, which is an unacceptable range for cracking RSA public key using quantum computing when considering quantum decoherence. And the validity time of highly confidential information needs to reach 50 or even 100 years, which is the time corresponding to $2^{48}$ and $2^{49}$ operations. For practical quantum computers, more than 100 years of computing time means they are completely decoherent before obtaining correct results. Even if the decoherence does not occur due to perfect error-correction codes (the cracking time will significantly increased when running error-correcting codes), the cracking time of 50 years or more is enough safe for commercial applications.

Then, we may find $n^3 \simeq 2^{48}$, roughly estimate that $n \sim 2^{16}$, which is about 8 KB for public key length. Under the current public key system, the KB-level public key length is not yet universal, but it can also be applied in some high security areas. In the future, the computing and storage capabilities will continue to increase, and the RSA public key length may really be completely acceptable in the KB level.

## 4 Discussion

*Quantum error correction.* The aforementioned complexity and time overhead have not taken into account the cost of error correction. The actual circuits construction and physical implementation need to build physical qubits into abstract qubits (fault-tolerant qubits) to ensure the complete operation of the algorithm. There are many types of quantum error correction schemes [17]. As the circuit complexity increases, the error correction capability also needs to be improved. When considering the necessity of quantum error correction in practical system, the RSA public key cryptosystem will be more robust against quantum computing attacks.

Surface code is a widely used error correction scheme up to now. If we use the same scheme as that in [25, 29] to estimate the time overhead including error correction, each Toffoli gate consists of 7 $\hat{T}_L$ non-Clifford gates in a 3-1-3 serial structure (3 means three gates are parallel), the time complexity of the whole circuit will be tripled. In the system of superconducting quantum computing, the operation time $t$ of the single-qubit gate is about 10 ns, and the cycle time of each surface code is about 100 ns [30]. If the same error correction scheme is adopted, the surface code cycle time of the ion trap system is estimated to be 50 $\mu s$ with the single qubit operation time of the ion trap about 5 $\mu s$. Therefore, the total circuit time $T$ with error correction is about 30 times than the previous result (the serial complexity of the circuit becomes 3 times, and the single operation time with error correction is 10 times.). If we consider it approximately 30 times, this increase of time cost reduces the safe number for RSA to about 2.57 KB. Our estimate with error correction may be rather rough, more detailed calculation of surface code error correction can be referred to [30]).

*Complexity.* To evaluate a quantum algorithm, we need to investigate both its time and space complexity. Fowler [30] listed time and space complexities of the different Shor's algorithm implementations, which differ in circuits depth and number of qubits required. As the number of qubits used increases, more parallel operations can be performed. The parallel schemes reduce the time complexity of Shor's algorithm, which is less than the complexity $O(n^3)$ used in this paper. However, the required qubits of these schemes increase exponentially. For example, the parallel scheme used in [19] reduces the time complexity of Shor's algorithm to the order of $O(\log^3 n)$, but increases the space complexity **from $O(n)$ to $O(n^3)$.** As a result, the spacetime volume of the circuits doesn't decrease.

If $n$ equals 2048, then $O(n^3)$ will be $2^{33}$ (1 GB logical qubits). However, when $n$ grows to the order of 8 KB (our result above) magnitude, the space complexity will reach approximately $2^{48}$, which is $2.56 \cdot 10^{14}$ qubits (32 TB). That requires a quantum computer to have at least 32 terabytes of memory, which is not achievable easily. So the parallel scheme is currently not a high priority.

In Google scheme [31], they estimates that 22 million physical qubits are needed, which are 14,238 logical qubits, corresponding to 1.8 KB of qubits memory. When $n$ reaches the magnitude of tens of KB, the required memory is approximately $0.2 \sim 1$ MB. The number of qubits required in their scheme is already considerable, but it is still negligible compared with the parallel scheme.

Besides requiring a large amount of qubits memory, the parallel scheme has a limitation in circuit structure. The circuit architecture of the $O(\log^3 n)$ scheme is AC architecture, while the $O(n^3)$ scheme is NTC architecture [32]. The difference between them is that the AC architecture is fully connected, and the NTC architecture is a neighbor-only interaction circuit model. In AC architecture, the quantum gate must be able to be constructed between two qubits with long distance, and no penalty. It does not support arbitrary control strings on control operations, only Toffoli gates with two ones as control. The NTC architecture does not support Toffoli gates, but only two-qubit gates.

Fully connected architecture allows multi-qubit gates to be built over long distance, such as Toffoli gates, which can be constructed directly. In NTC architecture, these gates need to be decomposed into adjacent single-qubit and two-qubit gates. As the number of qubits increases, the AC structure will be more and more difficult to be realized experimentally. Because multi-qubit gates are the operations between qubits through the coupling of external fields or their own interaction essentially. The precise control of long-distance coupling will become more and more difficult when circuit qubits increase. That is the reason why we mainly consider the NTC architecture scheme with time complexity of $O(n^3)$.

*Feasibility.* The most time-consuming part of running Shor's factoring algorithm is modular exponentiations, while modular exponentiations can be performed quickly in modern electronic computers. This makes it possible to ensure security of the RSA cryptography against quantum computing attacks by increasing the length of the key. In principle, the length of the RSA public key can be infinitely increased, so that the cracking time by quantum computing becomes unbearable. In practice, the key system serves daily information communication, and the time for encryption and decryption must be within an acceptable range to be reasonable. The currently widely used RSA public key length is 2048-bit, which is 256 B. The encryption and decryption of the 8 KB key can be completed in a few minutes, which is completely acceptable. Furthermore, hundreds KB key length may be chosen to ensure the security. Although encryption and decryption time is too long for instant secure communication with the key length increasing, it can be applied to distribute secure key bits that can be used as symmetric key later.

*Optimum.* In our calculations, we did not optimize the algorithm, but used the original Shor's algorithm. Gidney etc. [31] discussed the crack of the 2048-bit RSA takes about 7 hours to run the quantum part of the algorithm. Compared with the ion trap systems, the superconducting quantum computing system may have a shorter quantum operation time due to its adjustable, e.g., maybe 1000 times faster. In practice, different systems have different advantages and disadvantages. The superconducting qubit is an artificial atom, whose preparation and calculation fidelity is not as good as that of the natural atoms in the trapped ion system, which will cost more quantum resources in initialization and error correction. Based on the conclusion that cracking 2048-bit RSA costs 7 hours in the superconducting quantum computing system, the key length of RSA for 100 years information security is at least 16 KB, i.e., $\sqrt[3]{100 \cdot 365 \cdot 24 \div 7} \times 2^{11} \approx 2^{17} = 16$ KB.

At the same time, our estimation doesn't consider the construction and simulation of algorithm circuits in detail, we only give estimates on the order of magnitude. The time overhead can be reduced by several times or even tens of times by optimizing the algorithm, but there can be no substantial reduction. And definitely, the reduction cannot resist the increase of the key length.

*Decoherence.* The biggest obstacle to manufacturing quantum computers is how to maintain quantum coherence for an enough long time. The task must be completed before the decoherence occurs, otherwise the task fails. In order to overcome the occurrence of decoherence, it is necessary to use quantum error-correction codes in quantum computation. However, even if quantum error-correction codes are applied, it is impossible for any quantum computer to maintain the coherence time for more than 50 years in practice when considered time-energy uncertainty relation.[1] Therefore, more than 50 years cracking time of RSA with 8 KB key length is enough safe against quantum computing attacks.

## 5 Conclusion

By exploring the time overhead of the Shor's algorithm in the trapped ion quantum computing systems, we have evaluated the practical security of the RSA public key cryptosystem. Based on our calculations, we can speculate that, even if a universal quantum computer with NTC architecture can be successfully built in the future, with the length of the RSA public key increased to the order of KB, the actual cracking time will also become unbearable. The limit of the public key length will fluctuate due to factors such as different quantum computing models and the optimized implementation of Shor's algorithm, but this proposal will undoubtedly provide an avenue towards keeping information confidential against quantum computing attacks. Since RSA public key cryptosystem is currently widely used, an slightly improved RSA scheme against quantum computing attacks is clearly the most economical cryptographic scheme in the coming era of quantum computing.

[1] The energy-time uncertainty relation indicates that the lifetime of excited states is limited. The lifetime of metastable of atoms may be millisecond class, but it is so far from 50 years. So, 50 years cracking time is enough safe for some commercial applications of RSA. For a superconducting quantum computing system, quantum coherence can also maintain with millisecond class. A detailed calculation about the limit life of quantum coherence for quantum superconducting systems will be presented in the future.

## Appendix: Modular Exponentiation

The biggest circuit cost in implementing the Shor's algorithm is to calculate the modular exponentiation $|a^x \pmod N\rangle$. The algorithm for performing modular exponentiation in classic circuits is mature, which takes less than one second to calculate the modular exponentiation of thousands of bits. However, the difficulty in implementing modular exponentiation in the Shor's algorithm depends on the superposition of exponents, which requires quantum circuits and qubits to implement operations such as calculation and memory. This is also the focus of our work. When the same modular exponentiation operation is moved from classical computers to the quantum, the circuit cost and time overhead consumed must be completely different.

The calculation of the modular exponentiation is usually divided into two steps. First, binarize the exponent, and calculate the exponent of each bit separately, and then multiply these result. Specifically:

1. The exponent $x = x_t 2^{t-1} \cdot x_{t-1} 2^{t-2} \cdot \ldots \cdot x_1 2^0,\ t \sim N$. For the $j$-th exponent operation, the result can be obtained by continuously squaring and modulo multiplication, squaring $x \pmod N$ to get $x^2 \pmod N$, squaring to get $x^4 \pmod N$, and multiplying $x \pmod N$ to get $x^5 \pmod N$, and so on. So the number of overall multiplication operations is on the order of $O(N)$, the complexity of the multiplication is $O(N^2)$, and the total overhead is on the order of $O(N^3)$.
2. $a^x \pmod N = \left(a^{x_t 2^{t-1}} \pmod N\right)\left(a^{x_{t-1} 2^{t-2}} \pmod N\right) \cdots \left(a^{x_1 2^0} \pmod N\right)$. With the result of the modulo exponent of each bit, the modulo multiplication operation requires a total of $O(N^3)$ operations.

Therefore, the total cost of the modular exponentiation operations is on the order of $O(N^3)$. But it is only an estimate of the modular exponentiation algorithm in the classic circuit. If it is applied to a fully reversible quantum circuit, there will be some limitations. Vedral et al. [25] studied quantum circuit constructed for modular addition, modular multiplication, and modular exponentiation operations with a little bits. The conclusion shows that the circuit cost of modular multiplication operations is indeed of the order of $O(N^3)$. But from all the construction of modular addition, modular multiplication and modular exponent, the number of basic gates of those three-packed arithmetic unit has a constant coefficient, which makes the coefficient before the final $N^3$ item reach hundreds. Although there must be some more simplified schemes for building modular exponentiation quantum circuits, the circuit construction will become more complicated as the number of $N$ bits increases. And the influence of the coefficients before the $N^3$ item will become smaller. Just as has been reduced to 0.3 [31], which might be the smallest complexity at present, it won't produce an essential effect on the issues concerned in this paper.

**Acknowledgements** We thank Guoan Yan and Yitian Wang for fruitful discussions. This work was supported by National Natural Science Foundation of China under Grant No. 11725524.

**Author Contributions** Q.-y.C. conceived this project. K.L. mainly did the calculations. Both authors wrote the manuscript.

## Declarations

**Competing interests** The authors declare that they have no conflict of interest.

## References

1. Benioff, P.: The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. J. Stat. Phys. **22**(5), 563–591 (1980)
2. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6), 467–488 (1982)
3. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science, pp. 124-134, Ieee (1994)
4. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**(2), 303–332 (1999)
5. Monroe, C., Meekhof, D.M., King, B.E., et al.: Demonstration of a fundamental quantum logic gate. Phys. Rev. Lett. **75**(25), 4714 (1995)
6. Cirac, J.I., Zoller, P.: Quantum computations with cold trapped ions. Phys. Rev. Lett. **74**(20), 4091 (1995)
7. Blatt, R., Wineland, D.: Entangled states of trapped atomic ions. Nature **453**(7198), 1008 (2008)
8. Gottesman, D., Kitaev, A., Preskill, J.: Encoding a qubit in an oscillator. Phys. Rev. A **64**(1), 012310 (2001)
9. Kok, P., Munro, W.J., Nemoto, K., et al.: Milburn. Linear optical quantum computing with photonic qubits. Rev. Mod. Phys. **79**(1), 135 (2007)
10. Li, X.Q., Wu, Y.W., Steel, D., et al.: An all-optical quantum gate in a semiconductor quantum dot. Science **301**(5634), 809–811 (2003)
11. Petta, J.R., Johnson, A.C., Taylor, J.M., et al.: Coherent manipulation of coupled electron spins in semiconductor quantum dots. Science **309**(5744), 2180–2184 (2005)
12. DiCarlo, L., Chow, J.M., Gambetta, J.M., et al.: Demonstration of two-qubit algorithms with a superconducting quantum processor. Nature **460**(7252), 240–244 (2009)
13. Arute, F., Arya, K., Babbush, R., et al.: Quantum supremacy using a programmable superconducting processor. Nature **574**(7779), 505–510 (2019)
14. Nam, Y.S., Chen, J.S., Pisenti, N.C., et al.: Ground-state energy estimation of the water molecule on a trapped ion quantum computer. npj Quantum Inf. **6**, 33 (2020)
15. Wright, K., Beck, K.M., Debnath, S., et al.: Benchmarking an 11-qubit quantum computer. Nat. Commun. **10**, 5464 (2019)
16. Bernstein, D.J., Heninger, N., Lou, P., et al.: Post-quantum RSA. In: International Work-shop on Post-Quantum Cryptography, pp. 311-329. Springer (2017)
17. Nielsen, M.A., Chuang, I.: Quantum computation and quantum information (2002)
18. Cleve, R., Watrous, J.: Fast parallel circuits for the quantum Fourier transform. In: Proceedings 41st Annual Symposium on Foundations of Computer Science, pp. 526-536, IEEE (2000)
19. Meter, R.V., Itoh, K.M., Ladd, T.D.: Architecture-dependent execution time of Shor's algorithm Controllable Quantum States. pp. 183–188, World Scientific (2008)
20. Anandan, J., Aharonov, Y.: Geometry of quantum evolution. Phys. Rev. Lett. **65**(14), 1697 (1990)
21. Margolus, N., Levitin, L.B.: The maximum speed of dynamical evolution. Physica D: Nonlinear Phenomena **120**(1-2), 188–195 (1998)
22. Caneva, T., Murphy, M., Calarco, T., et al.: Optimal control at the quantum speed limit. Phys. Rev. Lett. **103**(24), 240501 (2009)
23. Levitin, L.B., Toffoli, T.: Fundamental limit on the rate of quantum dynamics: the unified bound is tight. Phys. Rev. Lett. **103**(16), 160502 (2009)
24. Aharonov, Y., Bohm, D.: Time in the quantum theory and the uncertainty relation for time and energy. Phys. Rev. **122**(5), 1649 (1961)
25. Vedral, V., Barenco, A., Ekert, A.: Quantum networks for elementary arithmetic operations. Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Phys. Rev. A **54**(1), 147 (1996)
26. Gulde, S., Häffner, H., Riebe, M., et al.: Quantum information processing with trapped ca$^+$ ions. Philosophical Transactions of the Royal Society of London. Series a: Mathematical. Phys. Eng. Sci. **361**(1808), 1363–1374 (2003)

27. Olmschenk, S., Younge, K.C., Moehring, D.L., et al.: Manipulation and detection of a trapped Yb$^+$ hyperfine qubit. Phys. Rev. A **76**(5), 052314 (2007)
28. Häffner, H., Roos, C.F., Blatt, R.: Quantum computing with trapped ions. Phys. Rep. **469**(4), 155–203 (2008)
29. Cuccaro, S.A., Draper, T.G., Kutin, S.A., et al.: arXiv:quant-ph/0410184
30. Fowler, A.G., Mariantoni, M., Martinis, J.M., et al.: Surface codes: Towards practical large-scale quantum computation, vol. 86 (2012)
31. Gidney, C., Ekerå, M.: How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. arXiv:1905.09749 (2019)
32. Meter, R.V., Itoh, K.M.: Fast quantum modular exponentiation. Phys. Rev. A **71**(5), 052320 (2005)