International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.261-272
http://dx.doi.org/10.14257/ijsia.2014.8.6.23

Quantum Cryptanalysis of Multivariate Permutation Problem

Guodong Sun[1*], Shenghui Su[1,2] and Maozhi Xu[1,3]

[1]*(College of Computer Science, Beijing University of Technology, Beijing, China)*
[2]*(College of Information Engineering, Yangzhou University, Yangzhou, China)*
[3]*(School of Mathematics Sciences, Peking University, Beijing, China)*
[1]*sgd-150@163.com*

Abstract

Quantum computation is a new computational model based on quantum mechanical principle. Shor invented the polynomial time algorithms for the prime factorization and discrete logarithm problem, which indicated that the cryptosystems based on them are totally unsafe in the quantum world. Grover constructed an algorithm that finds a solution in only $O(\sqrt{2^n})$steps whereas the exhaustive search algorithm needs $O(2^n)$ steps on average. In this paper we investigate the cryptanalysis of a new cryptography problem----multivariate permutation problem (MPP), which could be used to design public-key cryptosystem, with the help of the two quantum algorithms. Specially, we discuss the strength of a private key of the REESSE1+ public-key cryptosystem, whose security is based on the hardness of MPP. Besides, some suggestions are also given about the implementation of the REESSE1+.

Keywords: *Quantum cryptanalysis, Shor's algorithm, Grover's algorithm, the multivariate permutation problem, REESSE1+*

1. Introduction

Quantum computation [1] is a new computing model based on quantum physics principle. In early 1980s, R. Feynman [2] observed that exponential slowdown occurs when quantum physical phenomenon is simulated by a classical computer; he speculated that perhaps computation in general could be done more efficiently if it made use of these quantum physical phenomena. In 1985, Deutsch [3] gave the first quantum mechanical algorithm----Deutcsch algorithm to solve the Deutcsch problem; however, this algorithm has no practical applications. Inspired by Simon's result [4], in 1994 Shor [5] proposed a polynomial time quantum mechanical algorithm for solving the factorization problem and discrete logarithm problem (DLP) which were and still are widely believed to have no polynomial solution on a classical computer. This result can be used to break the widely used RSA cryptosystem [6] and Diffie-Hellman key exchange protocol [7]. However, despite enormous effort, there have been only a few other problems for which quantum algorithms provide an exponential speedup. After the pioneering work of Shor, in 1996, Grover [8] designed another quantum mechanical algorithm for searching a marked element in an unsorted database, providing a square root speedup for exhaustive search over classical algorithms.

Nowadays, with the development of wireless technology, mobile internet [9], which is a combination of mobile communication and the internet, has become a hot issue. Based on the mobile internet, various activities are engaged by people conveniently and frequently, such as the mobile tractions, mobile payment [10], mobile authentication [11], and so on. As is known to all, the security of these activities is guaranteed by public-key cryptography [12], which consists of problems and tools including encryption, key distribution, digital signatures

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2014 SERSC

and authentication. A great deal of public-key cryptosystems are believed to be secure against the classical computer, such as RSA [5] and ECC [13], however, when a quantum computer is considered, these public-key systems are thoroughly unsafe because of the invention of Shor's algorithm. In order to confront the challenge of the quantum computer in the future, we must find as more quantum-resistant public-key cryptosystems as possible to ensure the information security in the quantum computer world.

In this paper, the security of a new cryptographic problem named multivariate permutation problem [14], of which the hardness is the basis of the public-key cryptosystem REESSE1+ [15], is analyzed under a quantum computer's attack. Specially, we discuss the security of a private key of the REESSE1+ public-key cryptosystem using Shor's excellent algorithm for factorization and discrete logarithm and Grover's quadratic speed-up searching algorithm. Besides, some suggestions are also given about the implementation of the REESSE1+.

Throughout the paper, unless otherwise specified, $n \geq 80$ is the item-length of a sequence, the sign % represents 'modulo', $\overline{M}$ means 'M-1' with M prime, $\|x\|$ does the order of an element x % M or the size of a set x, and gcd(a, b) denotes the greatest common divisor of two integers, DLP stands for the discrete logarithm problem.

2. The MPP and the REESSE1+

In this section, we first give the definition of a coprime sequence and a lever function, then specify the multivariate permutation problem and introduce the REESSE1+ public-key cryptosystem.

2.1. Some Definitions

Definition 1: A coprime sequence is n pairwise distinct positive integers $A_1, \ldots, A_n$, which satisfy $\forall A_i, A_j (i \neq j)$, either $\gcd(A_i, A_j) = 1$ or $\gcd(A_i, A_j) = F \neq 1$ with $(A_i / F) \nmid A_k$ and $(A_j / F) \nmid A_k \ \forall k \neq i, j \in [1, n]$, denoted $\{A_1, \ldots, A_n\}$, and shortly $\{A_i\}$.

According to the definition 1, we know that the elements of a coprime sequence need not be pairwise coprime, whereas a pairwise coprime sequence must be a coprime sequence. It is easy to understand that the first n primes in the set $\mathbb{N}$ constitute a smallest coprime sequence.

Property 1: Let$\{A_1, \ldots, A_n\}$be a coprime sequence, randomly select m elements from the sequence and construct a subsequence $\{Ax_1, \ldots, Ax_m\}$, then the subset product $G = \prod_{i=1}^{m} Ax_i = Ax_1 \ldots Ax_m$ is uniquely determined, namely the mapping from $\{Ax_1, \ldots, Ax_m\}$ to G is a bijection.

To see a proof of property 1, refers to section 2 of [14], we will not discuss it here.

Definition 2: A lever function is the secret $\ell(i)$ in the key transform of a public-key cryptosystem, it has the following features:

①$\ell(i)$ is an injection from the domain$\{1,\ldots, n\}$ to the range $\Omega \subset \{1, \ldots, \overline{M}\}$;

②The mapping between i and $\ell(i)$ is established randomly without any analytical expression;

③When extracting a corresponding private key from a public key, an attacker has to face all the permutations of elements in Ω;

④When recovering a corresponding plaintext from a ciphertext, the owner of a private key only needs to consider the accumulative sum of elements in Ω.

In the light of definition 2, we know that a lever function is a random function, and if n is

 Copyright ⓒ 2014 SERSC

large enough, an attacker is impossible to obtain a private key while the owner of a private key is easy to recover a message.

2.2. The MPP and REESSE1+

Let Λ= {2, 3, …, 1201} denotes a coprime sequence, and Ω = {+/-5, +/-7, …, +/-2n+3}, using the above definitions, the multivariate permutation problem can be stated as below:

Definition 3: Assume {C_1, …, C_n}be a non-coprime sequence, M be a prime. Finding out the original{A_1, …, A_n} with $A_i \in \Lambda$, {$\ell(1)$, …, $\ell(n)$} with $\ell(i) \in \Omega$, W, δ from $C_i \equiv (A_i W^{\ell(i)})^{\delta}$ (% M) for i =1, …, n is called the multivariate permutation problem, shortly MPP.

It is known from $C_i \equiv (A_i W^{\ell(i)})^{\delta}$ (% M) for i =1, …, n that the MPP contains 2n+2 unknown variables, and each equation includes four almost independent variables. If any one of A_i, W and $\ell(i)$ is determined, the relation between the others is still nonlinear, thus the relation among A_i, W and $\ell(i)$ is very complicated. Through combinations among multiple variables, the MPP brings some different hardness. It is proved that the MPP is computationally at least equivalent to the DLP in the same prime field [16].

As is known to all, a one-way trapdoor function is the basis component to design a public-key cryptosystem. Obviously, the MPP is a one-way trapdoor function. It is known from the definition of the MPP that A_i, $\ell(i)$, W and δ are its trapdoor information. In fact, the MPP is used to design a public-key cryptosystem named REESSE1+ [14]. The REESSE1+ is a prototypal cryptosystem which is used to expound some foundational concepts, ideas, and methods. In the REESSE1+ public key cryptosystem, the MPP is used in the key transform, that is to say, the transform from a private key to a public key. In the encryption algorithm of REESSE1+, C_i are chosen randomly according to the plaintext, and the variables A_i, $\ell(i)$, W and δ are taken as the trapdoor information in the decryption algorithm. And n is usually chosen as 80, 96, 112, or 128 with log$M \approx$ 696, 864, 1030, or 1216.

3. Shor's Algorithm and Grover's Algorithm

In this section, we introduce the two quantum algorithms which are used for the cryptanalysis of the MPP. One is Shor's polynomial time algorithm for prime factorization and DLP, and the other is Grover's quadratic speed-up quantum searching algorithm.

3.1. Shor' Algorithm

A. The factorization algorithm

It is well known that factoring problem can be reduced to the order-finding problem [17], the order-finding problem is to find the least integer r, such that x^r =1 (mod N), given positive integers x and N, $x < N$, with no common factors. Suppose N is L bits length, choose m, a, such that $N^2 \le 2^m \le 2N^2$, $1< a < N$-1. The order-finding quantum algorithm is stated as follows:

1. Initialization: Prepare two quantum registers and initialize them in the state $|0^m, 0^L\rangle$, apply Walsh-Hadamard transformation H to the first register, where H is defined as below:

$$H^{ij} = 2^{-n/2}(-1)^{i \cdot j}, \text{ where } \underline{i} \cdot \underline{j} \text{ is the bitwise dot product operation.}$$

2. Using Oracle: Apply the unitary operator $U_{a, N}$ to the first and the second registers, where $U_{a, N}: |j, k\rangle \rightarrow |j, a^j \oplus k \pmod N\rangle$.

3. Using QFT: Using quantum fourier transform to the first register.

Copyright ⓒ 2014 SERSC

4. Measurement: Measure the first register to get the state. Use the continued fractions algorithm to obtain the period r.

With the above order-finding quantum algorithm, the factoring algorithm is described as below [17]:

1. IF N is even, return the factor 2.

2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a.

3. Randomly choose x in the range 1 to N-1, If gcd(x, N)>1 then return the factor gcd(x, N).

4. Finding the order r of x modulo N using above order-finding algorithm, if r is even and $x^{r/2} \neq -1 (\text{mod } N)$, then compute gcd($x^{r/2}$ -1, N) and gcd($x^{r/2}$+1, N), and test if any one of the two is a non-trivial factor, if so, return the factor. Otherwise the algorithm fails.

In the above quantum algorithm for factoring, Shor proved that the algorithm find a factor of N with a success rate $4\varphi(r)/\pi^2 r$, using O($\log^3 N$) quantum gates [5], where φ is the Euler function and r is the order of a. Comparing with the most effective classical number field sieve algorithm with running time $O(e^{(\log N)^{1/3}(\log \log N)^{2/3}})$ [18], it is a polynomial time algorithm.

B. The discrete logarithm algorithm

Given a generator g of $(Z_N^*, \cdot)$ and $y \equiv g^s (\text{mod } N)$, the discrete logarithm problem is to find s. Suppose there is a function $f(x_1, x_2) = g^{x_1 - sx_2}$ with period (ls, l), let the order of g is r, find t satisfying $N < 2^t < 2N$. The algorithm is described as below:

1. Initialization: Prepare three quantum registers and initialize them in the state $|0^t, 0^t, 0^m>$.

2. Using Oracle: Apply H transformation to the first two registers and the unitary operator U_{x_1, x_2} to the third register, where $U_{x_1, x_2}: |j, k> \rightarrow |j, g^{x_1} y^{-x_2} \oplus k (\text{mod } N)>$.

3. Using QFT: Using quantum fourier transform to the first register and the second register.

4. Measurement: Measure the first and the second registers to get the state, then apply generalized continued fractions algorithm to obtain s.

According to Shor's analysis, the number of quantum gates used to design the algorithm is O($\log^3 N$), and the success rate is at least $N/240p$, where $p = 2^t$. So with constant number of execution of the algorithm, we are assured of a high probability of success.

In the rest of this paper, we denote the quantum algorithm for factorizing an integer N as SHOR (N) and the algorithm to solve DLP $y \equiv g^s (\text{mod } N)$ as SHOR(y, g, s).

3.2. Grover's Algorithm

In 1996, Grover gave a quantum algorithm for searching the needed element in an unsorted database; we first describe the problem and then introduce the algorithm.

A. The Definition of the problem

Assume that there exist $N=2^n$ elements in the database, each element is labeled by 0,1, …. , N-1 orderly. We may represent the index of these elements by n bit binary strings. Let F be a Boolean function of the set of these N elements. Suppose there be a unique element S_V that satisfies the condition $F(S_V) =1$, which is labeled by α, whereas for all the other elements S, $F(S) =0$. The *searching problem* is to identify the element S_V. We suppose that F is effectively

 Copyright ⓒ 2014 SERSC

computable and the functional call to F is considered as an oracle call. Clearly the exhaustive search algorithm needs $O(N)$ oracle queries on average in order to find the element S_V on a classical computer.

B. The algorithm

1. Initialization: Prepare two quantum registers, the first register has n qubits and the other has one qubit. Applying the transformation H to each bit of the initial state which is presented to $|0\rangle$, the following superposition is obtained in the first register

$$1/\sqrt{N}\sum_{j=0}^{N-1}|j\rangle$$

2. Iteration: Repeat the following unitary operation $O(\sqrt{N})$ times.

(a) For the state α in the superposition, rotate the phase by π radians, leave the other states unaltered. A method to realize this operation is given in paper [19].

(b) Apply the diffusion transform D which is defined by the matrix D_{ij} as below:

$$D_{ij}=2/N, \text{ if } i\neq j;\ D_{ij}=-1+2/N.$$

Note that the transform D can be constructed by $D = HRH$, where R is the rotation matrix that define as follows:

$$R_{ij}=0 \text{ if } i\neq j;\quad R_{ii}=1 \text{ if } i=0;\quad R_{ii}=-1 \text{ if } i\neq 0.$$

3. Measurement: Measure the resulting state, the state α is observed with a high probability.

In paper [20], it is proved that after m iterations of 2(a), (b), the system is in the superposition $\sin(2m+1)\theta\,|\alpha\rangle + \cos(2m+1)\theta\,|\beta\rangle$, where the angle θ satisfies $\sin\theta = 1/\sqrt{N}$ and $|\beta\rangle$is the states other than $|\alpha\rangle$. After the above process, the probability that we observe the state $|\alpha\rangle$ is $|\sin(2m+1)\theta|^2$, in order to observe the desired state $|\alpha\rangle$, the proper number of iterations of the process 2 can be estimated. When θ is small enough, due to $\sin\theta \approx \theta$, thus it is easy to understand that $O(\sqrt{N})$ iterations are needed to observe the desired state $|\alpha\rangle$ with a probability at least 1/2.

In fact, we need iterate the process 2(a), (b) $O(\sqrt{N/t})$ times to find one of t desired states out of N states with a probability of at least 1/2(see [20]).

4. Attack by a Single C_i

Since in the MPP the transform $C_i \equiv (A_i W^{\ell(i)})^{\delta} (\% M)$ for $i = 1, \ldots, n$ contains $2n+2$ unknown variables, and each equation contains four almost independent variables, there seems not have a periodic structure, thus we can not analyze it directly using Shor's algorithm. We consider the attack of divining the variables with the known variables $\{C_i\}$, namely the heuristic attack using a quantum computer. In the REESSE1+ public-key cryptosystem, n is selected as 80, 96, 112, or 128, and $A_i \in \Lambda$, $\ell(i) \in \Omega$, due to the sets $\Lambda = \{2,3, \ldots, 1201\}$ and $\Omega = \{+/-5, +/-7, \ldots, +/-2n+3\}$ contain polynomial number of elements, we can divine A_i in the set Λ and $\ell(i)$ in the set Λ. However, since W and δ are chosen in the interval (0, M-1) [14], it is not realistic to divine the value of W and δ.

In the next, we give a quantum searching algorithm to find the target variables $\{A_i\}$, $\{\ell(i)\}$, W and δ from $\{C_i\}$, then analyze the time complexity and success rate of the algorithm.

Copyright ⓒ 2014 SERSC

4.1. The Attack Algorithm

For a given A_i and $\ell(i)$, with $A_i \in \Lambda$ and $\ell(i) \in \Omega$, chosen a C_i. Suppose there is a quantum gate circuit which computes $(A_i W^{\ell(i)})^{\delta}(\% M)$, the algorithm is stated below:

1. Choose an element in the set Λ and Ω respectively, prepare two quantum registers that preset to $|\, 0^m, 0^m\rangle$, where $m = \log M$. Design an Oracle U which marks the expected state, that is to say, the Oracle U is define as below:

$$U(A_i, \ell(i)) = 1 \text{ if } A_i W^{\ell(i)} \equiv C_i \ (\% M); \ U(A_i, \ell(i)) = 0 \text{ if } A_i W^{\ell(i)} \neq C_i \ (\% M)$$

2. Initialize the two registers by making a superposition of all possible W and δ with the same amplitude, namely both W and δ are in the superposition

$$W, \delta = 1/\sqrt{M} \sum_{j=0}^{M-1} |\, j\rangle$$

3. Repeat the procedure 2(a) and (b) in Section 3.2, note that there may be more than one marked state, the exact number of repetition should be discussed.

4. Measuring the system to observe a state $|\, W, \delta\rangle$.

4.2. The Running Time and Success Rate

Now we analyze the running time and the success rate of the above algorithm. Suppose we choose some A_i and $\ell(i)$, and a state $|W', \delta'\rangle$ is observed. For a concrete A_i and $\ell(i)$, the value W and δ vary between 0 and M-1, that is, the possible number of value of $(A_i W^{\ell(i)})^{\delta}$ is M^2. However, there is only M possible values for the operation % M, so the number of (W, δ) which satisfy $A_i W^{\ell(i)} \equiv C_i \ (\% M)$ is almost M. Besides, since the searching space is M^2, so we need to iterate $O(\sqrt{M^2/M}) = O(\sqrt{M})$ times.

In step 4, for a measured state $|W', \delta'\rangle$, owing to there may be M marked states, the probability that it is the right result is only $1/M$. To verity it, we need to try all the A_i and $\ell(i)$, and test whether all the $(A_i W^{\ell(i)})^{\delta'}$ are in the set $\{C_i\}$, if so, the observed state $|W', \delta'\rangle$ is considered right. The probability of success is only $1/M\,||\Lambda||||\Omega||$, for a large enough M, it is nearly zero.

In conclusion, the exhaustive attack to the MPP is impossible by a quantum computer.

5. Attack by Eliminating W Through $\ell(x_i)+\ell(x_j) = \ell(y_b)+\ell(y_d)$

Consider the lever function $\ell(i)$ in the set Ω, where $\Omega = \{5,7, \ldots, 2n+3\}$, $\forall x_i, x_j, y_b, y_d \in [1, n]$, there may have $\ell(x_i)+\ell(x_j) = \ell(y_b)+\ell(y_d)$, so the adversaries may eliminating W through $\ell(x_i)+\ell(x_j) = \ell(y_b)+\ell(y_d)$.

Let $G_z \equiv C_{x_i} C_{x_j} (C_{y_b} C_{y_d})^{-1} (\% M)$, namely

$$G_z \equiv (A_{x_i} A_{x_j} (A_{y_b} A_{y_d})^{-1})^{\delta} (\% M).$$

For $A_i \in \Lambda$, the adversaries may divine the values of A_{x_i}, A_{x_j}, A_{y_b} and A_{y_d}, and using the quantum discrete logarithm algorithm SHOR(y, g, s) to compute u, v_{x_i}, v_{x_j}, v_{y_b}, v_{y_d} such that

 Copyright ⓒ 2014 SERSC

$$G_z \equiv u, A_{x_i} \equiv g^{v_{x_i}}, A_{x_j} \equiv g^{v_{x_j}}, A_{y_b} \equiv g^{v_{y_b}}, A_{y_d} \equiv g^{v_{y_d}} (\% M),$$

where g is a generator of $(Z_M^*, \bullet)$, then there is

$$u \equiv (v_{x_i} + v_{x_j} - v_{y_b} - v_{y_d})\delta (\% \overline{M}).$$

For the above congruence, if $\gcd(v_{x_i} + v_{x_j} - v_{y_b} - v_{y_d}, \overline{M}) \mid u$, it has solutions in δ. There are $\gcd(v_{x_i} + v_{x_j} - v_{y_b} - v_{y_d}, \overline{M})$ solutions for the congruence. Use the SHOR($\overline{M}$) algorithm to factorize $\overline{M}$, the congruence $u \equiv (v_{x_i} + v_{x_j} - v_{y_b} - v_{y_d})\delta (\% \overline{M})$ is equivalent to a congruence set according to the Chinese remainder theorem [21]. Through finding the solution of every congruence, the solutions δ can be obtained.

In the next step, since δ is already known, the attackers may seeking W through diving A_i and $\ell(i)$, $i \in [1, n]$. We denote the possible value set of W is V_i for every i, if there exists $W_1 \in V_1$, $W_2 \in V_2$, ..., $W_n \in V_n$ that satisfy $W_1 = W_2 =$, ..., $= W_n$, the divination of δ, $\{A_i\}$, and $\{\ell(i)\}$ is thought right. We now give a quantum black box algorithm to find W.

The problem can be described as: Given the sets V_1, V_2, ..., V_n, find $W_1 \in V_1$, $W_2 \in V_2$, ... , $W_n \in V_n$ satisfying $W_1 = W_2 =$, ..., $= W_n$. Clearly, the classical exhaustive search needs $O(\|V\|)$ query. We give a quantum searching algorithm for this problem. Suppose there is a quantum black box oracle F defined as below:

$$F(\mathrm{x}) = 1, \text{ if } W_1 = W_2 =, ..., = W_n$$

$F(\mathrm{x}) = 0$, or else.

Apply the iteration of Grover's algorithm in Section 3.2, we can find the solution W in $O(\|V\|^{1/2})$ iteration.

In summary, we analyze the running time of this attack. The entire quantum algorithm used in the above attack can be realized in polynomial time. Since the value of x_i, x_j, y_b and y_d are chosen randomly, the number of potential values of δ is about $n^5\|\Lambda\|^4$. Therefore the set V_i may have $n^5\|\Lambda\|^4 n\|\Omega\|\|\Lambda\|$ values. To eliminate W through $\ell(x_i) + \ell(x_j) = \ell(y_b) + \ell(y_d)$, the running time of quantum algorithm and the classical algorithm are showed in Table 1 when n =80, 96, 112, or 128.

Table 1. The Running Time on a Classical and a Quantum Computer

The value of n	lg$M$	The running time on a classical computer	The running time on a quantum computer
80	696	2^{110}	2^{55}
96	864	2^{115}	2^{58}
112	1030	2^{125}	2^{63}
128	1216	2^{129}	2^{65}

From the Table above, we can see that, to solve the MPP, the efficiency of a quantum computer is a quadratic speedup over that of a classical computer.

Copyright ⓒ 2014 SERSC

Obviously, the attack through eliminating W through $\ell(x_a) + \ell(x_b) + \ell(x_c) = \ell(y_d)$ ($\forall x_a, x_b, x_c, y_d \in [1, n]$) is similar as that of eliminating W through $\ell(x_i) + \ell(x_j) = \ell(y_b) + \ell(y_d)$ ($\forall x_i, x_j, y_b, y_d \in [1, n]$), so the time complexity of the two attacks is in the same degree.

6. Eliminating W through $||W||$-th Power

Use the algorithm Shor(M-1), M-1 can be factorized in polynomial time. In the REESSE1+ public key cryptosystem, due to $\Pi_{i=1}^{k} p_i^{e_i} \mid M$-1 and $\Pi_{i=1}^{k} e_i \geq 2^{10}$, where k meets $p_k \approx 2n$. The order $||W||$ of W can be divined in the running time of about 2^{10}.

Raising either side of $C_i \equiv (A_i W^{\ell(i)})^{\delta} (\% M)$ to the $||W||$-th power yields

$$C_i^{||W||} \equiv (A_i)^{\delta||W||} (\% M)$$

Let $C_i \equiv g^{ui} (\% M)$, and $A_i \equiv g^{vi} (\% M)$, where g is a generator of $(Z_M^*, \bullet)$, then

$$u_i||W|| \equiv v_i||W||\delta \ (\% \overline{M})$$

for $i = 1, \ldots, n$. Notice that $u_i \neq v_i\delta \ (\% \overline{M})$.

The above congruence is similar to the MH transform [22], so the Shamir attack by the accumulation point of minima [23] may be possible. However, we consider the attack by the quantum algorithms in this paper.

The adversary may divine value of A_i in running time of $||\Lambda||$, where $i \in [1, n]$, and compute δ by $u_i||W|| \equiv v_i||W||\delta \ (\% \overline{M})$. The adversary can use the same method in section 5 to compute δ in polynomial time. Because of $||W|| \mid \overline{M}$, the equation will have $||W||$ solutions. We denote the possible value set of δ is U_i for every i, if there exists $\delta_1 \in U_1$, $\delta_2 \in U_2$, ..., $\delta_n \in U_n$ that satisfy $\delta_1 = \delta_2 =$, ..., $= \delta_n$, the δ is thought right. Using the quantum black box algorithm in section 5, δ could be found in $O(||W||^{1/2})$ iteration. Therefore, the running time of finding the original δ is at least

$$\begin{aligned} T &= n||\Lambda||(\log^2 M) + 2^{10}||\Lambda||||W||^{1/2} \\ &= n||\Lambda||(\log^2 M) + 2^{10}||\Lambda||2^{n/2-10} \\ &\approx 2^{n/2} \end{aligned}$$

which is the square root contrasting to the classical attack method in the running time of at least 2^n.

All in all, the time complexity of the attack through eliminating W through the $||W||$-th power is $O(2^{n/2})$.

7. Attack when W or δ is Revealed

7.1. When W is Revealed

When the variable W is revealed to the attacker, he can compute the variable δ through divining the value of A_i and $\ell(i)$. For a concrete A_i and $\ell(i)$, denote $V \equiv A_i W^{\ell(i)} (\% M)$, suppose g is a generator of $(Z_M^*,)$, through the Shor(V, g, u) algorithm, he can obtain u which satisfies $V = g^u (\% M)$, so the MPP $C_i \equiv (A_i W^{\ell(i)})^{\delta} (\% M)$ can be written as

$$C_i \equiv g^{u\delta} (\% M)$$

 Copyright ⓒ 2014 SERSC

In the following, the Shor(C_i, g, v) algorithm can be used again by the attacker to obtain v which satisfies $C_i = g^v (\% M)$, then

$$v \equiv u\delta (\% \overline{M})$$

If gcd(u, $\overline{M}$) | v, the above congruence has solution in δ, use the same quantum algorithm in Section 5, the attacker can obtain the n solutions. In the following, the attacker may check the possible value sets of δ. If there is a identical δ that appears in most sets, it is the right δ. since there are $n\|\Lambda\|$ congruences, using the black box algorithm in Section 5, he may obtain original δ in $O(n^{1/2})$.

In conclusion, the time complexity of the attack is polynomial when W is revealed.

7.2. When δ is Revealed

When the variable δ is revealed and other variables are unknown to the attacker, he can compute the variable W through divining the value of A_i and $\ell(i)$. In this case, let $A_i W^{\ell(i)} = X_i (\% M)$, the expression $C_i \equiv (A_i W^{\ell(i)})^{\delta} (\% M)$ can be denoted as

$$C_i \equiv (X_i)^{\delta} (\% M)$$

In the next step, the attacker needs to obtain the δ-th root of each C_i. For each C_i, compute the discrete logarithm using Shor(C_i, g, v_i), that is $C_i \equiv g^{v_i} (\% M)$, let $X_i \equiv g^{u_i} (\% M)$, such that

$$g^{v_i} \equiv (g^{u_i})^{\delta} (\% M)$$

where g is a generator of $(Z_M^*, \bullet)$, then

$$v_i \equiv u_i \delta (\% \overline{M})$$

Using the same method in the above section, u_i can be computed in polynomial time. Then the attacker obtains W through $X_i \equiv g^{u_i} (\% M)$ and $A_i W^{\ell(i)} = X_i (\% M)$. So W can also be obtained in quantum polynomial time when δ is revealed.

8. Impact on the REESSE1+

According to the analysis of the above attack, we conclude that for a cryptosystem based on the hardness of the MPP, when it is implemented, in order to resist the attack against a quantum computer the following points should be noted:

1. The security parameter should be larger enough to ensure the safety of the cryptosystem. Specifically, the parameter n in the MPP should be at least 160, namely the length of the coprime sequence $\{A_1, \ldots, A_n\}$ and the lever function$\{\ell(1), \ldots, \ell(n)\}$ should be at least 160.

2. If none of the variables in the MPP is revealed, the attack to the MPP using a quantum computer is not a polynomial time algorithm. The time complexity of all the attacks is still exponential. However, compared to classical attacks, they are quadratic speed-up attack algorithms compared to their classical counterpart.

3. Because the MPP is a multivariable problem, multiple variables problem make more hardness than single variable problem, through the analysis of the MPP against the quantum algorithms, we conclude that multivariate problem is a very competitive candidate to design public-key cryptosystem which can resist quantum computer attack in the future.

Copyright ⓒ 2014 SERSC

Acknowledgements

The author would like to thank the professor Huanguo Zhang, Jiabin Yuan, Yuguang Yang, Hongfu Wang and Hailou Yao for their important advices, guidance and help.

References

[1] P. Xia, "Quantum Computing", Journal of Computer Research and Development, vol. 38, no. 10, **(2001).**
[2] R. P. Feynman, "Simulating Physics with Computers", International Journal of Theoretical Physics, vol. 21, no. 6/7, **(1982**).
[3] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", Proceedings of the Royal Society London A, vol. 400, no. 1818, **(1985).**
[4] D. Simon, "On the Power of Quantum Computation", Proceeding of the 35th Annual Symposium on Foundations of Computer Science, **(1994)** October 12-15, Los Alamitos, America.
[5] P. W. Shor, "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing, vol. 26, no. 5, **(1997).**
[6] R. L. Rivest, A. Shamir and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Communications of the ACM, vol. 21, no. 2, **(1978).**
[7] A. Johannes, Buchmann and C. H. Williams, "A Key Exchange System Based on Real Quadratic Fields", In G. Brassard, editor, Advances inCryptology—CRYPTO'89, volume 435 of Lecture Notes in Computer Science, Springer-Verlag, **(1989)** August.
[8] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search", Proceeding of 28th ACM Symposium on Theory of Computation (STOC'96), ACM Press, **(1996),** New York.
[9] A. Jamalipour, "The Wireless Mobile Internet", Abbas Jamalipour Publishers, Los Angeles, **(2003).**
[10] L. Chen, "A Model of Consumer Acceptance of Mobile Payment", International Journal of Mobile Communications, vol. 6, no. 1, **(2008).**
[11] T. Caimu and D. O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 4, **(2008).**
[12] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transaction of Information Theory, vol. 22, no. 6, **(1976).**
[13] I. F. Blake, G. Seroussi and N. P. Smart, "Elliptic Curves in Cryptography", Cambridge University Press, Cambridge, UK, **(1999).**
[14] S. Shenghui and L. Suwang, "A Public Key Cryptosystem Based on Three New Provable Problems", Theoretical Computer Science, **(2012),** pp. 426-427**.**
[15] S. Shenghui and L. Suwang, "The REESSE1+ Public-key Cryptosystem. Reward: Proof by Experiment on 80-bit Moduli", arXiv.org, **(2009)** August 4.
[16] S. Shenghui, L. Suwang and F. Xiubin, "Asymptotic Granularity Reduction and Its Application", Theoretical Computer Science, vol. 412, no. 39, **(2011).**
[17] A. Nielsen and L. C. Isaac, "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, **(2000).**
[18] D. M. Gordon, "Discrete Logarithms in GF (p) Using the Number Field Sieve", Society for Industrial and Applied Mathematics Journal on Discrete Mathematics, vol. 6, no. 1, **(1993).**
[19] J. Preskill, "Quantum Information and Computation", Lecture Notes for Physics, California Institute of Technology, **(1998).**
[20] M. Boyer, G. Brassard, P. Hoyer and A. Tapp, "Tight bounds on quantum searching", PhysComp'96, **(1996).**
[21] Y. Song-Yuan, "Number Theory for Computing", Berlin: Springer-Verlag, **(2002)**.
[22] R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions on Information Theory, vol. 24, no. 5, **(1978).**
[23] A. Shamir, "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", IEEE Transactions on Information Theory, vol. 30, no. 5, **(1984).**

 Copyright ⓒ 2014 SERSC

Author

Guodong Sun, he was born in 1985, in Fanshi, Shanxi Province, China. He received his bachelor's degree in Tianjin University of Science and Technology, and master's degree in Beijing University of Technology. Now he is a Ph.D candidate in College of Computer Science, Beijing University of Technology. His main interests are information security and quantum computation.

Shenghui Su, a professor, received his bachelor's degree in National University of Defense Technology, master's degree in Peking University, and Doctor's degree in University of Science and Technology Beijing. His research interests include computational complexity, digital identity, public-key cryptography, and information security.

Maozhi Xu, a professor, he is the director of Security and Cryptography Engineering research center of Peking University. He received his master's degree in Wuhan University and doctor's degree in Peking University. His research interests include algebra, cryptology and information security.

Copyright ⓒ 2014 SERSC

Copyright ⓒ 2014 SERSC