The decomposition of RSA public key and decryption method and system

Abstract

The invention discloses a kind of decomposition of RSA public key and decryption method and system, wherein RSA public key decomposition method includes: that (1) obtains RSA public key n；(2) prime factor pair for being less than or equal to n/3 is obtained<p,q>, and according to the prime factor pair<p,q>corresponding two-dimentional Hermitian matrix is formed with public key n, the additional electromagnetic field for controlling quantized system simultaneously, makes the Hamiltonian of the quantized system two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix whether at x=0, if it was not then to other prime factors pair<p,q>judged, if determining the prime factor pair<p,q>for two prime factors obtained after being decomposed to RSA public key n, exported.The present invention calculating time is few, and required stored bits number is few, and efficiency of algorithm is high, and stability is good.

CN109450634A
China

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: 于扬, 谭新生, 于海峰, 陶先平

Worldwide applications

2018 • CN

Application CN201811213095.XA events

2018-10-18 • Application filed by 南京大学

2018-10-18 • Priority to CN201811213095.XA

2019-03-08 • Publication of CN109450634A

Info: Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (6)

Hide Dependent

1. a kind of RSA public key decomposition method, it is characterised in that this method comprises:

(1) RSA public key n is obtained；

(2) prime factor pair for being less than or equal to n/3 is obtained<p,q>, and according to the prime factor pair<p,q>it is formed pair with public key n The two-dimentional Hermitian matrix answered, while the additional electromagnetic field of quantized system is controlled, make the Hamiltonian of quantized system two dimension strategic point Close matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix whether at x=0, if it was not then to it His prime factor pair<p,q>judged, if determining the prime factor pair<p,q>for after being decomposed to RSA public key n Two prime factors arrived, are exported.

2. RSA public key decomposition method according to claim 1, it is characterised in that: step (2) specifically includes:

(2.1) prime factor pair is set<p,q>initial value be<3,3>；

(2.2) judge whether p is less than or equal to n/3, if so, (2.3) are executed, if it is not, then determining that current RSA public key n can not divide Solution terminates；

(2.3) according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

(2.4) additional electromagnetic field for controlling quantized system, makes the Hamiltonian of the quantized system two dimension Hermitian matrix, and measure Whether quantized system power spectrum sees the characteristic value of the two dimension Hermitian matrix at x=0；

(2.5) it if not existing, executes (2.6)； If judging whether n=pq is true, determining prime factor pair if setting up<p,q> Current value be two prime factors obtained after being decomposed to RSA public key n, exported, if not, execute (2.6)；

(2.6) by q=q+1, and judge whether q is less than or equal to n/3, (2.3) are executed if so, returning, if it is not, then executing (2.7)；

(2.7) by p=p+1, and execution (2.2) are returned to.

3. a kind of RSA public key decomposing system, characterized by comprising:

Public key acquisition module, for obtaining RSA public key n；

Public key decomposing module, for obtaining the prime factor pair for being less than or equal to n/3<p,q>, and according to the prime factor pair<p,q> Corresponding two-dimentional Hermitian matrix is formed with public key n, while controlling the additional electromagnetic field of quantized system, makes the Hamilton of quantized system Amount is the two dimension Hermitian matrix, and measure quantized system power spectrum see the characteristic value of the two dimension Hermitian matrix whether at x=0, such as Fruit does not exist, then to other prime factors pair<p,q>judged, if determining the prime factor pair<p,q>for to RSA public key n Two prime factors obtained after being decomposed, are exported.

4. RSA public key decomposing system according to claim 3, it is characterised in that: the public key decomposing module specifically includes:

Initial value setup unit, for prime factor pair to be arranged<p,q>initial value be<3,3>；

P value judging unit, for judging whether p is less than or equal to n/3, if so, executing two-dimentional Hermitian matrix forms unit, if It is no, then determine that current RSA public key n can not be decomposed, terminates；

Two-dimentional Hermitian matrix forms unit, according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

Quantized system spectroscopy detection module makes the Hamiltonian of quantized system for controlling the additional electromagnetic field of quantized system The two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix whether at x=0； If not existing, Q value updating unit is executed, if executing prime factor judging unit；

Prime factor judging unit determines prime factor pair if setting up for judging whether n=pq is true<p,q>current value be Two prime factors obtained after decomposing to RSA public key n, are exported, if not, execute q value updating unit；

Q value updating unit is used for q=q+1, and judges whether q is less than or equal to n/3, executes two-dimentional Hermit square if so, returning Formation is at unit, if it is not, then executing p value updating unit；

P value updating unit is used for p=p+1, and is returned and executed p value judging unit.

5. a kind of RSA decryption method, it is characterised in that this method comprises:

(1) RSA public key n is decomposed using claim 1 the method, obtains two prime factors p, q；

(2) private key d is calculated according to the prime factor p, q in the following ways:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

(3) ciphertext data C to be decrypted is obtained, and following formula is used to decrypt ciphertext data C for clear data M:

$M=C^{d}modn$。

6. a kind of RSA decryption system, characterized by comprising:

RSA public key decomposing system as claimed in claim 3 obtains two prime factors p, q for decomposing to RSA public key n；

Private key computing module, for private key d to be calculated in the following ways according to the prime factor p, q:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

Data decryption module for obtaining ciphertext data C to be decrypted, and uses following formula to decrypt ciphertext data C to be bright Literary data M:

$M=C^{d}modn$。

Description

The decomposition of RSA public key and decryption method and system

Technical field

The present invention relates to information security field more particularly to a kind of RSA public key decomposition method and system and it is based on RSA public key The decryption method and system of decomposition.

Background technique

RSA public key encryption system is the great infrastructure that advanced information society carries out security assurance information.The body Lie in 1978 by Peter Lonard Lee Vista (Ron Rivest), A Di Shamir (Adi Shamir) and Leonard Ah [1] that De Man (Leonard Adleman) is proposed together.It is a kind of asymmetric-key encryption system.As shown in table 1, base Present principles are to appoint to take two Big primes p, q, calculate n=pq.Then optional one and (p-1) (q-1) relatively prime small odd number e, with (e, n) is that public key main body is externally issued.Meanwhile the inverse element d of e is calculated in (p-1) (q-1) multiplicative group, with (d, n) for private key master The keeping of body secret.The a pair of secret keys can carry out two-way encryption and decryption.Under this theoretical frame, if it is possible to easily from public key N (public key in this specification is uniformly interpreted as n) in obtain p and q, can also crack out d (this explanation in private key easily Private key in book is uniformly interpreted as d).It is obvious, it is that two prime factors p, q become RSA system reliability by public key inverse decomposition It is crucial.Although number theory research field, by feasible in classical number theory calculating completion public key resolution theory, because its calculation amount is huge It can not be completed in classic computer in reality greatly.

Table 1

At present classic computer use public key prime factorization method still rest on exhaustive trying division method [2] (although Some mutation, but rudimentary algorithm method remains the method for exhaustion): public key to be decomposed is removed with different prime numbers, it must if divided exactly To answer." detection " number of obvious this method becomes larger with the gradually big of public key to be decomposed.If being with public key n to be decomposed The progressive index of Algorithms T-cbmplexity analysis, the current getable best general number field screening method (General of classic algorithm of institute Number Field Sieve) Complexity classes be O (exp $((logN)^{1/3}(loglogN)^{2/3})$) [2,3].As can be seen that calculating Complexity it is in exponential increase.There is data to suggest that RSA-768 (the big number that a binary representation length is 768) is decomposed, The time [4] in 2000 is needed in one-of-a-kind system most fast at present.And the usual key length of RSA system run at present be two into 1024 in representation processed.This makes RSA system from being born 1978, is gradually received by people and becomes world wide The great infrastructure of interior information security escorts for mankind's civilization.But we are also undeniable to be: pacifying in information Full field, researcher attempting to find new decomposition method or new calculation method always to obtain private key crack it is prominent It is broken, and attempt to establish new security system.

In terms of novel computing platform and computation model, the appearance of quantum calculation brings RSA Public Key Infrastructure to us and breaks A possibility that solution [5].The superimposed characteristics of quantum bit can support 0 and 1 two state of a quantum bit while storage, if It is a N quantum-bit systems, then the system can store 2N data simultaneously.And from the point of view of calculating, quantum computer The 2N data can be manipulated simultaneously in once-through operation, the effect 2N classic computer that can compare carries out at the same time It is primary to calculate.This natural concurrency brings brilliant speed advantage [5,6] to quantum calculation.On this basis, 1994 Year, MIT applied mathematics system professor Peter Williston Shor proposes the Shor quantum that can be used for public key prime factorization Algorithm [7,8].Public key N prime factorization problem is changed into find a period of a function problem first by this method, is then utilized Quantum Fourier transform in quantized system searches this period of a function.Shor algorithm really can be in the multinomial of N The interior decomposition for completing a public key.The quantum bit number for the interaction that the algorithm needs is about n ≈ log2N, and The public key that theoretically a 512 quantum bit computers can complete 1024 bit lengths in 1 second cracks.But it is measured now Sub- mechanics forefront, best quantum chip operation is under best performance, and the quantity and control precision of quantum bit are much It does not reach requirement, therefore can't see the possibility of realization.Disclosed document report is 2001, and a computer MSR Information system of IBM passes through Experimental verification Shor algorithm can resolve into 3 × 5 for 15.In conclusion on the basis of quantum calculation basic principle, breakthrough amount The working performance of sub- chip simultaneously attempts new calculation method, becomes the focus of current RSA public key prime factorization.

Summary of the invention

Goal of the invention: quantum algorithm existing quantum of the present invention for RSA public key prime factorization in the prior art Bit number requires problem too many, that quantum manipulation required precision is excessively high, provides a kind of RSA public key decomposition method and system and is based on The decryption method and system that RSA public key decomposes are based on single quantum bit system, by the way that public key N to be decomposed is carried out two dimension strategic point Close diagonalization of matrix monitors the power spectrum of quantized system, the technological means such as 0 characteristic value of diagonal matrix solves, complete the matter of public key N because Son decomposes.The present invention and classic algorithm compare, and are a kind of prime factorization method based on single quantum bit, required calculating time Few, required stored bits number is few, and efficiency of algorithm is high, and stability is good.

Technical solution: RSA public key decomposition method of the present invention includes:

(1) RSA public key n is obtained；

(2) prime factor pair for being less than or equal to n/3 is obtained<p,q>, and according to the prime factor pair<p,q>with public key n shape At corresponding two-dimentional Hermitian matrix, while controlling the additional electromagnetic field of quantized system, make quantized system Hamiltonian this two Tie up Hermitian matrix, and measure quantized system power spectrum see the characteristic value of the two dimension Hermitian matrix whether at x=0, if it was not then To other prime factors pair<p,q>judged, if determining the prime factor pair<p,q>to be decomposed to RSA public key n Two prime factors obtained afterwards, are exported.

Further, above-mentioned steps (2) specifically include:

(2.1) prime factor pair is set<p,q>initial value be<3,3>；

(2.2) judge whether p is less than or equal to n/3, if so, execute (2.3), if it is not, then determine current RSA public key n without Method is decomposed, and is terminated；

(2.3) according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

(2.4) additional electromagnetic field for controlling quantized system, makes the Hamiltonian of the quantized system two dimension Hermitian matrix, and Whether measurement quantized system power spectrum sees the characteristic value of the two dimension Hermitian matrix at x=0；

(2.5) it if not existing, executes (2.6)； If, judge whether n=pq true, if set up if determine prime factor to < P, q > current value be two prime factors obtained after being decomposed to RSA public key n, exported, if not, execute (2.6)；

(2.6) by q=q+1, and judge whether q is less than or equal to n/3, (2.3) are executed if so, returning, if it is not, then executing (2.7)；

(2.7) by p=p+1, and execution (2.2) are returned to.

RSA public key decomposing system of the present invention includes:

Public key acquisition module, for obtaining RSA public key n；

Public key decomposing module, for obtaining the prime factor pair for being less than or equal to n/3<p,q>, and according to the prime factor pair< P, q > and public key n form corresponding two-dimentional Hermitian matrix, while controlling the additional electromagnetic field of quantized system, make the Kazakhstan of quantized system Whether close amount is the two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix in x=0 Place, if it was not then to other prime factors pair<p,q>judged, if determining the prime factor pair<p,q>for to RSA Two prime factors that public key n is obtained after being decomposed, are exported.

Further, the public key decomposing module specifically includes:

Initial value setup unit, for prime factor pair to be arranged<p,q>initial value be<3,3>；

P value judging unit, for judging whether p is less than or equal to n/3, if so, executing two-dimentional Hermitian matrix forms unit, If it is not, then determining that current RSA public key n can not be decomposed, terminate；

Two-dimentional Hermitian matrix forms unit, according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

Quantized system spectroscopy detection module makes the Hamilton of quantized system for controlling the additional electromagnetic field of quantized system Whether amount is the two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix at x=0； If Do not exist, execute q value updating unit, if executing prime factor judging unit；

Prime factor judging unit determines prime factor pair if setting up for judging whether n=pq is true<p,q>it is current Value is two prime factors obtained after decomposing to RSA public key n, is exported, if not, execute q value updating unit；

Q value updating unit is used for q=q+1, and judges whether q is less than or equal to n/3, executes two dimension strategic point if so, returning Close matrix forms unit, if it is not, then executing p value updating unit；

P value updating unit is used for p=p+1, and is returned and executed p value judging unit.

RSA decryption method of the present invention includes:

(1) RSA public key n is decomposed using above-mentioned RSA public key decomposition method, obtains two prime factors p, q；

(2) private key d is calculated according to the prime factor p, q in the following ways:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

(3) ciphertext data C to be decrypted is obtained, and following formula is used to decrypt ciphertext data C for clear data M:

$M=C^{d}$ modn。

RSA decryption system of the present invention includes:

Above-mentioned RSA public key decomposing system obtains two prime factors p, q for decomposing to RSA public key n；

Private key computing module, for private key d to be calculated in the following ways according to the prime factor p, q:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

Data decryption module is decrypted ciphertext data C for obtaining ciphertext data C to be decrypted, and using following formula For clear data M:

$M=C^{d}$ modn。

Key point of the invention is using public key to be decomposed and to attempt prime factor as matrix element, then establishes quantum system System, using the characteristic value of quantum bit detection matrix, to carry out the prime factorization of RSA public key.Matter of the present invention public key Factorization and quantum detection combine and the prior art is entirely different.

It first decomposes screening technique with classical big number by of the invention and compares.Screening method is normally discussed based on classic computer sum number , it usually selects different numbers to remove public key to be decomposed, needs classical CPU to do trial division operation always, at the optimization of algorithm Reason gives a public key n, decomposes expense and is increased with the exponential form of n, can not be practical.And this programme is to be based on quantum theory, It is completed in quantum computing systems, two different number p, q is enumerated in 3-n/3, its Hermitian matrix is set, it is intrinsic to detect its Value extreme value and complete, be not required to do multiplication.Two kinds of strategies belong to entirely different theoretical model and computing system, and the present invention has day Right, essential advantage.If having to compare, gives a public key n and carry out prime factorization, classical screening method multiplication expends Time index increase, and this method be it is linearly increasing, performance is extremely superior.

The present invention and quantum algorithm are compared again.Common Shor algorithm decomposes given public key n (assuming that its binary form Show and need N) when, it is necessary first to about N number of quantum register is classified as 2 groups, and one group puts 1 to r natural number, then selects It selects one and is arbitrarily less than n and relatively prime number m, successively seek m^{r}Divided by the remainder of n, it is put into another set register.Then it carries out Measurement.In calculating process, Quantum fourier transform is carried out to first group of register and takes around N/2 single-bit logic gate of execution It is manipulated with N (N-1)/2 dibit logic gate.Index acceleration can be proved to be in Shor theory of algorithm, but at most may be used at present The controllable quantum bit number of high-precision for quantum calculation is 10 or so, and the time that quantum entanglement is kept also only has 10 microseconds, And to realize that Shor algorithm also needs redundant bit error correction, with current techniques, the number that can be decomposed can only be less than 20, substantially can not It is practical.

Finally algorithm comparison is insulated with quantum.(n-ab) is asked with quantum insulation algorithm^{2}Minimum value method decompose.Equally As n increases, quantum bit number is also linearly increasing.

And as quantum bit number increases, the control precision of quantized system must decline.This is widely present in existing each Contradiction in kind of quantized system make the existing various existing Quantum Computings that can be used for RSA public key prime factorization be difficult into Row practical application.And the present invention need to only control single quantum bit, this is that current technology can be made extraordinary.In addition, logical It crosses and continuously improves control, measurement method (these classical circuits can do better), can constantly increase to enable the public key of decomposition.

The utility model has the advantages that compared with prior art, the present invention its remarkable advantage is:

(1) present invention need to only control a quantum bit, easy to accomplish, and precision is high；

(2) present invention only needs to scan possible prime factor pair<p,q>, quantized system power spectrum is then measured, is not needed interior Portion's storage unit, therefore reduce storage unit requirement.

(3) present invention is not in oscillatory occurences, more efficient, stability is more preferable without processes such as iteration.

(4) only precision scans power spectrum to needs to the present invention as required, and public key prime factorization calculating speed has the breakthrough of matter, energy Enough progress for greatly pushing RSA public key decomposition technique promote the sound of RSA Public Key Infrastructure and develop in a healthy way, promote the information age The reliability of information security infrastructure.

Detailed description of the invention

Fig. 1 is the flow diagram of one embodiment of RSA public key decomposition method provided by the invention；

Fig. 2 is the result schematic diagram decomposed using method in Fig. 1 to public key 15；

Fig. 3 is the result schematic diagram decomposed using method in Fig. 1 to public key 35.

Specific embodiment

Embodiment 1

A kind of RSA public key decomposition method is present embodiments provided, as shown in Figure 1, including the following steps:

(1) RSA public key n is obtained；

(2) prime factor pair for being less than or equal to n/3 is obtained<p,q>, and according to the prime factor pair<p,q>with public key n shape At corresponding two-dimentional Hermitian matrix, while controlling the additional electromagnetic field of quantized system, make quantized system Hamiltonian this two Hermitian matrix is tieed up, and measures quantized system power spectrum and sees whether the characteristic value of the two dimension Hermitian matrix (experimentally shows at x=0 To there is the appearance of the maximum an of formant at 0), if it was not then to other prime factors pair<p,q>judged, if Then determining the prime factor pair<p,q>for two prime factors obtained after being decomposed to RSA public key n, exported.The step Suddenly it specifically includes:

(2.1) prime factor pair is set<p,q>initial value be<3,3>；

(2.2) judge whether p is less than or equal to n/3, if so, execute (2.3), if it is not, then determine current RSA public key n without Method is decomposed, and is terminated；

(2.3) according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

(2.4) additional electromagnetic field for controlling quantized system, makes the Hamiltonian of the quantized system two dimension Hermitian matrix, and Whether measurement quantized system power spectrum sees the characteristic value of the two dimension Hermitian matrix at x=0；

Specifically, eigenvalue of matrix x centainly meets according to the definition [1] of the characteristic value of two-dimentional Hermit diagonal matrix:

Namely: p × q- (p+q) $x+x^2$- n=0 observes the equation it can be found that if equation has the solution of x=0, also Be 0 be matrix Φ characteristic value, n=p × q, n can resolve into p and multiply q.On the other hand, in quantum binary states system, system Hamiltonian is 2 × 2 Hermitian matrixs.Different characteristic values (or energy) correspond to different eigenstates, if at the beginning of system Beginningization arrives ground state, then system can be energized into excitation eigenstate with electromagnetic field.And the frequency of electromagnetic field is exactly equal to ground state and arrives The energy difference of eigenstate, here it is RESONANCE ABSORPTIONs.General measure can not know energy difference in advance, using scanning electromagnetic field frequency, Monitor the i on population in excitation state, can see resonance absorbing peak in certain frequencies, and this i on population with frequency variation diagram just It is called power spectrum.Therefore measurement power spectrum just provides energy eigenvalues, that is, the characteristic value of matrix in fact.

(2.5) it if not existing, executes (2.6)； If, judge whether n=pq true, if set up if determine prime factor to < P, q > current value be two prime factors obtained after being decomposed to RSA public key n, exported, if not, execute (2.6)；

(2.6) by q=q+1, and judge whether q is less than or equal to n/3, (2.3) are executed if so, returning, if it is not, then executing (2.7)；

(2.7) by p=p+1, and execution (2.2) are returned to.

In addition, the measurement error of quantized system will increase with the increase of public key n to be decomposed, may have<p,q>it is right, Even if they are not the prime factors of public key N, but its Hermitian matrix characteristic value can also show to can use at this time close to extreme value 0 Inspection institute obtains as a result, excluding these puppets classic computer quickly<p,q>it is right.It macroscopically says, this method is scanning<p,q>clock synchronization, It only need to monitor whether corresponding Hermitian matrix characteristic value x extreme value 0 occurs, therefore this can be rapidly completed<p,q>pair scanning, because And<3,3>it arrives<n/3,n/3>in the range of carry out prime factor<p,q>pair exhaustive search efficiency also ensured, with this Meanwhile this method does not need memory substantially.In addition, can have a scheme advanced optimized in scanning, for example, even number and 3,5 times Number can be skipped and not scanned, to further save the time.

Experimental verification is carried out to the present embodiment below.

The present invention is based on Superconducting Quantum systems, have carried out experimental verification to RSA public key prime factorization with single quantum bit. In this quantized system, within its coherence time, superconductive quantum bit is a Two-level quantum systems.Its Hamiltonian can be with Write as [2]

Wherein H_{11}And H_{12}The mutually accurate control of microwave amplitude, frequency, position can be passed through.Specifically H_{12}Microwave amplitude is proportional to, H_{11}It is adjusted by frequency.We can also change diagonal item by choosing 0 point of different-energy.I.e. in H_{11}Upper increase is any normal Number.This can use an other additional energy as 0 point of energy, then change the energy of additional energy.It is micro- by careful design Wave amplitude, frequency, phase, the Hamiltonian of available needs:

Then the power spectrum of superconductive quantum bit is scanned, whether measuring system characteristic value is at 0 point, if in successful decomposition； Such as Fruit does not exist, and changes a, b, duplicate measurements power spectrum.To the last obtain answer.It can use simple odd number and carry out Proof-Of Principle.

1) prime factor number when n=15 decomposes: for n=15, choosing nondiagonal element $15^{1/2}$, p, q are then scanned, as a result such as Fig. 2.Trunnion axis is to change p and q respectively, and square height is i on population of the energy in 0 point of excitation state, that is, under different parameters The probability that characteristic value is 0, when p, q are 3 and 5, x=0 is in maximum, therefore prime factor is 3 and 5.

2) prime factorization when n=35: if selecting n=35, same available result p, q is 7 and 5.Fig. 3 is experiment As a result plan view.Each lattice represent a parameter combination, and the brightness of grid represents the probability for having x=0 characteristic value.It chooses different Parameter, measures the probability of the characteristic value of x=0, and size is indicated with brightness (yellow).It can be seen that brightness is most when p, q are 7 and 5 Greatly, i.e. probability highest, therefore, prime factor is 5 and 7.

Embodiment 2

Present embodiment discloses a kind of RSA public key decomposing systems, comprising:

Public key acquisition module, for obtaining RSA public key n；

Public key decomposing module, for obtaining the prime factor pair for being less than or equal to n/3<p,q>, and according to the prime factor pair< P, q > and public key n form corresponding two-dimentional Hermitian matrix, while controlling the additional electromagnetic field of quantized system, make the Kazakhstan of quantized system Whether close amount is the two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix in x=0 Place, if it was not then to other prime factors pair<p,q>judged, if determining the prime factor pair<p,q>for to RSA Two prime factors that public key n is obtained after being decomposed, are exported.

Wherein, the public key decomposing module specifically includes:

Initial value setup unit, for prime factor pair to be arranged<p,q>initial value be<3,3>；

P value judging unit, for judging whether p is less than or equal to n/3, if so, executing two-dimentional Hermitian matrix forms unit, If it is not, then determining that current RSA public key n can not be decomposed, terminate；

Two-dimentional Hermitian matrix forms unit, according to current prime factor pair<p,q>value and public key n form two-dimentional Hermitian matrix Φ:

Quantized system spectroscopy detection module makes the Hamilton of quantized system for controlling the additional electromagnetic field of quantized system Whether amount is the two dimension Hermitian matrix, and measure quantized system power spectrum and see the characteristic value of the two dimension Hermitian matrix at x=0； If Do not exist, execute q value updating unit, if executing prime factor judging unit；

Prime factor judging unit determines prime factor pair if setting up for judging whether n=pq is true<p,q>it is current Value is two prime factors obtained after decomposing to RSA public key n, is exported, if not, execute q value updating unit；

Q value updating unit is used for q=q+1, and judges whether q is less than or equal to n/3, executes two dimension strategic point if so, returning Close matrix forms unit, if it is not, then executing p value updating unit；

P value updating unit is used for p=p+1, and is returned and executed p value judging unit.

The embodiment and embodiment 1 correspond, and not detailed place please refers to embodiment 1, repeats no more.

Embodiment 3

Present embodiments provide a kind of RSA decryption method, comprising:

(1) RSA public key n is decomposed using the RSA public key decomposition method of embodiment 1, obtains two prime factors p, q；

(2) private key d is calculated according to the prime factor p, q in the following ways:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

(3) ciphertext data C to be decrypted is obtained, and following formula is used to decrypt ciphertext data C for clear data M:

$M=C^{d}$ modn。

Embodiment 4

Present embodiments provide a kind of RSA decryption system, comprising:

Above-mentioned RSA public key decomposing system obtains two prime factors p, q for decomposing to RSA public key n；

Private key computing module, for private key d to be calculated in the following ways according to the prime factor p, q:

$D=e^{-1}(mod(p-1)(q-1))$

In formula, e is the odd number relatively prime with (p-1) (q-1)；

Data decryption module is decrypted ciphertext data C for obtaining ciphertext data C to be decrypted, and using following formula For clear data M:

$M=C^{d}$ modn。

The present embodiment and embodiment 3 correspond, and not detailed place please refers to embodiment 3, repeats no more.

The above disclosure is only the preferred embodiments of the present invention, and the scope of the invention cannot be limited thereby, Therefore equivalent changes made in accordance with the claims of the present invention, are still within the scope of the present invention.

Bibliography:

1.L.Adleman,R.Rivest,The use of public key cryptography in communication system design,IEEE Communications Society Magazine 16,20–23 (1978).

2.J.M.Pollard,Theorems on factorization and primality testing, Proceedings of the Cambridge Philosophical Society 76,521-228(1974).

3.K.Bimpikis,R.Jaiswal,Modern Factoring Algorithms,a Technical Report Presented to the University of California San Diego,1-15(2005).

4.https://en.wikipedia.org/wiki/RSA_numbers#RSA-768.

5.M.A.Nielsen and I.L.Chuang,Quantum computation and quantum information,Cambridge University Press 2000.

6. quantum computer research-principle and physics realization, Li Chengzu etc. is write, Science Press.

7.Peter Shor,Algorithms for Quantum Computation:Discrete Logarithms and Factoring,Proceedings of FOCS,124-134(1994).

Peter W.Shor,Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,SIAM Journal on Computing,26(5), 1484-1509(1997).

Similar Documents

Publication	Publication Date	Title
Kotliar et al.	2006	Electronic structure calculations with dynamical mean-field theory
Henderson et al.	2003	The theory and practice of simulated annealing
Wall et al.	1995	Extraction, through filter-diagonalization, of general quantum eigenvalues or classical normal mode frequencies from a small number of residues or a short-time segment of a signal. I. Theory and application to a quantum-dynamics model
Fagotti et al.	2014	Relaxation after quantum quenches in the spin-1 2 Heisenberg XXZ chain
Albuquerque et al.	2011	Phase diagram of a frustrated quantum antiferromagnet on the honeycomb lattice: Magnetic order versus valence-bond crystal formation
Vojta et al.	2000	Competing orders and quantum criticality in doped antiferromagnets
Malek et al.	2000	Dynamics of Lennard-Jones clusters: A characterization of the activation-relaxation technique
Boutsidis et al.	2009	An improved approximation algorithm for the column subset selection problem
Haegeman et al.	2011	Time-dependent variational principle for quantum lattices
Cai et al.	2010	A singular value thresholding algorithm for matrix completion
Santha	2008	Quantum walk based search algorithms
Ishizaka et al.	2000	Maximally entangled mixed states under nonlocal unitary operations in two qubits
Jaklič et al.	1994	Lanczos method for the calculation of finite-temperature quantities in correlated systems
Jerrum et al.	1996	The Markov chain Monte Carlo method: an approach to approximate counting and integration
Assaraf et al.	1999	Zero-variance principle for Monte Carlo algorithms
Chakrabarti et al.	2007	Quantum control landscapes
Sieberer et al.	2016	Keldysh field theory for driven open quantum systems
Pitowsky et al.	2001	Optimal tests of quantum nonlocality
Kotliar et al.	2001	Cellular dynamical mean field approach to strongly correlated systems
Mulet et al.	2002	Coloring random graphs
Wright	2015	Coordinate descent algorithms
García-García et al.	2016	Spectral and thermodynamic properties of the Sachdev-Ye-Kitaev model
Trebst et al.	2004	Optimizing the ensemble for equilibration in broad-histogram Monte Carlo simulations
Silver et al.	1996	Kernel polynomial approximations for densities of states and spectral functions
Gelfand et al.	2000	High-order convergent expansions for quantum many particle systems

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
CN201811213095.XA	2018-10-18	2018-10-18	The decomposition of RSA public key and decryption method and system

Applications Claiming Priority (1)

Application	Filing date	Title
CN201811213095.XA	2018-10-18	The decomposition of RSA public key and decryption method and system

Legal Events

Date	Code	Title	Description
2019-03-08	PB01		