2015 International Conference on Computer Science and Mechanical Automation

A Passive Attack Against an Asymmetric Key Exchange Protocol

YunFei CAO
Science and Technology on Communication Security Laboratory, Chengdu 610041, China
e-mail: cao_426@126.com

Jian BAI
Science and Technology on Communication Security Laboratory, Chengdu 610041, China
e-mail: baijian@126.com

***Abstract*—Constructing key exchange protocols which can resist the quantum-attack is a hot topic. In ChinaCrypt2014, S. Mao *et al* claimed a new quantum-resistant key exchange protocol and also recommended a set of practical parameter. In this paper, we present a passive attack against this key exchange protocol. Specifically, an eavesdropper can recover the exchange key in polynomial time provided with an oracle solving the discrete logarithm problem. Particularly, this key exchange protocol with the recommended parameter can be attacked by a polynomial time algorithm.**

Keywords-asymmetric key exchange protocol, passive attack, quantum-resistant, ergodic matrix

I. Introduction

All manuscripts must be in English. These guidelines in clKey exchange is a fundamental cryptographic primitive, which allows two communication parties to generate a common secret key over insecure networks. The Diffie-Hellman key exchange protocol, proposed in 1976[1], has two characteristics: (1) Both entities are under a peer-to-peer computing environment and their computing is symmetric (computing symmetrically means that both sides have the same operations); (2) It is based on the discrete logarithm problem. But with the development of the information technology industry, the key exchange scheme is possibly used in the asymmetric computing environment, such as the cloud computing, server and mobile devices. Additionally, the Shor's quantum algorithm [2] can solve integer factorization and the discrete logarithm problem in polynomial time [3,4]. The cryptosystems like RSA and ECC, or the key exchange protocols like the Diffie-Hellman key exchange protocol, are not secure if a quantum computer is practically feasible in future. Therefore, it is a hot topic to devise new key exchange protocols based on the quantum-resistant hard problem, such as lattice problem [5], MQ problem [6], braid group problem.

Many encryption schemes based on the quantum-resistant hard problem were proposed [7,8]. Contrarily, the key exchange protocol which can resist the quantum attack has attracted less research. However, In China Crypt 2014, an asymmetric-computing key exchange protocol [9] was proposed based on the newly defined Decisional Tensor and Subset-Product of Ergodic Matrix Problem (DTSPEM) and was claimed to resist the quantum algorithm.

In this paper, we propose an attack against the key exchange protocol [9] with an oracle solving the discrete logarithm. By our method, an eavesdropper, with the help of a quantum computer, can use the data transmitted through public channels to retrieve the common secret key negotiated by the key exchange protocol [9].

The rest of this paper is organized as follows. Sect.2 includes some basic notations and facts. In Sect.3 we recall the asymmetric key exchange protocol in [9]. In Sect.4 we present the passive attack against the protocol. Sect. 5 is a toy example. Finally, Sect.6 is a summary and conclusion.

II. Preliminary

To clearly present the key exchange protocol [9] and our attack, we prepare some notations and basic facts in this section.

Let F_q be a finite field of q elements, F_q^n the set of n-dimensional vectors over F_q, $F_q^{n\times n}$ the set of $n \times n$ matrices over F_q.

Definition1 A matrix $Q \in F_q^{n\times n}$ is called an *ergodic matrix* over F_q if for any nonzero $v \in F_q^n$,

$$\{Qv, Q^2v, \dots, Q^{q^n}v\} = F_q^n \backslash \{0\}.$$

Lemma 1[14] If $Q \in F_q^{n\times n}$ is an ergodic matrix, then$(F_q[Q], +, \times)$ is a finite field with q^nelements.

Definition 2 Given $A = [a_{ij}]_{m\times n} \in F_q^{m\times n}$ and $B = [b_{ij}]_{k\times l} \in F_q^{k\times l}$, the *tensor* of $A \otimes B$ is a $mk \times kl$ matrix described by the following block matrix

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix},$$

where each block (i, j) in $A \otimes B_{mk\times nl}$ is a $k \times l$ matrix $a_{ij}B$.

Lemma 2[9] Let A, B, C, D be respectively $k_1 \times l_1$,$k_2 \times l_2$, $l_1 \times m_1$, $l_2 \times m_2$ matrices. Then $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$.

Theorem 1[2]There is a quantum algorithm that given a finite field F_{q^n}, runs in time poly($\log q^n$) and solves the discrete logarithm problem over F_{q^n}.

Definition 3 Decisional Tensor & Subset-product of Ergodic Matrix problem(DTSPEM)For $m > 2n\log q$, given ergodic matrix $Q \in F_q^{n\times n}$, choose uniformly at random $x_1, \dots. x_m \in F_{q^n}$, and $\widetilde{x_1}, \dots. \widetilde{x_m} \in F_{q^n}$, compute $Q_1 = Q^{x_1}, \dots, Q_m = Q^{x_m}$ and $\tilde{Q}_1 = Q^{\widetilde{x_1}}, \dots, \tilde{Q}_m = Q^{\widetilde{x_m}}$, choose

978-1-4673-9166-5/15 $31.00 © 2015 IEEE
DOI 10.1109/CSMA.2015.16

uniformly at random $\mathbf{r} = (r_1, \dots, r_m) \in \{0,1\}^m$ with $\mathrm{wt}(\mathbf{r}) = s$, and $M \in F_q^{n\times n}\backslash\{0\}$, when $(Q_1^k \otimes M \otimes \tilde{Q}_1^l, \dots, Q_m^k \otimes M \otimes \tilde{Q}_m^l, \prod_{i=1}^m Q_i^{r_i}, \prod_{i=1}^m \tilde{Q}_i^{r_i}, A \otimes B \otimes C)$ are known, decide whether $A \otimes B \otimes C = \prod_{i=1}^m Q_i^{kr_i} \otimes M^s \otimes \prod_{i=1}^m \tilde{Q}_i^{lr_i}$ or not.

III. THE KEY EXCHANGE PROTOCOL PROPOSED BY MAO ET AL

Mao et al [9] gave the new key exchange protocol as follows.

Protocol 1 Asymmetric-computing key exchange protocol

System setup: Find anergodicmatrix $\boldsymbol{Q} \in \boldsymbol{F_q^{n\times n}}$, in$\{\boldsymbol{0}, \boldsymbol{1}, \dots, \boldsymbol{q^n} - \boldsymbol{2}\}$choose uniformly randomnumbers $\boldsymbol{x_1}, \dots. \boldsymbol{x_m}, \tilde{\boldsymbol{x}}_1, \dots. \tilde{\boldsymbol{x}}_m$. The public parameters are $\boldsymbol{Q_1} = \boldsymbol{Q}^{x_1}, \dots, \boldsymbol{Q_m} = \boldsymbol{Q}^{x_m}$and $\tilde{\boldsymbol{Q}}_1 = \boldsymbol{Q}^{\tilde{x}_1}, \dots, \tilde{\boldsymbol{Q}}_m = \boldsymbol{Q}^{\tilde{x}_m}$.

Exchange phases:

Step 1 Alice uniformly choosesa random vector$\mathbf{r} = (\boldsymbol{r_1}, \dots, \boldsymbol{r_m}) \in \{\boldsymbol{0}, \boldsymbol{1}\}^m$ of weight $\lfloor\frac{m}{2}\rfloor$, and then sends $\prod_{i=1}^m \boldsymbol{Q}_i^{r_i}$ and $\prod_{i=1}^m \tilde{\boldsymbol{Q}}_i^{r_i}$ to Bob.

Step 2 Bob uniformly chooses random numbers$\boldsymbol{k}, \boldsymbol{l}$ in $\{\boldsymbol{0}, \boldsymbol{1}, \dots, \boldsymbol{q^n} - \boldsymbol{2}\}$and $\boldsymbol{M} \in \boldsymbol{F_q^{n\times n}}\backslash\{\boldsymbol{0}\}$, and then sends $(\boldsymbol{Q}_1^k \otimes \boldsymbol{M} \otimes \tilde{\boldsymbol{Q}}_1^l, \dots, \boldsymbol{Q}_m^k \otimes \boldsymbol{M} \otimes \tilde{\boldsymbol{Q}}_m^l)$ to Alice.

Step 3 Alice computes $\mathbf{key}_A = \prod_{i=1}^m (\boldsymbol{Q}_i^k \otimes \boldsymbol{M} \otimes \tilde{\boldsymbol{Q}}_i^l)^{r_i}$.

Step 4 Bob computes $\mathbf{key}_B = \left(\prod_{i=1}^m \boldsymbol{Q}_i^{r_i}\right)^k \otimes \boldsymbol{M}^{\lfloor\frac{m}{2}\rfloor} \otimes \left(\prod_{i=1}^m \tilde{\boldsymbol{Q}}_i^{r_i}\right)^l$.

Through Protocol 1, Alice and Bob successfully negotiate a common key since

$$\mathrm{key}_B = \mathrm{key}_A = \prod_{i=1}^m \left(Q_i^k \otimes M \otimes \tilde{Q}_i^l\right)^{r_i} = \prod_{i=1}^m \left(Q_i^k\right)^{r_i} \otimes M^{\sum_{i=1}^m r_i} \otimes \prod_{i=1}^m \left(\tilde{Q}_i^l\right)^{r_i} = \left(\prod_{i=1}^m Q_i^{r_i}\right)^k \otimes M^{\lfloor\frac{m}{2}\rfloor} \otimes \left(\prod_{i=1}^m \tilde{Q}_i^{r_i}\right)^l = \mathrm{key}_B..$$

IV. THE ATTACK FOR THE ASYMMETRIC-COMPUTING KEY EXCHANGE PROTOCO

Below we give an attack against Protocol 1.

Theorem2 Given an oracle solving the discrete logarithm problem over F_{q^n}, there is a probabilistic polynomial-time algorithm that queries the oracle $4m$ polynomials times and solve the DTSPEM problem for $m > 3$.

According to Theorem 1 and Theorem 2, the asymmetric key exchange protocol by Mao [9] is not quantum resistant.

Lemma 3 Let A be a $m \times n$ matrix and B a $k \times l$ matrix. Given k, l, m, n and a $mk \times nl$ nonzero matrix $M = A \otimes B$, there is a polynomial-time algorithm to get a $m \times n$ matrix A' and a $k \times l$ matrix B' satisfying $A' = A/\lambda$ and $B' = \lambda B$ for some $\lambda \neq 0$.

Proof As in Definition 2, we take M as a block matrix with mn blocks, where each block is a $k \times l$ matrix. Since M is nonzero, there is a nonzero block $a_{ij}B = \lambda B$ for some $1 \le i \le m$, $1 \le j \le n$. Let $B' = \lambda B = a_{ij}B$. Comparing each block $a_{ij}B$with B', we can compute $a'_{ij} = a_{ij}/\lambda$. Let $A' = \left(a'_{ij}\right)_{m\times n}$. Then $A' = A/\lambda$. □

Below is our attack against the DTSPEM problem (and hence Protocol 1.)

ALGORITHM 1SOLVE THE DTSPEM PROBLEM

Input: The public parameters$\boldsymbol{Q_1}, \dots, \boldsymbol{Q_m}$and $\tilde{\boldsymbol{Q}}_1, \dots, \tilde{\boldsymbol{Q}}_m$. The eavesdropped data $\prod_{i=1}^m \boldsymbol{Q}_i^{r_i}$, $\prod_{i=1}^m \tilde{\boldsymbol{Q}}_i^{r_i}$ and $(\boldsymbol{Q}_1^k \otimes \boldsymbol{M} \otimes \tilde{\boldsymbol{Q}}_1^l, \dots, \boldsymbol{Q}_m^k \otimes \boldsymbol{M} \otimes \tilde{\boldsymbol{Q}}_m^l)$.

Output: the exchange key $\mathbf{key}_A$, i.e.,$\mathbf{key}_B$.

Step 1 If$\boldsymbol{Q}$is unkown, find an ergodic matrix $\boldsymbol{Q_0}$in $\{\boldsymbol{Q_1}, \dots, \boldsymbol{Q_m}, \tilde{\boldsymbol{Q}}_1, \dots, \tilde{\boldsymbol{Q}}_m\}$. If $\boldsymbol{Q}$ is known, let $\boldsymbol{Q_0} = \boldsymbol{Q}$.

Step 2 Following Lemma 3, compute $\boldsymbol{R_i}, \boldsymbol{M_i}, \boldsymbol{S_i} \in \boldsymbol{F_q^{n\times n}}$, such that $\boldsymbol{R_i} = \boldsymbol{\lambda_i} \boldsymbol{Q}_i^k$, $\boldsymbol{M_i} = \tilde{\boldsymbol{\lambda}}_i \boldsymbol{M}$,$\boldsymbol{S_i} = \frac{1}{\lambda_i\tilde{\lambda}_i}\tilde{\boldsymbol{Q}}_i^l$, for $\boldsymbol{1} \le \boldsymbol{i} \le \boldsymbol{m}$.

Step 3 Since $\boldsymbol{M}$ is a nonzero matrix, get $\boldsymbol{\sigma_i} \in \boldsymbol{F_q}$satisfying $\boldsymbol{M_i} = \boldsymbol{\sigma_i M_1}$.

Step 4 Compute discrete logarithms and have equations over the residue ring $\mathbb{Z}/(\boldsymbol{q^n} - \boldsymbol{1})\mathbb{Z}$

$$\frac{\boldsymbol{x_i}}{\boldsymbol{x_0}} = \mathbf{log}_{Q_0} \boldsymbol{Q_i},$$
$$\frac{\tilde{\boldsymbol{x}}_i}{\boldsymbol{x_0}} = \mathbf{log}_{Q_0} \tilde{\boldsymbol{Q}}_i,$$
$$\frac{\tilde{\boldsymbol{x}}_i \boldsymbol{l}}{\boldsymbol{x_0}} - \boldsymbol{v_i} = \mathbf{log}_{Q_0} \boldsymbol{S_i},$$
$$\frac{\boldsymbol{x_i k}}{\boldsymbol{x_0}} + \boldsymbol{u_i} = \mathbf{log}_{Q_0} \boldsymbol{R_i} + \mathbf{log}_{Q_0} \boldsymbol{\sigma_i I}.$$

Step 5 Adding in equations$\boldsymbol{u_i} + \boldsymbol{v_i} \equiv \boldsymbol{u_j} + \boldsymbol{v_j} \mathbf{mod} \boldsymbol{q^n} - \boldsymbol{1}$, $\boldsymbol{1} \le \boldsymbol{i}, \boldsymbol{j} \le \boldsymbol{m}$, compute $\boldsymbol{k}$ and $\boldsymbol{l}$.

Step 6 Compute $\boldsymbol{M} = \boldsymbol{Q}_0^{-(u_i+v_i)}\boldsymbol{M_1}and\mathbf{key}_A = \mathbf{key}_B = \left(\prod_{i=1}^m \boldsymbol{Q}_i^{r_i}\right)^k \otimes \boldsymbol{M}^{\lfloor\frac{m}{2}\rfloor} \otimes \left(\prod_{i=1}^m \tilde{\boldsymbol{Q}}_i^{r_i}\right)^l$.

Lemma 4 For the majority of numbers like $q^n - 1$, it is efficient to an ergodic matrix among $Q_1, \dots, Q_m$ if $m \ge e^\gamma \mathrm{loglog}(q^n - 1)$.

Proof The matrix $Q_i = Q^{x_i}$ is ergodic iff x_i is coprime to $q^n - 1$. Thus, $\Pr[\gcd(x_i, q^n - 1) = 1] = \phi(q^n - 1)/(q^n - 1)$, where ϕ is the Euler totient function. As the inferior limit of $\phi(k)\mathrm{loglog}k/k$ is $e^{-\gamma}$ by [15], where $\gamma =$ is the Euler constant. For most numbers $q^n - 1$, there exists at least one ergodic matrix among $Q_1, \dots, Q_m$ as long as $m \ge e^\gamma \mathrm{loglog}(q^n - 1)$. □

Proof of Theorem 2 Denote $x_0 = \log_Q Q_0$, $u_i = \log_{Q_0}(\lambda_i\sigma_i I)$, $v_i = \log_{Q_0}(\lambda_i\tilde{\lambda}_i I)$, where I is the identity matrix. Use the relation $\sigma_i Q_i^k \otimes \lambda_1 M \otimes \frac{1}{\lambda_i\tilde{\lambda}_i}\tilde{Q}_i^l = Q_i^k \otimes M \otimes \tilde{Q}_i^l$ .By the definition of Q_i and $\tilde{Q}_i$, we have $\frac{x_i}{x_0} = \log_{Q_0} Q_i$, and $\frac{\tilde{x}_i}{x_0} = \log_{Q_0} \tilde{Q}_i$. By $S_i = \frac{1}{\lambda_i\tilde{\lambda}_i}\tilde{Q}_i^l$, we have $\frac{\tilde{x}_i l}{x_0} - v_i = \log_{Q_0} S_i$. By $R_i = \lambda_i Q_i^k$, we have $\frac{x_i k}{x_0} + u_i = \log_{Q_0} R_i + \log_{Q_0}\sigma_i I = \log_{Q_0} Q_i^k + \log_{Q_0}\lambda_i I + \log_{Q_0}\sigma_i I$. Noticing $\sigma_i\lambda_1 = \tilde{\lambda}_i$, we have $\lambda_i\sigma_i \cdot \lambda_1 \cdot \lambda_i\tilde{\lambda}_i = 1$ and hence $u_i + v_i = \log_{Q_0}(\lambda_i\sigma_i I) + \log_{Q_0}(\lambda_i\tilde{\lambda}_i I) = -\log_{Q_0}(\lambda_1 I) \bmod q^n - 1$. Finally, taking $\frac{x_i}{x_0}$ and $\frac{\tilde{x}_i}{x_0}$ as known solved parameters, we have $3m - 1$ independent equations of $2m + 2$ variables. Similar to the proof of Lemma 4, since $x_1, \dots. x_m, \widetilde{x_1}, \dots. \widetilde{x_m}$ are uniformly chosen random numbers, with a high probability we have at least one among $\frac{x_1}{x_0}, \dots, \frac{x_m}{x_0}$(resp. $\frac{\tilde{x}_1}{x_0}, \dots, \frac{\tilde{x}_m}{x_0}$) coprime to $q^n - 1$. Then we can get the exact value of k and $l$in $\mathbb{Z}/(q^n - 1)\mathbb{Z}$. Thus, with a high probability we have the exact value of u_i, v_i and also λ_1. Thus, we get

$Q_0^{-(u_i+v_i)}M_1 = Q_0^{-\log_{Q_0}(\lambda_1 I)}M_1 = \frac{1}{\lambda_1}M_1 = M$. By Protocol 1, we can obtain the key $\mathrm{key}_A, \mathrm{key}_B$ directly.□

Corollary1 If protocol 1 has a parameter setup $m > 3$ and solving the discrete **logarithm** problem over F_{q^n} is efficient, then there is a probabilistic polynomial-time algorithm to compute the exchange key from eavesdropped data.

For example, **Mao** et al [9] proposed the parameter (F_{2^8},3,80) for Protocol 1, i.e., $q = 2^8, n = 3, m = 80$. The finite field $F_{2^{24}}$ is so small that the discrete logarithm problem is computable. Thus, Protocol 1 with such given parameter setup is not secure, even in the classical computing model instead of quantum computing .

V. A TOY EXAMPLE

In this subsection we give a toy example. We follow the example of the paper [9]. Use primitive polynomial $p(x) = x^3 + x^2 - 1$ in over finite field F_3, and its corresponding companion matrix (ergodic matrix) is

$$Q = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 1 \end{pmatrix}.$$

Choose $x_1 = 3, x_2 = 4, x_3 = 5, x_4 = 1$, and $\overline{x}_1 = 1, \overline{x}_2 = 5, \overline{x}_3 = 2, \overline{x}_4 = 6$, compute

$$Q_1 = Q^3 = \begin{pmatrix} 2 & 0 & 1 \\ 2 & 2 & 1 \\ 2 & 2 & 0 \end{pmatrix} Q_2 = Q^4 = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

$$Q_3 = Q^5 = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 1 \end{pmatrix} Q_4 = Q^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

$$\tilde{Q}_1 = Q^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 1 \end{pmatrix} \tilde{Q}_2 = Q^5 = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

$$\tilde{Q}_3 = Q^2 = \begin{pmatrix} 0 & 0 & 1 \\ 2 & 0 & 1 \\ 2 & 2 & 1 \end{pmatrix} \tilde{Q}_4 = Q^6 = \begin{pmatrix} 0 & 2 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

Alice chooses $r = (1,0,1,0)$, compute $\prod_{i=1}^{4} Q_i^{r_i}$ and $\prod_{i=1}^{4} \tilde{Q}_i^{r_i}$.

Bob chooses $2, 7$ and $M = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, compute $Q_1^2 \otimes_3 M \otimes_3 \tilde{Q}_1^7$, $Q_2^2 \otimes_3 M \otimes_3 \tilde{Q}_2^7$, $Q_3^2 \otimes_3 M \otimes_3 \tilde{Q}_3^7$, $Q_4^2 \otimes_3 M \otimes_3 \tilde{Q}_4^7$.

By protocol 1, we can achieve the exchange key

$$key = \begin{pmatrix} 2 & 1 & 1 & 1 & \cdots & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 1 & \cdots & 2 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Now suppose the attacker can get $(\prod_{i=1}^{4} Q_i^{r_i}, \prod_{i=1}^{4} \tilde{Q}_i^{r_i})$ and $Q_1^2 \otimes_3 M \otimes_3 \tilde{Q}_1^7$, $Q_2^2 \otimes_3 M \otimes_3 \tilde{Q}_2^7$, $Q_3^2 \otimes_3 M \otimes_3 \tilde{Q}_3^7$, $Q_4^2 \otimes_3 M \otimes_3 \tilde{Q}_4^7$ and try to compute the exchange key. Denote

$$Z_1 = \prod_{i=1}^{4} Q_i^{r_i} = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{pmatrix},$$

$$Z_2 = \prod_{i=1}^{4} \tilde{Q}_i^{r_i} = \begin{pmatrix} 2 & 0 & 1 \\ 2 & 2 & 1 \\ 2 & 2 & 0 \end{pmatrix},$$

$$C_1 = Q_1^2 \otimes_3 M \otimes_3 \tilde{Q}_1^7 = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 2 & 2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 2 & 2 & 2 & 2 \end{pmatrix}$$

$$C_2 = Q_2^2 \otimes_3 M \otimes_3 \tilde{Q}_2^7 = \begin{pmatrix} 1 & 1 & 1 & 2 & \cdots & 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 1 & \cdots & 2 & 1 & 2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 2 & 1 & 0 & 2 & \cdots & 0 & 2 & 1 & 0 \end{pmatrix}$$

$$C_3 = Q_3^2 \otimes_3 M \otimes_3 \tilde{Q}_3^7 = \begin{pmatrix} 0 & 2 & 0 & 0 & \cdots & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & \cdots & 1 & 0 & 0 & 2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 & 2 \end{pmatrix}$$

$$C_4 = Q_4^2 \otimes_3 M \otimes_3 \tilde{Q}_4^7 = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 2 & 2 & 0 & 2 & \cdots & 0 & 1 & 1 & 0 \end{pmatrix}$$

Following Algorithm 1, we can write C_1, C_2, C_3 and C_4 as $(\lambda_1 Q_1, \tilde{\lambda}_1 M, \frac{1}{\lambda_1 \tilde{\lambda}_1} \tilde{Q}_1), \cdots, (\lambda_4 Q_4, \tilde{\lambda}_4 M, \frac{1}{\lambda_4 \tilde{\lambda}_4} \tilde{Q}_4)$ in polynomial time. Because the number of matrix and the modular are too small, the data we achieve is $(Q_1^2, M, \tilde{Q}_1^7)$, $(Q_2^2, M, \tilde{Q}_2^7)$, $(Q_3^2, M, \tilde{Q}_3^7)$, $(Q_4^2, M, \tilde{Q}_4^7)$ .If we can solve the discrete logarithm problem, we can get $2m$ equations as follows:

$$\begin{cases} u_1 + x_1 k = 6 \\ u_2 + x_2 k = 8 \\ u_3 + x_3 k = 10 \\ u_3 + x_4 k = 2 \\ u_1 + v_1 + \tilde{x}_1 l = 7 \\ u_2 + v_1 + \tilde{x}_2 l = 35 \\ u_3 + v_1 + \tilde{x}_3 l = 14 \\ u_4 + v_1 + \tilde{x}_4 l = 42 \end{cases}$$

Because $x_i = \tilde{x}_i = 1$, we can easily solve this equations and achieve $(k = 2, l = 7)$. Then the exchange key can be recovered by (Z_1, Z_2, k, l).

VI. CONCLUSION

Since the quantum Shor's algorithm[2] has the ability to solve large integer factorization and the discrete logarithm problem, quantum resistant cryptography has been a hot topic. And there are many encryption and signature schemes are constructed. However, it is hitherto difficult to construct quantum-resistant key exchange protocols. In this paper, we present an attack to the quantum-resistant key exchange protocol proposed in paper [9]. Through our attack, we can restore the key by the transmitted data of the key exchange protocol, and prove that this protocol is not immune to quantum attacks.

REFERENCES

[1] Diffie W, Hellman M. New directions in cryptography[J]. Information Theory, IEEE Transactions on, 1976, 22(6):644-654.

[2] P. Shor, "Prolynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAMJ. Computing 26(5), pp.1484-1509, 1997.

[3] D. Simon. On the power of quantum computation. SIAM J. Comput., 26(5):1474-1483, 1997.

[4] D. Boneh and R. J. Lipton. Quantum Cryptanalysis of Hidden Linear Functions (Extended Abstract). In CRYPTO, papges 424-437, 1995.

[5] Daniel J. Bernstein. Introductions to post-quantum cryptography. Post-Quantum Cryptography 2009, pp1-14.

[6] WANG HouZhen, ZHANG HuanGuo, WANG ZhangYi, TANG Ming. Extended multivariate public key cryptosystems with secure encryption function. SCIENCE CHINA information Sciences. 2011 Vol. 54(6):1161-1171.

[7] P. L. Cayrel, R. Lindner, M. Ruckert, R. Silva. A Lattice-based Threshhold Ring Signature Scheme. In Proceedings of the First International Conference on Cryptology and in Information Security in Latin America, Puebla, 8-11 August, 2010, LNCS 6212, pp.255-272.

[8] C. Gentry, C. Peikert, V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC, ACM, 2008, pp.197-206.

[9] Shao-Wu Mao, Huan-Guo Zhang, Wan-Qing Wu, Hou-Zhen Wang. An Asymmetric-computing Key Exchange Protocol[C]. Advances in Cryptology, ChinaCrypt 2014, pp.135-149.

[10] Li J, Wan D. On the subset sum problem over finite fields[J]. Finite Fields and Their Applications, 2008, 14(4):911-929.

[11] Hillar C J, Lim L H. Most tensor problems are NP-hard[J]. Journal of the ACM(JACM), 2013, 60(6): 45.

[12] QU Peng-cheng,WANG Yue-hong,ZHAO Yong-zhe,YUAN Zhe,ZHANG Wen-rui, Characteristics of Ergodic Matrix over Finite Field,,Journal of Jilin University(Science Edition), 2012, 50(3): 523-526.

[13] GU Chunsheng,JING Zhengjun,YU Zhiming, Polynomial Time Algorithm for the Two-Side Exponentiation Problem about Ergodic Matrices over Finite Field,Wuhan University Journal of Natural Sciences ,2012, 17(3):233-237.

[14] PEI Shihui, ZHAO Hongwei, ZHAO Yongzhe,Public Key Cryptography Based on Ergodic Matrices over Finite Field, Wuhan University Journal of Natural Sciences,2006, 11(6):1525-1528.

[15] G.H.Hardy, E.M.Wright, An introduction to the theory of numbers (5th edition), Oxford University Press.