SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2016, Vol. 59 032111:1–032111:9
doi: 10.1007/s11432-015-5447-y

Cryptanalysis of an MOR cryptosystem based on a finite associative algebra

Wanqing WU[1], Huanguo ZHANG[1], Houzhen WANG[1], Shaowu MAO[1], Shuomei WU[3] & Haiqing HAN[2*]

[1]*Computer School of Wuhan University, Wuhan* 430072*, China;*
[2]*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi* 435003*, China;*
[3]*Computer Department, Shijiazhuang University, Shijiazhuang* 050035*, China*

Received April 24, 2015; accepted July 24, 2015; published online January 26, 2016

Abstract The Shor algorithm is effective for public-key cryptosystems based on an abelian group. At CRYPTO 2001, Paeng (2001) presented a MOR cryptosystem using a non-abelian group, which can be considered as a candidate scheme for post-quantum attack. This paper analyses the security of a MOR cryptosystem based on a finite associative algebra using a quantum algorithm. Specifically, let L be a finite associative algebra over a finite field F. Consider a homomorphism $\phi : \mathrm{Aut}(L) \to \mathrm{Aut}(H) \times \mathrm{Aut}(I)$, where I is an ideal of L and $H \cong L/I$. We compute $\dim \mathrm{Im}(\phi)$ and $\dim \mathrm{Ker}(\phi)$, and combine them by $\dim \mathrm{Aut}(L) = \dim \mathrm{Im}(\phi) + \dim \mathrm{Ker}(\phi)$. We prove that $\mathrm{Im}(\phi) = \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$ and $\mathrm{Ker}(\phi) \cong Z^1(H, I)$. Thus, we can obtain $\dim \mathrm{Im}(\phi)$, since the algorithm for the stabilizer is a standard algorithm among abelian hidden subgroup algorithms. In addition, $Z^1(H, I)$ is equivalent to the solution space of the linear equation group over the Galois fields $GF(p)$, and it is possible to obtain $\dim \mathrm{Ker}(\phi)$ by the enumeration theorem. Furthermore, we can obtain the dimension of the automorphism group $\mathrm{Aut}(L)$. When the map $\varphi \in \mathrm{Aut}(L)$, it is possible to effectively compute the cyclic group $\langle\varphi\rangle$ and recover the private key a. Therefore, the MOR scheme is insecure when based on a finite associative algebra in quantum computation.

Keywords MOR cryptosystem, cryptanalysis, quantum algorithm, finite associative algebra, hidden subgroup problem, stabilizer

Citation Wu W Q, Zhang H G, Wang H Z, et al. Cryptanalysis of an MOR cryptosystem based on a finite associative algebra. Sci China Inf Sci, 2016, 59(3): 032111, doi: 10.1007/s11432-015-5447-y

1 Introduction

A number of quantum algorithms have been presented in the past three decades: the first quantum algorithm by Deutsch [1], an exponential separation algorithm by Simon [2], a polynomial-time quantum algorithm to solve the integer factorization problem by Shor [3], an algorithm for the search problem by Grover [4], and an algorithm to solve the hidden subgroup problem (HSP) by Mosca [5].

The Shor and HSP algorithms pose great challenges to cryptosystems based on abelian groups. Thus, attempts have been made to find new cryptosystems for post-quantum computation based on non-abelian

* Corresponding author (email: hanhaiqing8866@sina.com)

groups. In this context, Ko-Lee [6] presented a public cryptosystem using the braid group, Magliveras [7] proposed a public cryptosystem that has no message expansion and is based on a non-abelian group, Lempken [8] presented a new public-key cryptosystem using the covers and logarithmic signatures of non-abelian groups, and Magliveras [9] presented a simple example of ElGamal encryption using a non-abelian group. However, the security level and efficiency of such schemes have not reached the level of classical cryptography, and therefore further studies in this direction are needed. In this context, at CRYPTO 2001, Paeng et al. [7] presented a MOR scheme using the inner automorphism group. The MOR cryptosystem is an analog of ElGamal encryption. Later, Paeng et al. generalized the MOR cryptosystem to the automorphism group.

We first give a short review of previous work addressing the security of MOR. The authors of MOR briefly discussed the security of the scheme, and showed that there exists a sub-exponential-time algorithm to attack the MOR cryptosystem based on inner automorphism groups [10]. At PKC 2003, Tobias [11] discussed security for the group $SL(2, Z_p) \times_\theta Z_p$. At ASIACRYPT 2004, Lee et al. [12] analyzed the MOR cryptosystem using group extension notation. They showed that the complexity of the MOR cryptosystem over a group G is $\log|G|$ times larger than the DLP over G. Korsten [13] pointed out that the complexity of the MOR cryptosystem based on the group $GL(n, q) \times_\theta H$ is less than that of the discrete logarithm in small fields F_q. Ayan Mahalanobis [14] pointed out that the security of the MOR cryptosystem is equivalent to that of the ELGamal cryptosystem over the fields F_q. In addition, Babai [15] pointed that there exists a randomized polynomial-time algorithm that uses number theory oracles to solve membership testing and the order of the matrix group for factoring and discrete logarithm given a finite field of odd characteristic and a Lie-type simple group of arbitrary characteristic.

Stimulated by these results, this paper analyzes the security of the MOR cryptosystem based on a finite associative algebra using a quantum algorithm. We point out that the MOR scheme based on a finite associative algebra L is unsafe if $\varphi \in \mathrm{Aut}(L)$. There exists a quantum polynomial-time algorithm to recover the privacy of the MOR scheme.

We assume that readers are familiar with the Shor algorithm and the hidden subgroup problem (HSP) [3, 5, 16–18]. The HSP is an extension of the Shor algorithm to finite groups. The core of the HSP algorithm is computation of the period of a function given by quantum oracles.

The organization of this paper is as follows. In Section 2, we introduce the necessary background. In Section 3, we present the relevant results for quantum attack on the MOR cryptosystem based on a finite associative algebra considered in this paper. In Section 4, we present a quantum algorithm for recovering the private key, and we analyze the correctness and complexity of this algorithm. In Section 5, we draw our conclusions and compare our results with the existing cryptanalysis results for the MOR cryptosystem.

2 Background

2.1 MOR cryptosystem based on a finite associative algebra

Let L be a finite associative algebra over a finite field F, where $F = F_p$ and p is prime. Next, we describe MOR cryptography based on a finite associative algebra.

Proposed MOR encryption scheme: Let $l_i, i = 1, \ldots, n$, be the set of generators of L. If we express a message m as the product $l_{i_1} \cdots l_{i_j}$, then $\varphi(m) = \varphi(l_{i_1}) \cdots \varphi(l_{i_j})$ and $(\varphi)^x = \varphi^{x-1}(\varphi)$, where $\varphi \in \mathrm{Aut}(L)$. The details are as follows.

Public key: φ, φ^x.

Private key: x.

Encryption:

1. Alice expresses the message $m \in L$ as the product of $l_i, i = 1, \ldots, n$;
2. Alice randomly chooses a number y and computes $(\varphi^x)^y$;
3. Alice computes $D = \varphi^{xy}(m) = (\varphi^x)^y(m)$;
4. Alice computes $\psi = \varphi^y$;

5. Alice sends (D, ψ).

Decryption:

1. Bob expresses D as the product of $l_i, i = 1, \ldots, n$;
2. Bob computes ψ^{-x} and $\psi^{-x}(D)$.

2.2 Stabilizer and hidden subgroup problem (HSP)

For a finite group G and a finite set S, the stabilizer is a subgroup of G, defined by $H_x = \{g \in G | g.x = x\}$ for any $x \in S$ through the group action of G on set S. For an abelian group (e.g., the additive group), Friedl [16] pointed out that the algorithm for the stabilizer is a standard algorithm for the abelian hidden subgroup problem (AHSP) connected with the parameter ε.

Proposition 1 ([16]). Let G be a finite abelian group and α a group action of G. When $t = \Omega(\log(|G|)\log(1/\varepsilon))$, the stabilizer can be solved in quantum time $\mathrm{poly}(l)\log(1/\varepsilon)$ with error ε.

For a non-abelian group, Hallgren [17] pointed out that there exists an efficient quantum algorithm for the hidden subgroup problem when H is a normal subgroup of G. Moreover, Childs [18] reduced these quantum algorithms to finding a normal subgroup H of any group as follows:

Algorithm 1. Finding a normal hidden subgroup [18].

Input: Block box function hiding $H \trianglelefteq G$.

Output: Normal subgroup H.

Step 1. Let $K_0 := G$. For $t = 1, \ldots, T$, where $T = O(\log |G|)$.

a) Perform weak Fourier sampling, obtaining an irrep $\sigma_t \in \widehat{G}$.

b) Let $K_t := K_{t-1} \cap \mathrm{Ker}\, \sigma_t$.

Step 2. Output K_T.

3 Our results for quantum attack on the MOR cryptosystem based on a finite associative algebra

The MOR cryptosystem is an analog of the ElGamal scheme. Its security is built on the discrete logarithm problem for the automorphism group of a non-abelian group. The cryptography hypothesis of the MOR scheme presented in this paper based on the automorphism group of a finite associative algebra is as follows.

Discrete logarithm problem (DLP). Let L be a finite-dimensional associative algebra over the finite field F, where $F = F_p$ and p is prime. Let $l_1, l_2 \in L$ be such that $\varphi^r(l_1) = l_2 \mod p$ for some $r \in Z$, where $\varphi \in \mathrm{Aut}(L)$. Given $\varphi, \varphi^r \in \mathrm{Aut}(L)$, find an r such that $\varphi^r(l_1) = l_1 \mod p$.

Theorem 1. Consider an n-dimensional finite associative algebra L and $\varphi \in \mathrm{Aut}(L)$. Then there exists a polynomial-time $O(n^2)$ quantum algorithm to solve the above discrete logarithm problem.

This directly yields the following theorem.

Theorem 2. Consider an n-dimensional finite associative algebra L and $\varphi \in \mathrm{Aut}(L)$. Then there exists a polynomial-time $O(n^2)$ quantum algorithm to recover the private key of the MOR scheme based on a finite associative algebra.

4 Proof of Theorem 2

In this section, we present the proof of Theorem 2 as follows. We first describe the quantum algorithm to attack the MOR scheme based on an associative algebra. Then, we illustrate the correctness of the algorithm. Finally, we illustrate the time complexity of the quantum algorithm.

4.1 The quantum algorithm

Before presenting our quantum algorithm, we introduce a modified version of the discrete logarithm quantum algorithm on a cyclic group. Let the cyclic group be $G = Z/pZ$, with $m = |G|$ the order of G and $N = km, k \in Z^+$.

Algorithm 2. Modified version of discrete logarithm.

Input: The cyclic group $G = \langle e \rangle$, the rank N, and an element $d \in G$.

Output: $a = \log_e^d$.

Step 1. Set up the uniform superposition

$$|Z/NZ \times Z/NZ\rangle = |Z/kmZ \times Z/kmZ\rangle = \frac{1}{km} \sum_{\overline{x},\overline{y} \in Z/kmZ} |\overline{x}, \overline{y}, 0\rangle.$$

Step 2. Compute the oracle U_f and store $f(x, y)$ in the third register, where the function $f(\overline{x}, \overline{y}) = d^{\overline{x}} e^{\overline{y}}$ and $(\overline{x}, \overline{y}) \in |Z/kmZ \times Z/kmZ\rangle$. Since $\overline{x} = i_1 N + i_2 m + x, \overline{y} = j_1 N + j_2 m + y, x, y \in \{0, \ldots, m-1\}, i_1, j_1 \in Z^+, i_2, j_2 = 0, 1, \ldots, k-1$, then $f(\overline{x}, \overline{y}) = d^{\overline{x}} e^{\overline{y}} = d^x e^y$. Thus, we obtain

$$\frac{1}{m} \sum_{x', y' \in Z/mZ} |x', y', f(x', y')\rangle.$$

Step 3. Discard the third register. Since $f(\overline{x}, \overline{y}) = f(x', y') = e^{x' \log_e^d + y'}$, let $G_z = \{(x', y') \in |Z/mZ \times Z/mZ\rangle : z = x' \log_e^d + y'\}$. Create the superposition

$$|G_z\rangle = \frac{1}{\sqrt{m}} \sum_{x' \in Z/mZ} |x', z - x' \log_e^d\rangle.$$

Step 4. Applying the quantum Fourier transform over $Z/mZ \times Z/mZ$, we obtain

$$\frac{1}{\sqrt[3]{m}} \sum_{x', y', w \in Z/mZ} \lambda_m^{tx' + w(z - x' \log_e^d)} |t, w\rangle = \frac{1}{\sqrt{m}} \sum_{w \in Z/mZ} \lambda_m^{wz} |w \log_e^d, w\rangle.$$

Step 5. By the quantum measure, we can obtain the quantum state $|w \log_e^d, w\rangle$ with uniformly random $w \in Z/mZ$.

Step 6. Repeating this process, we can obtain the other quantum state $|w' \log_e^d, w'\rangle$, and the probability of $(w, w') = 1$ is at least 0.61. In this case, we can find u, v such that $uw + vw' = 1$. Compute $uw \log_e^d + vw' \log_e^d = \log_e^d$.

Step 7. Output a.

Note 1. Algorithm 2 shows that there exists an efficient quantum algorithm for solving the discrete logarithm problem in Z/pZ, even if the order of the cyclic group has been expanded several times.

Next, we integrate the discussion and present a quantum algorithm 3 to recover the private key.

Algorithm 3. Break the MOR based on a finite associative algebra.

Input: The finite associative algebra L, $\varphi(l)$, and $\varphi(l^a)$.

Output: The private key a.

Step 1. Initialize $A = GL(d_H, F)$ and $B = GL(d_I, F)$;

Step 2. Set up $D = A \times B$;

Step 3. Compute $\mathrm{Comp}(H, I) = \mathrm{Stab}_D(\rho)$ using Algorithm 1, where $\rho \in \mathrm{Hom}(H, \mathrm{End}(I))$ is defined by (5) in Subsection 4.2.1;

Step 4. Compute $C = \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$ using Algorithm 1, where $\mu \in Z^2(H, I)$ satisfies $L = L_\varepsilon$.

Step 5. Compute $\phi(E) = C$ by corollary 1 and the order $|E|$ in Subsection 4.2.2.

Step 6. Set $U = \mathrm{Ker}(\phi)$ and compute $|U|$.

Step 7. Set $P \leftarrow E + U$ and compute $|P| = |E| + |U| = N$.

Step 8. Set $\varphi(l) \to e$ and $\varphi(l)^a \to d$.

Step 9. Compute $a = \log_e^d$ using Algorithm 2.
Step 10. Output a.

4.2 Correctness of the quantum algorithm

How to compute the dimension of the automorphism map is crucial to our quantum algorithm. In this paper, we consider the automorphism map on a finite associative algebra.

Consider a finite associative algebra $L = H \oplus I$, where I is an ideal. The automorphism group of L can be defined as

$$\mathrm{Aut}(L) = \{\sigma \in GL(d_L, F) | \sigma(l_1 \circ l_2) = \sigma(l_1) \circ \sigma(l_2), \sigma(c_1 l_1 + c_2 l_2) = c_1\sigma(l_1) + c_2\sigma(l_2)\}, \tag{1}$$

where $\forall l_1, l_2 \in L, c_1, c_2 \in F$ and $d_L = \dim(L)$.

Given the definition of the ideal I and the direct product of the group, there exists a homomorphism map as follows:

$$\phi : \mathrm{Aut}(L) \to \mathrm{Aut}(H) \times \mathrm{Aut}(I). \tag{2}$$

ϕ transforms α to (α_H, α_I), where $\alpha \in \mathrm{Aut}(L)$ and $\alpha_H \in \mathrm{Aut}(H), \alpha_I \in \mathrm{Aut}(I)$. The addition of ϕ can be defined as $\phi(\alpha^{(1)} + \alpha^{(2)}) = \phi(\alpha^{(1)}) + \phi(\alpha^{(2)})$. The multiplication of ϕ can be viewed as $\phi(\alpha^{(1)}\alpha^{(2)}) = \phi(\alpha^{(1)})\phi(\alpha^{(2)}) = (\alpha_H^{(1)}, \alpha_I^{(1)})(\alpha_H^{(2)}, \alpha_I^{(2)}) = (\alpha_H^{(1)}\alpha_H^{(2)}, \alpha_I^{(1)}\alpha_I^{(2)})$ for the group direct product, where $\alpha^{(i)} \in \mathrm{Aut}(L), i = 1, 2$, and $(\alpha_H^{(1)}, \alpha_I^{(1)}), (\alpha_H^{(2)}, \alpha_I^{(2)}) \in \mathrm{Aut}(H) \times \mathrm{Aut}(I)$.

Thus, our overall approach is to respectively compute $\dim \mathrm{Im}(\phi)$ and $\dim \mathrm{Ker}(\phi)$, and combine them to give $\dim \mathrm{Aut}(L) = \dim \mathrm{Im}(\phi) + \dim \mathrm{Ker}(\phi)$. Next, we describe the calculation process.

4.2.1 *Compute* $\dim \mathrm{Im}(\phi)$

We compute the image of the homomorphism ϕ in two steps.

In the first step, we determine the compatible pairs $\mathrm{Comp}(H, I)$ for computing $\mathrm{Im}(\phi)$. For this, we can define the compatible pairs as follows:

$$\mathrm{Comp}(H, I) = \{(\alpha, \beta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(I) | \beta(h \circ a) = \alpha(h) \circ \beta(a), \beta(a \circ h) = \beta(a) \circ \alpha(h), a \in I, h \in H\}, \tag{3}$$

where the operation $\circ$ denotes the multiplication of the finite associative algebra L.

Proposition 2. The set of compatible pairs $\mathrm{Comp}(H, I)$ is a subgroup of $(\mathrm{Aut}(H), \mathrm{Aut}(I))$.

Proof. Let $\forall(\alpha_i, \beta_i) \in \mathrm{Comp}(H, I), i = 1, 2$; then $(\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1\alpha_2, \beta_1\beta_2)$. Thus, $\beta_1\beta_2(a \circ h) = \beta_1(\beta_2(a) \circ \alpha_2(h)) = \beta_1\beta_2(a) \circ \alpha_1\alpha_2(h)$ and $\beta_1\beta_2(h \circ a) = \beta_1(\alpha_2(h) \circ \beta_2(a)) = \alpha_1\alpha_2(h) \circ \beta_1\beta_2(a)$, where $a \in I, h \in H$. So $(\alpha_1\alpha_2, \beta_1\beta_2) \in \mathrm{Comp}(H, I)$. It is clear that $(\alpha_i^{-1}, \beta_i^{-1}) \in \mathrm{Comp}(H, I)$ by definition. Thus, the set of compatible pairs $\mathrm{Comp}(H, I)$ is a subgroup.

Next we show that the subgroup $\mathrm{Comp}(H, I)$ is the stabilizer of $\mathrm{Aut}(H) \times \mathrm{Aut}(I)$. We define the stabilizer as

$$\mathrm{Stab}_{\mathrm{Aut}(H)\times\mathrm{Aut}(I)}(\rho) = \{(\alpha, \beta) \in \mathrm{Aut}(H) \times \mathrm{Aut}(I) | (\alpha, \beta)\rho = \rho\}, \tag{4}$$

where the map $\rho \in \mathrm{Hom}(H, \mathrm{End}(I))$ satisfies $\rho(h)(a) = a \circ h$. Let the group $\mathrm{Aut}(H) \times \mathrm{Aut}(I)$ act on ρ via

$$\sigma\rho(h) = \beta(\rho(\alpha^{-1}(h)))\beta^{-1}, \tag{5}$$

where $h \in H, a \in I, \sigma \in \mathrm{Aut}(H) \times \mathrm{Aut}(I)$. We have the following theorem:

Theorem 3. The set of compatible pairs $\mathrm{Comp}(H, I)$ is equal to $\mathrm{Stab}_{\mathrm{Aut}(H)\times\mathrm{Aut}(I)}(\rho)$.

Proof. Let $(\alpha, \beta) \in \mathrm{Comp}(H, I)$. It is clear that $(\alpha^{-1}, \beta^{-1}) \in \mathrm{Comp}(H, I)$. Let $h \in H, a \in I, \alpha \in \mathrm{Aut}(H), \beta \in \mathrm{Aut}(I)$. By (3), we obtain $a \circ h = \beta(\beta^{-1}(a) \circ \alpha^{-1}(h)), a \in I, h \in H$. Since $\rho(h)(a) = a \circ h$, we have $\rho(h)(a) = \beta(\beta^{-1}(a) \circ \alpha^{-1}(h))$. By (5), we obtain $\rho(h) = \beta(\rho(\alpha^{-1}(h)))\beta^{-1}$ and $\rho(h) = (\alpha, \beta)\rho(h)$. So $\mathrm{Comp}(H, I) = \mathrm{Stab}_{\mathrm{Aut}(H)\times\mathrm{Aut}(I)}(\rho)$, as desired.

In the second step, we compute $\dim \mathrm{Im}(\phi)$. Consider a sequence $\{C^n, -\infty < n < \infty\}$ in the category of modules and $d^n \in \mathrm{Hom}(C^{n-1}, C^n)$, satisfying

$$\cdots \longrightarrow C^{n-1} \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n+1}} \cdots, \tag{6}$$

such that $d^n d^{n-1} = 0$.

The condition $d^n d^{n-1} = 0$ is equivalent to $\mathrm{Im}(d^{n-1}) \subseteq \mathrm{Ker}(d^n)$. Let $Z^n = \mathrm{Ker}(d^n)$ and $B^n = \mathrm{Im}(d^{n-1})$. Then Z^n/B^n is called the nth cohomology group. C^n, Z^n, and B^n are called n-dimensional cochains, cocycles, and coboundaries, respectively. Next, we present the definition of the second cohomology group:

$$C^2(H, I) = \{\varepsilon : H^2 \to I\}, \tag{7}$$

$$Z^2(H, I) = \{\varepsilon \in C^2(H, I) | \varepsilon(h_1 \circ h_2, h_3) - \varepsilon(h_1, h_2 \circ h_3) = h_1 \circ \varepsilon(h_2, h_3) - \varepsilon(h_1, h_2) \circ h_3\}, \tag{8}$$

$$B^2(H, I) = \{\varepsilon \in C^2(H, I) | \varepsilon(h_1, h_2) = \nu(h_1 \circ h_2) - h_1 \circ \nu(h_2) - \nu(h_1) \circ h_2\}, \tag{9}$$

$$Z^1(H, I) = \{\nu : H \to I | \nu(h_1 \circ h_2) = h_1 \circ \nu(h_2) + \nu(h_1) \circ h_2\}, \tag{10}$$

where $h_1, h_2, h_3 \in h^{[15]}$.

Lemma 1. $B^2(H, I) \subseteq Z^2(H, I)$.

Proof. By (8) and (9),

$$\begin{aligned}
&h_1 \circ \varepsilon(h_2, h_3) - \varepsilon(h_1 \circ h_2, h_3) + \varepsilon(h_1, h_2 \circ h_3) - \varepsilon(h_1, h_2) \circ h_3 \\
&\quad = h_1 \circ \nu(h_2 \circ h_3) - h_1 \circ h_2 \circ \nu(h_3) - h_1 \circ \nu(h_2) \circ h_3 + h_1 \circ h_2 \circ \nu(h_3) \\
&\qquad - \nu(h_1 \circ h_2 \circ h_3) + \nu(h_1 \circ h_2) \circ h_3 - h_1 \circ \nu(h_2 \circ h_3) + \nu(h_1 \circ h_2 \circ h_3) \\
&\qquad - \nu(h_1) \circ h_2 \circ h_3 + h_1 \circ \nu(h_2) \circ h_3 - \nu(h_1 \circ h_2) \circ h_3 + \nu(h_1) \circ h_2 \circ h_3 = 0.
\end{aligned}$$

So $B^2(H, I) \subseteq Z^2(H, I)$ holds.

$Z^2(H, I)$ yields a new algebra. More precisely, every element $\mu \in Z^2(H, I)$ induces a new extension $L_\mu = H \oplus_\mu I$. The new multiplication bracket is defined as

$$(h_1, a_1) \circ_\mu (h_2, a_2) = (h_1 \circ h_2, \mu(h_1, h_2) + h_1 \circ a_2 + a_1 \circ h_2). \tag{11}$$

Lemma 2. The vector space L_μ is a finite associative algebra.

Proof. We prove that the new multiplication bracket satisfies the associative law. We have, $\forall h_i \in H, a_i \in I, i = 1, 2, 3$ and $\mu \in Z^2(H, I)$,

$$\begin{aligned}
&((h_1, a_1) \circ_\mu (h_2, a_2)) \circ_\mu (h_3, a_3) \\
&\quad = (h_1 \circ h_2, \mu(h_1, h_2) + h_1 \circ a_2 + a_1 \circ h_2) \circ_\mu (h_3, a_3) \\
&\quad = (h_1 \circ h_2 \circ h_3, \mu(h_1 \circ h_2, h_3) + h_1 \circ h_2 \circ a_3 + \mu(h_1, h_2) \circ h_3 + h_1 \circ a_2 \circ h_3 + a_1 \circ h_2 \circ h_3), \\
&(h_1, a_1) \circ_\mu ((h_2, a_2) \circ_\mu (h_3, a_3)) \\
&\quad = (h_1, a_1) \circ_\mu (h_2 \circ h_3, \mu(h_2, h_3) + h_2 \circ a_3 + a_2 \circ h_3) \\
&\quad = (h_1 \circ h_2 \circ h_3, \mu(h_1, h_2 \circ h_3) + h_1 \circ h_2 \circ a_3 + h_1 \circ \mu(h_2, h_3) + h_1 \circ a_2 \circ h_3 + a_1 \circ h_2 \circ h_3).
\end{aligned}$$

So the associative law holds. L_μ is a finite associative algebra, as desired.

Further, the action of $\mathrm{Comp}(H, I)$ on $Z^2(H, I)$ can be defined via $(\alpha, \beta)\mu(h_1, h_2) = \beta\mu(\alpha^{-1}(h_1), \alpha^{-1}(h_2))$. Let $\mu \in Z^2(H, I)$ such that $L = L_\mu$. We have the following theorem.

Theorem 4. $\mathrm{Im}(\phi)$ is equal to $\mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$.

Proof. Let $(\alpha, \beta) \in \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$. Since $B^2(H, I)$ is a subspace of $Z^2(H, I)$, then $(\alpha, \beta)\mu \equiv \mu \bmod (B^2(H, I))$. Thus, there is an element $\varepsilon \in B^2(H, I)$ such that $(\alpha, \beta)\varepsilon + (\alpha, \beta)\mu = \mu$ and $\mu(\alpha(h_1), \alpha(h_2)) = \beta(\mu(h_1, h_2) + \varepsilon(h_1, h_2))$.

Let $\upsilon : H \to I$ induce $\varepsilon \in B^n(H, I)$. Then we define a map $\psi : L \to L$ as $\psi(h, a) = (\alpha(h), \beta(a) + \beta\upsilon(h))$ for $a \in I, h \in H$. In the following, it remains to show that ψ is a homomorphism of the associative algebra L_μ:

$$\begin{aligned}
&\psi((h_1, a_1) \circ_\mu (h_2, a_2)) \\
&\quad = \psi(h_1 \circ h_2, \mu(h_1, h_2) + h_1 \circ a_2 + a_1 \circ h_2) \\
&\quad = (\alpha(h_1 \circ h_2), \beta\mu(h_1, h_2) + \beta(h_1 \circ a_2) + \beta(a_1 \circ h_2) + \beta\nu(h_1 \circ h_2)) \\
&\quad = (\alpha(h_1) \circ \alpha(h_2), \beta\mu(h_1, h_2) + \alpha(h_1) \circ \beta(a_2) + \beta(a_1) \circ \alpha(h_2) \\
&\qquad + \beta\varepsilon(h_1, h_2) + \alpha(h_1) \circ \beta\upsilon(h_2) + \beta\upsilon(h_1) \circ \alpha(h_2)) \\
&\quad = (\alpha(h_1) \circ \alpha(h_2), \mu(\alpha(h_1), \alpha(h_2)) + \alpha(h_1) \circ (\beta(a_2) + \beta\nu(h_2)) + (\beta(a_1) + \beta\nu(h_1)) \circ \alpha(h_2)) \\
&\quad = (\alpha(h_1), \beta(a_1) + \beta\nu(h_1)) \circ_\mu (\alpha(h_2), \beta(a_2) + \beta\nu(h_2)) \\
&\quad = \psi(h_1, a_1) \circ_\mu \psi(h_2, a_2).
\end{aligned}$$

Thus, $\mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I)) \subseteq \mathrm{Im}(\phi)$.

Let $(\alpha, \beta) \in \mathrm{Im}(\phi)$. Then there exists $\psi \in \mathrm{Aut}(L_\mu)$ such that $\phi(\psi) = (\alpha, \beta)$. Our task is to prove $\beta(\mu(h_1, h_2) + \varepsilon(h_1, h_2)) = \mu(\alpha(h_1), \alpha(h_2))$ as follows:

$$\begin{aligned}
&(\alpha(h_1 \circ h_2), \beta\mu(h_1, h_2) + \beta\nu(h_1 \circ h_2)) \\
&\quad = \psi(h_1 \circ h_2, \mu(h_1, h_2)) = \psi((h_1, 0) \circ_\mu (h_2, 0)) = \psi(h_1, 0) \circ_\mu \psi(h_2, 0) \\
&\quad = (\alpha(h_1), \beta\nu(h_1)) \circ_\mu (\alpha(h_2), \beta\nu(h_2)) \\
&\quad = (\alpha(h_1) \circ \alpha(h_2), \mu(\alpha(h_1), \alpha(h_2)) + \alpha(h_1) \circ \beta\nu(h_2) + \beta\nu(h_1) \circ \alpha(h_2)) \\
&\quad = (\alpha(h_1 \circ h_2), \mu(\alpha(h_1), \alpha(h_2)) + \beta\nu(h_1 \circ h_2) - \beta\varepsilon(h_1, h_2)).
\end{aligned}$$

Hence, $\beta(\mu(h_1, h_2) + \varepsilon(h_1, h_2)) = \mu(\alpha(h_1), \alpha(h_2))$. Further, $(\alpha, \beta)\mu \equiv \mu \bmod B^2(H, I)$ and hence $(\alpha, \beta) \in \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$, as desired.

Corollary 1. Let $(\alpha, \beta) \in \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$, where $\mu \in Z^2(H, I)$ such that $L = L_\mu$ and $\nu \in Z^1(H, I)$. Then $\psi(h, a) = (\alpha(h), \beta(a) + \beta\nu(h))$ such that the map ψ is a preimage of (α, β) under ϕ.

Note 2. By the above theorem, $\mathrm{Im}(\phi)$ can be obtained as a stabilizer of the cocycle. The theorem provides a method for computing the preimages. Thus, it can compute $\dim \mathrm{Im}(\phi)$ by calling the quantum Algorithm 1 [18].

4.2.2 *Compute* $\dim \mathrm{Ker}(\phi)$

The following theorem yields a description of $\mathrm{Ker}(\phi)$, which can be used to compute generators for this kernel.

Theorem 5. $\mathrm{Ker}(\phi) \cong Z^1(H, I)$.

Proof. Let $\sigma \in \mathrm{Ker}(\phi)$ have the form $\sigma(l_i) = l_i + a_{l_i}$, where $l_i = h_i + a_i \in L, h_i \in H, a_i, a_{l_i} \in I$. Then

$$\begin{aligned}
a_{l_1 \circ_\mu l_2} &= \sigma(l_1 \circ_\mu l_2) - l_1 \circ_\mu l_2 \\
&= \sigma(l_1) \circ_\mu \sigma(l_2) - l_1 \circ_\mu l_2 \\
&= (l_1 + a_{l_1}) \circ_\mu (l_2 + a_{l_2}) - l_1 \circ_\mu l_2 \\
&= (h_1 + a_1 + a_{l_1}) \circ_\mu (h_2 + a_2 + a_{l_2}) - (h_1 + a_1) \circ_\mu (h_2 + a_2) \\
&= h_1 \circ h_2 + \mu(h_1, h_2) + h_1 \circ a_2 + h_1 \circ a_{l_2} + a_1 \circ h_2 + a_{l_1} \circ h_2 \\
&\quad - (h_1 \circ h_2 + \mu(h_1, h_2) + h_1 \circ a_2 + a_1 \circ h_2) \\
&= h_1 \circ a_{l_2} + a_{l_1} \circ h_2.
\end{aligned}$$

Further, $a_{l_1} = a_{l_2}$ if $l_1 \equiv l_2 \bmod (I)$. Therefore, it yields a map $\upsilon : H \to I$ via $\upsilon(h_i) = a_{h_i}$.

Thus, we define a group homomorphism from the multiplicative group $\mathrm{Ker}(\phi)$ to the additive group V, namely, $\mathrm{Ker}(\phi) \to V : \sigma \to \upsilon$. So the map $\mathrm{Ker}(\phi)$ is bijective and it is also an isomorphism.

Let $h_1, \ldots, h_{d_H}$ and $e_1, \ldots, e_{d_I}$ be respectively the bases of H and I. Then $\{h_1, \ldots, h_{d_H}, e_1, \ldots, e_{d_I}\}$ is a basis of L, where $d_H = \dim(H)$ and $d_I = \dim(I)$. Thus,

$$\begin{cases} \upsilon(h_1) = a_{11}e_1 + \cdots + a_{1d_I}e_{d_I}, \\ \upsilon(h_2) = a_{21}e_1 + \cdots + a_{2d_I}e_{d_I}, \\ \quad \vdots \\ \upsilon(h_{d_H}) = a_{d_H1}e_1 + \cdots + a_{d_Hd_I}e_{d_I}. \end{cases}$$

Let b_{12}^i, c_{r2}^j, and c_{2r}^l be respectively structure constants. Then the multiplication table can be defined as

$$h_1 \circ h_2 = \sum_{i=1}^{d_H} b_{12}^i h_i, e_r \circ h_2 = \sum_{j=1}^{d_I} c_{r2}^j e_j, h_2 \circ e_r = \sum_{l=1}^{d_I} c_{2r}^l e_l. \tag{12}$$

From $\nu(h_1 \circ h_2) = \nu(h_1) \circ h_2 + h_1 \circ \nu(h_2)$, we obtain that

$$\sum_{i=1}^{d_H} b_{12}^i \sum_{j=1}^{d_I} a_{ij}e_j = \sum_{s=1}^{d_I} a_{1s} \sum_{j=1}^{d_I} c_{r2}^j e_j + \sum_{t=1}^{d_I} a_{2t} \sum_{l=1}^{d_I} c_{2r}^l e_l, \tag{13}$$

where the parameter $b_{12}^i, c_{r2}^j, c_{2r}^l \in F$ are given by the multiplication bracket of L and the a_{it} are variables. So the computation of $\mathrm{Ker}(\phi)$ is equivalent to solving a linear equation system.

In our quantum algorithm, we must know the dimension of $\mathrm{Ker}(\phi)$, but need not know all the solutions of $\mathrm{Ker}(\phi)$. When $h_i \circ h_j$ run through all cases, we obtain a system of equations containing $d_H d_I$ variables and $d_H(d_H - 1)$ equations. By the enumeration theorem for solutions of matrix equations over finite fields [19], we know that the dimension of $\mathrm{Ker}(\phi)$ is p^k, where k is the dimension of the solution space and p is prime. Thus, we can obtain k from a computer calculation of the coefficient determinant.

Thus, we obtain $\dim \mathrm{Im}(\phi)$ and $\dim \mathrm{Ker}(\phi)$, and combine them to give $\dim \mathrm{Aut}(L) = \dim \mathrm{Im}(\phi) + \dim \mathrm{Ker}(\phi)$. Thus, we can recover the private key a by calling the quantum Algorithm 2.

4.3 Complexity of the quantum algorithm

Algorithm 3 needs two stabilizer (or hidden normal subgroup) computations and one discrete logarithm computation. This is the main part of the algorithm. In Algorithm 3, the order $|D| \leqslant p^{d_H^2 + d_I^2} < p^{n^2}$, where $n = d_H + d_I$. Without loss of generality, let the prime $p < 2^k, k \in Z^+$, and the order $|D| < 2^{kn^2}$. Thus, the time complexity of the stabilizer (or hidden normal subgroup) problem computation is at most $O(kn^2)$ [18].

In addition, the time complexity of the discrete logarithm computation is polynomial in the input size. Therefore, the time complexity of Algorithm 2 is $O(n^2)$. Thus, the MOR scheme based on a finite associative algebra is unsafe, and there exists an effective quantum algorithm to compute the private key a in this case.

5 Conclusion

In this paper, we have provided a cryptanalysis of the MOR cryptosystem based on a finite associative algebra using a quantum algorithm. If the map belongs to the automorphism group of a finite associative algebra, the private key is insecure and there exists an effective quantum algorithm to solve it. From the analysis in this paper, the stabilizer is a very important part of the algorithm, since there exists an effective quantum algorithm to compute the stabilizer even in a non-abelian group. This paper has shown that $\mathrm{Im}(\phi) = \mathrm{Stab}_{\mathrm{Comp}(H,I)}(\mu + B^2(H, I))$ and $\mathrm{Ker}(\phi) \cong Z^1(H, I)$. We can compute $\dim \mathrm{Aut}(L)$ in polynomial time using a quantum algorithm. We can simulate the calculation of the discrete logarithm and recover the private key from the public key using a quantum algorithm. Thus, the computational

Table 1 Comparison of current cryptanalysis results

Author	Cryptography group	Current cryptanalysis results
Paeng [10]	Non-abelian group	Sub-exponential-time algorithm
Lee [12]	Non-abelian group	Complexity $\log \lvert G\rvert$ times larger than that of DLP
Korsten [13]	$GL(n,q) \times_\theta H$	Complexity less than that of DLP in small fields F_q.
Tobias [11]	$SL(2,Z_p) \times_\theta Z_p$	No harder than $SL(2,Z_p)$
Babai [15]	Odd-characteristic matrix group	Randomized quantum polynomial-time algorithm
Babai [15]	Lie-type simple group	Randomized quantum polynomial-time algorithm
Our scheme	Finite associative algebra	Quantum polynomial-time complexity $O(n^2)$

complexity of the algorithm is $O(n^2)$. From the above discussion, it is seen that the map of the new public cryptosystem is nonlinear. Otherwise, it may be unsafe when faced with a quantum computer.

This paper has analysed the security of the MOR cryptosystem using a quantum algorithm. Table 1 compares the current cryptanalysis of the MOR cryptosystem with several existing results.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 60970006, 61003267, 61332019), Major State Basic Research Development Program of China (Grant No. 2014CB340600), Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-14-002), and Fundamental Research Funds for the Central Universities (Grant No. 2012211020213).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. Proc Roy Soc A-Math Phys Eng, 1992, 439: 553–558
2 Simon D R. On the power of quantum computation. SIAM J Comput, 1997, 26: 1474–1483
3 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev, 1999, 41: 303–332
4 Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett, 1997, 79: 325–328
5 Mosca M, Ekert A. The hidden subgroup problem and eigenvalue estimation on a quantum computer. Quantum Comput Quantum Commun, 1999: 174–188
6 Ko K H, Lee S J, Cheon J H, et al. New public-key cryptosystem using braid groups. In: Proceedings of 20th Annual International Cryptology Conference, Santa Barbara, 2000. 166–183
7 Paeng S H, Ha K C, Kim J H, et al. New public key cryptosystem using finite non Abelian groups. In: Proceedings of 21st Annual International Cryptology Conference, Santa Barbara, 2001. 470–485
8 Lempken W, van Tran T, Magliveras S S, et al. A public key cryptosystem based on non-abelian finite groups. J Cryptol, 2009, 22: 62–74
9 Mahalanobis A. A simple generalization of the ElGamal cryptosystem to non-abelian groups II. Commun Algebra, 2012, 40: 3583–3596
10 Paeng S H. On the security of cryptosystem using automorphism groups. Inf Process Lett, 2003, 88: 293–298
11 Tobias C. Security analysis of the MOR cryptosystem. In: Proceedings of 6th International Workshop on Practice and Theory in Public Key Cryptography, Miami, 2002. 175–186
12 Lee I S, Kim W H, Kwon D, et al. On the security of MOR public key cryptosystem. In: Proceedings of 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, 2004. 387–400
13 Korsten A. Cryptanalysis of MOR and discrete logarithms in inner automorphism groups. In: Proceedings of 2nd Western European Workshop on Research in Cryptology, Bochum, 2008. 78–89
14 Mahalanobis A. A simple generalization of ElGamal cryptosystem to non-abelian groups. Commun Algebra, 2006, 40: 3583–3596
15 Babai L, Beals R, Seress Á. Polynomial-time theory of matrix groups. In: Proceedings of 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 55–64
16 Friedl K, Ivanyos G, Magniez F, et al. Hidden translation and orbit coset in quantum computing. In: Proceedings of 35th Annual ACM Symposium on Theory of Computing. New York: ACM, 2003. 1–9
17 Hallgren S, Russell A, Ta-Shma A. The hidden subgroup problem and quantum computation using group representations. SIAM J Comput, 2003, 32: 916–934
18 Childs A M, van Dam W. Quantum algorithms for algebraic problems. Rev Mod Phys, 2010, 82: 1–52
19 Wei H Z, Wang Y X. Enumeration theorems of solutions of some matrix equations over finite field (in Chinese). J Hebei Normal Univ, 1993, 17: 1–13