SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Cryptanalysis of a Lattice Based Key Exchange Protocol

Shaowu MAO [1], Pei ZHANG [1], Houzhen WANG [1*], Huanguo ZHANG [1] & Wanqing WU [1,2]

[1]*Computer School of Wuhan University, The Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan* 430072*, China;*
[2]*Hebei University, Baoding* 071002*, China*

Appendix A Preliminaries

First we give some relevant basic definitions and problems depictions. the notations can be seen in the table A1.

Given two integers $n, m(m > n)$ and a matrix $\mathbb{Z}_q^{n\times m}$, two types of m-dimensional q-ary lattices are defined as following:

$$\Lambda(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^t\mathbf{x} \mod q, \mathbf{x} \in \mathbb{Z}^n\}$$

$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{A}\mathbf{y} = 0 \mod q\}$$

The first q-ary lattice is generated by the rows of $\mathbf{A}$; the second contains all vectors that are orthogonal modulo q to the rows of $\mathbf{A}$.

The lattice problems SIS problem and ISIS problem in l_2 norm are defined as following:

Definition 1 ($SIS_{q,n,m,\beta}$)**.** The SIS is defined as follows: given integers $n, m, q(m > n\log q)$, a real β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the goal is to find an integer vector $\mathbf{s} \in \mathbb{Z}^m \setminus \{0\}$ satisfying $\mathbf{A}\mathbf{s} = 0 \mod q$ *and* $\| \mathbf{s} \| \leqslant \beta$.

It is well-known that the SIS problem is equivalent to finding some short nonzero vector in $\Lambda^{\perp}(\mathbf{A})$. The SIS problem is, in essence, to solve a system of diophantine equations, where it is easy to find many solutions that satisfy the equations, but it is hard to find a small solution. Also, the ISIS which is a variant of the SIS problem is defined as follows:

Definition 2 ($ISIS_{q,n,m,\beta}$)**.** The ISIS is as follows: given integers $n, m, q(m > n\log q)$, a real β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{0\}$, the goal is to find an integer vector $\mathbf{s} \in \mathbb{Z}^m \setminus \{0\}$ satisfying $\mathbf{A}\mathbf{s} = \mathbf{u} \mod q$ with $\| \mathbf{s} \| \leqslant \beta$.

The ISIS problem is equivalent to the problem of decoding an arbitrary integer point $\mathbf{s} \in \mathbb{Z}^m$ to within β on the lattice $\Lambda^{\perp}(\mathbf{A})$. For some appropriate parameters, the SIS/ISIS instances are guaranteed to have a solution. The following proposition states that SIS and ISIS are as hard as the worst-case problems in lattices.

Lemma 1. Given m and $\beta = poln(n)$, as well as any prime $q \geqslant \beta\sqrt{\omega(n\log n)}$, the problems $SIS_{q,n,m,\beta}$ and $ISIS_{q,n,m,\beta}$ in the average case are as hard as approximating $SIVP_\gamma$ and $GapSVP_\gamma$ in the worst case to within certain $\gamma = \beta \cdot O(\sqrt{n})$.

Definition 3 (CBi-ISIS problem and DBi-ISIS problem)**.** Given the parameters n, m, q and $m > n\log q$ as in ISIS problem, a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals to n. For any vectors $\mathbf{x} \in \mathbb{Z}$ with $\| \mathbf{x} \| \leqslant \beta$, and $\mathbf{y} \in \mathbb{Z}$ with $\| \mathbf{y} \| \leqslant \beta$, there exists two vector sets $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ which is linear independent with rows vectors of $\mathbf{A}$, and $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ which is linear independent with column vectors of $\mathbf{A}$, such that $< \mathbf{v}_i, \mathbf{x} >= 0 \mod q$ and $< \mathbf{u}_i, \mathbf{y} >= 0 \mod q (1 \leqslant i \leqslant n)$. The CBi-ISIS problem and the DBi-ISIS problem are defined as follows:

- **Computational Bi-ISIS (CBi-ISIS) problem**: given $\mathbf{A}\mathbf{x} + \mathbf{e}_1$ and $\mathbf{y}^t\mathbf{A} + \mathbf{e}_2^t$, the goal is to compute $\mathbf{y}^t\mathbf{A}\mathbf{x} \mod q$.
- **Decisional Bi-ISIS (DBi-ISIS) problem**: the goal is to distinguish between the two distributions $(\mathbf{A}, \mathbf{A}\mathbf{x}+\mathbf{e}_1, \mathbf{y}^t\mathbf{A}+\mathbf{e}_2^t, \mathbf{y}^t\mathbf{A}\mathbf{x})$ and $(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{e}_1, \mathbf{y}^t\mathbf{A} + \mathbf{e}_2^t, \mathbf{z})$, where $\mathbf{z} \in \mathbb{Z}_q$ are chosen uniformly at random.

where $\mathbf{e}_1 = \sum_{i\in S} \mathbf{u}_i \mod q$ by using $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$, where $S \subseteq \{1, \cdots, n\}$ is a random subset, $\mathbf{e}_2^t = \sum_{i\in S'} \mathbf{v}_i^t \mod q$ by using $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$, where $S' \subseteq \{1, \cdots, n\}$ is a random subset.

* Corresponding author (email: whz@whu.edu.cn)

Table A1 Notations:

$\mathbb{Z}$ is the ring of integers	$\mathbb{Z}_q$ is the finite field module q
$\mathbb{Z}_q^{m\times m}$ is the space of $m\times m$-dimensional matrices in $\mathbb{Z}_q$	$\|\cdot\|$ is the l_2 Euclidean norm
capital bold letter is a matrix such as $\mathbf{A}$	0 : is a zeros matrix or zeros vector
lowercase bold letter is a column vector such as $\mathbf{x}$	$<\mathbf{x},\mathbf{y}>$ is an inner product of $\mathbf{x},\mathbf{y}$
$\mathbf{x}^t$ is the transposition of $\mathbf{x}$	$rank(\cdot)$ is the rank in $\mathbb{Z}_q^{m\times m}$

Appendix B The Details of Our Attack

The security of WANG et al.'s key exchange protocol is based on the hardness assumption of CBi-ISIS problem and DBi-ISIS problem, the definitions of CBi-ISIS problem and DBi-ISIS problem is depicted in definition 3. Our attack core idea is based on attacking the CBi-ISIS problem.

Appendix B.1 The Main Notations of Our Attack

Some elements are used in our method, for giving a clear description our attack, firstly we give some notations. We let

$$\Delta^{\perp}(\mathbf{A})=\{\mathbf{t}\in\mathbb{Z}_q^m:\mathbf{A}\mathbf{t}=0 \mod q\},\Delta^{\perp}(\mathbf{A}^t)=\{\mathbf{s}\in\mathbb{Z}_q^m:\mathbf{A}^t\mathbf{s}=0 \mod q\}$$

$$\Delta^{\perp}(\mathbf{V})=\{\mathbf{t}\in\mathbb{Z}_q^m:\mathbf{V}\mathbf{t}=0 \mod q\},\Delta^{\perp}(\overline{\mathbf{U}}^t)=\{\mathbf{s}\in\mathbb{Z}_q^m:\overline{\mathbf{U}}^t\mathbf{s}=0 \mod q\},$$

where $\mathbf{V}=\begin{pmatrix}\mathbf{v}_1^t\\ \vdots\\ \mathbf{v}_n^t\end{pmatrix}\in\mathbb{Z}_q^{n\times m},\overline{\mathbf{U}}=\begin{pmatrix}\mathbf{u}_1\Big|\cdots\Big|\mathbf{u}_n\end{pmatrix}\in\mathbb{Z}_q^{m\times n}$, $\mathbf{v}_1,\cdots,\mathbf{v}_n$ and $\mathbf{u}_1,\cdots,\mathbf{u}_n$ are column vectors which are same with Step 2 in the key exchange protocol of WANG et al.

$\Delta^{\perp}(\mathbf{A}),\Delta^{\perp}(\mathbf{A}^t),\Delta^{\perp}(\mathbf{V})$ and $\Delta^{\perp}(\overline{\mathbf{U}}^t)$ are four vectors space, they are generated by $\mathbf{A}$, $\mathbf{A}^t$, $\mathbf{V}$ and $\overline{\mathbf{U}}^t$ respectively.

For convenience, we denote the perturbation vector $\sum\limits_{i\in S}\mathbf{u}_i$ and $\sum\limits_{i\in S'}\mathbf{v}_i^t$ as

$$\mathbf{e}_1=\sum_{i\in S}\mathbf{u}_i=\overline{\mathbf{U}}^t\mathbf{z}_1,\mathbf{e}_2^t=\sum_{i\in S'}\mathbf{v}_i^t=\mathbf{z}_2^t\mathbf{V}$$

where $\mathbf{z}_1$ and $\mathbf{z}_2$ are vectors in $\{0,1\}^n$, because $S\subseteq\{1,\cdots,n\}$ and $S'\subseteq\{1,\cdots,n\}$ are random subsets, and $\mathbf{z}_1$ is known by Alice, $\mathbf{z}_2$ is known by Bob.

Appendix B.2 The Details of Our Attack

Definition 4 (Permutation Matrix)**.** A permutation matrix is a square binary matrix that has exactly one entry 1 in each row and each column and 0s elsewhere, usually denote it as $\mathbf{P}$.

Each permutation matrix represents a specific permutation of m elements, and a permutation matrix can produce that permutation in the rows or columns of the other matrix when permutation matrix is used to multiply another matrix.

The permutation matrix has some properties: (i)det($\mathbf{P}$) = ±1, (ii) $\mathbf{P}^{-1}=\mathbf{P}^t$.

Lemma 2. [1] Any n-by-n matrix over a field can be written as

$$\mathbf{A}=\mathbf{PLU}$$

where $\mathbf{P}$ is a permutation matrix, $\mathbf{L}$ is a lower triangular invertible matrix and $\mathbf{U}$ is an upper triangular matrix.

The PLU decomposition is an extension of the Gaussian elimination algorithm, and it can use to the case of not necessarily invertible matrices. When $\mathbf{A}$ is an invertible matrix, the $\mathbf{U}$ is invertible. When $\mathbf{A}$ is a non-invertible matrix with $rank(\mathbf{A})=k$, the $\mathbf{U}$ is a non-invertible matrix with (k+1)th to n-th are zeros.

Theorem 1. For parameters $m>n$, a matrix $\mathbf{A}\in\mathbb{Z}_q^{m\times m}$ with rank($\mathbf{A}$)=n, by PLU decomposition the $\mathbf{A}$ can written as:

$$\mathbf{A}=\mathbf{PLU}=\mathbf{U}_1^t\mathbf{L}_1^t\mathbf{P}_1^t,$$

where $\mathbf{P},\mathbf{L},\mathbf{U}$ is the PLU decomposition of $\mathbf{A}$. $\mathbf{P}_1,\mathbf{L}_1,\mathbf{U}_1$ is the PLU decomposition of $\mathbf{A}^t$, $\mathbf{P},\mathbf{P}_1$ is a permutation matrix, $\mathbf{L},\mathbf{L}_1$ is a lower triangular invertible matrix, $\mathbf{U},\mathbf{U}_1$ is an upper triangular singular matrix with $(n+1)$-th to m-th rows are zeros.

Proof. From the lamma 2, the PLU decomposition of $\mathbf{A}$ is $\mathbf{A}=\mathbf{PLU}$, and the PLU decomposition of $\mathbf{A}^t$ is $\mathbf{A}^t=\mathbf{P}_1\mathbf{L}_1\mathbf{U}_1$, where $\mathbf{P},\mathbf{P}_1$ is a permutation matrix, $\mathbf{L},\mathbf{L}_1$ is a lower triangular invertible matrix, $\mathbf{U},\mathbf{U}_1$ is an upper triangular singular matrix with $(n+1)$-th to m-th rows are zeros. Then we can obtain $\mathbf{A}=\mathbf{PLU}=\mathbf{U}_1^t\mathbf{L}_1^t\mathbf{P}_1^t$ directly.

Lemma 3 (rank+nullity theorem)**.** [2] If T is a linear transformation from a finite-dimensional vector space V to a finite-dimensional vector space W , then $\dim(V)=rank(T)+nullity(T)$, where $rank(T)=\dim(im(T))$ and $nullity(T)=\dim(ker(T))$, where $im(T)$ is the image space of T, $ker(T)=\{\alpha:T\alpha=0,\alpha\in V\}$.

Theorem 2. Given a m-dimension vectors space $\mathbb{Z}_q^{m\times m}$ and $\mathbf{A}\in\mathbb{Z}_q^{m\times m}$ whit $rank(\mathbf{A})=n$, then

$$\dim(\Delta^{\perp}(\mathbf{A}))=\dim(\Delta^{\perp}(\mathbf{A}^t))=m-n.$$

Proof. Because $\dim(\mathbb{Z}_q^{m\times m})=m$, from the rank+nubillity theorem 3, we know that $\dim(\mathbb{Z}_q^{m\times m})=rank(A)+nullity(A)$, where $nullity(A)=\dim(\Delta^{\perp}(\mathbf{A}))$ or $nullity(A)=\dim(\Delta^{\perp}(\mathbf{A}^t))$, thus $\dim(\Delta^{\perp}(\mathbf{A}))=\dim(\Delta^{\perp}(\mathbf{A}^t))=m-n$.

Corollary 1. Given a m-dimension vectors space $\mathbb{Z}_q^{m\times m}$, $\mathbf{V}\in\mathbb{Z}_q^{n\times m}$ and $\overline{\mathbf{U}}\in\mathbb{Z}_q^{m\times n}$ with $rank(\mathbf{V})=rank(\overline{\mathbf{U}})=n$, then $\dim(\Delta^{\perp}(\mathbf{V}))=\dim(\Delta^{\perp}(\overline{\mathbf{U}}^t))=m-n$.

The Corollary can be proofed similarly with proposition 2.

Theorem 3. Given $\overline{\mathbf{U}}\in\mathbb{Z}_q^{m\times n}$, whose columns are linear independent with column vectors of $\mathbf{A}$, if $\mathbf{T}^t\in\mathbb{Z}_q^{m\times(m-n)}$ is one basis of $\Delta^{\perp}(\mathbf{A}^t)$, thus $rank(\mathbf{T}\overline{\mathbf{U}})=n$.

Proof. From the condition of $\overline{\mathbf{U}}\in\mathbb{Z}_q^{m\times n}$ are linear independent with column vectors of $\mathbf{A}$, then $rank(\begin{pmatrix}\mathbf{A}^t\\ \overline{\mathbf{U}}^t\end{pmatrix})=2n$. We know that

$$\dim(\Delta^{\perp}(\mathbf{A}^t)\cap\Delta^{\perp}(\overline{\mathbf{U}}^t))=m-2n. \tag{B1}$$

And because $\overline{\mathbf{U}}\in\mathbb{Z}_q^{m\times n}$ and $\mathbf{T}^t\in\mathbb{Z}_q^{m\times(m-n)}$, then $\overline{\mathbf{U}}^t\mathbf{T}^t\in\mathbb{Z}^{n\times(m-n)}$, we have $rank(\overline{\mathbf{U}}^t\mathbf{T}^t)\leqslant n$.

Assume $rank(\overline{\mathbf{U}}^t\mathbf{T}^t)<n$, we can assume that $rank(\overline{\mathbf{U}}^t\mathbf{T}^t)=n-1$ and denote $\overline{\mathbf{U}}^t\mathbf{T}^t=\mathbf{S}$, then there exists an invertible matrix $\mathbf{P}\in\mathbb{Z}_q^{(m-n)\times(m-n)}$ to make sure

$$\overline{\mathbf{U}}\mathbf{T}^t\mathbf{P}=\mathbf{S}\mathbf{P}=\mathbf{S}'$$

such that from the n-th to the $(m-n)$-th columns of $\mathbf{S}'$ are zeros. Because $\mathbf{T}^t\mathbf{P}$ is column full rank, which means that it is still a basis of $\Delta^{\perp}(\mathbf{A}^t)$, and the n-th to the $(m-n)$-th columns of $\mathbf{T}^t\mathbf{P}$ still belong to the basis of $\Delta^{\perp}(\overline{\mathbf{U}})$. Then $\dim(\Delta^{\perp}(\mathbf{A}^t)\cap\Delta^{\perp}(\overline{\mathbf{U}}))>(m-n)-(n-1)=m-2n+1$, which contradicts the equation B1, thus the assumption does not establish. Hence we conclude that $rank(\mathbf{T}\overline{\mathbf{U}})=n$.

Similar with the proposition 3, we have the following corollary.

Corollary 2. Given $\mathbf{V}\in\mathbb{Z}_q^{n\times m}$ are linear independent with row vectors of $\mathbf{A}$, thus if $\mathbf{T}\in\mathbb{Z}_q^{m\times(m-n)}$ is one basis of $\Delta^{\perp}(\mathbf{A})$, thus $rank(\mathbf{V}\mathbf{T})=n$.

From Kerchkhoff's principle, the attacker may intercept Alice's public key $\mathbf{b}_1=\mathbf{A}\mathbf{x}+\mathbf{e}_1$ and Bob's public key $\mathbf{b}_2^t=\mathbf{y}^t\mathbf{A}+\mathbf{e}_2^t$. Let n,m,q be the parameters as in the key exchange protocol of WANG et al. The analysis procedure can be seen as follows:

(i) For $\mathbf{b}_1=\mathbf{A}\mathbf{x}+\mathbf{e}_1$, firstly we find $\mathbf{T}_1\in\mathbb{Z}_q^{(m-n)\times m}$ satisfying $\mathbf{T}_1\mathbf{A}=0 \mod q$ with $rank(\mathbf{T}_1)=m-n$, which means that $\mathbf{T}_1^t$ is one basis of space $\Delta^{\perp}(\mathbf{A}^t)=\{\mathbf{y}\in\mathbb{Z}_q^m:\mathbf{A}^t\mathbf{y}=0 \mod q\}$. If $\mathbf{X}$ satisfy $\mathbf{X}\mathbf{A}=0 \mod q$, then

$$\begin{aligned}\mathbf{X}\mathbf{A} &= 0 \mod q\\ \mathbf{X}\mathbf{U}_1^t\mathbf{L}_1^t\mathbf{P}_1^t &= 0 \mod q\\ \mathbf{X}\mathbf{U}_1^t &= 0(\mathbf{L}_1^t\mathbf{P}_1^t)^{-1}=0 \mod q\end{aligned}$$

Then because the $(n+1)$-th to m-th columns in $\mathbf{U}_1^t$ are zeros we can get a $\mathbf{T}_1\in\mathbb{Z}^{(m-n)\times m}$ satisfying $\mathbf{T}_1\mathbf{U}_1^t=\mathbf{V}(\mathbf{L}_1^t)^{-1}$, which means that $\mathbf{T}_1\in\mathbb{Z}^{(m-n)\times m}$ is obtained to satisfy $\mathbf{T}_1\mathbf{A}=0 \mod q$. Next we left multiply $\mathbf{b}_1$ with $\mathbf{T}_1$,

$$\mathbf{T}_1\mathbf{b}_1=\mathbf{T}_1(\mathbf{A}\mathbf{x}+\mathbf{e}_1)=\mathbf{T}_1\mathbf{A}\mathbf{x}+\mathbf{T}_1\mathbf{e}_1=0\mathbf{x}+\mathbf{T}_1\mathbf{e}_1=\mathbf{T}_1\mathbf{e}_1=\mathbf{T}_1\overline{\mathbf{U}}\mathbf{z}_1 \mod q \tag{B2}$$

Because from proposition 3 we know $rank(\mathbf{T}_1\overline{\mathbf{U}}^t)=n$ and $\mathbf{T}_1\mathbf{b}_1\in\mathbb{Z}^{m\times 1}$ is known, from the equation B2, we can obtain the $\mathbf{z}_1\in\{0,1\}^n$, then

$$\mathbf{A}\mathbf{x}=\mathbf{b}_1-\overline{\mathbf{U}}\mathbf{z}_1 \mod q$$

(ii) For $\mathbf{b}_2^t=\mathbf{y}^t\mathbf{A}+\mathbf{e}_2^t$, similarly, we find firstly $\mathbf{T}_2\in\mathbb{Z}^{m\times(m-n)}$ satisfying $\mathbf{A}\mathbf{T}_2=0 \mod q$ with $rank(\mathbf{T}_2)=m-n$, which means that $\mathbf{T}_2$ is a basis of space $\Delta^{\perp}(\mathbf{A})=\{\mathbf{y}\in\mathbb{Z}_q^m:\mathbf{A}\mathbf{y}=0 \mod q\}$. If $\mathbf{A}\mathbf{X}=0 \mod q$, then

$$\begin{aligned}\mathbf{A}\mathbf{X} &= 0 \mod q\\ \mathbf{P}\mathbf{L}\mathbf{U}\mathbf{X} &= 0 \mod q\\ \mathbf{U}\mathbf{X} &= (\mathbf{P}\mathbf{L})^{-1}0=0 \mod q\end{aligned}$$

Then because the $(n+1)$-th to m-th rows in $\mathbf{U}$ are zeros we can get a $\mathbf{T}_2\in\mathbb{Z}^{m\times m\times(m-n)}$ satisfying $\mathbf{U}\mathbf{T}_2=0 \mod q$, which means that $\mathbf{A}\mathbf{T}_2=0 \mod q$. Next we right multiply $\mathbf{b}_2^t$ with $\mathbf{T}_2$,

$$\mathbf{b}_2^t\mathbf{T}_2=(\mathbf{y}^t\mathbf{A}+\mathbf{e}_2^t)\mathbf{T}_2=\mathbf{y}^t\mathbf{A}\mathbf{T}_2+\mathbf{e}_2^t\mathbf{T}_2=\mathbf{y}^t0+\mathbf{z}_2^t\mathbf{V}\mathbf{T}_2=\mathbf{z}_2^t\mathbf{V}\mathbf{T}_2 \mod q \tag{B3}$$

Because from the corollary 2 we know $rank(\mathbf{V}\mathbf{T}_2)=n$ and $\mathbf{b}_2^t\mathbf{T}_2\in\mathbb{Z}^{1\times(m-n)}$ is known, from the equation B3, we can obtain the $\mathbf{z}_2\in\{0,1\}^n$, then we can compute $\mathbf{y}^t\mathbf{A}$ through

$$\mathbf{y}^t\mathbf{A}=\mathbf{b}_2^t-\mathbf{z}_2^t\mathbf{V}$$

(iii) For the obtained $\mathbf{A}\mathbf{x}$ and $\mathbf{y}^t\mathbf{A}$, we denote

$$\mathbf{A}\mathbf{x}=\mathbf{k}_1 \mod q, \mathbf{y}^t\mathbf{A}=\mathbf{k}_2^t \mod q.$$

Table C1 Recovering the Shared Key by Attack Algorithm

n	m	q	design security	time	result
128	3854	10007	2^{128}	27842.891801 seconds.	Success
80	3240	6421	2^{80}	8201.055194 seconds	Success
64	1536	4099	2^{64}	1638.645816 seconds.	Success

From the PLU decomposition of $\mathbf{A} = \mathbf{PLU}$ with $rank(\mathbf{U}) = n$, then

$$\mathbf{PLUx} = \mathbf{k}_1 \mod q, \mathbf{y}^t\mathbf{PLU} = \mathbf{k}_2 \mod q.$$

Thus the $\mathbf{Ux} = (\mathbf{PL})^{-1}\mathbf{k}_1 \mod q$ can be obtained.

Besides, for $\mathbf{y}^t\mathbf{PLU} = \mathbf{k}_2^t \mod q$, we can find $\mathbf{y}'$ satisfying $\mathbf{y}'^t\mathbf{U} = \mathbf{k}_2^t = \mathbf{y}^t\mathbf{PLU} \mod q$. $\mathbf{y}'^t\mathbf{U} = \mathbf{k}_2^t$ must have solution because $\mathbf{y}^t\mathbf{PL}$ is a trivial solution. Essentially, the $\mathbf{y}'^t$ is the first n components of $\mathbf{y}^t\mathbf{PL}$, it is determined by the form of the $\mathbf{U}$ in proposition 1.

From the above, we can compute the share key through

$$\mathbf{y}'^t(\mathbf{PL})^{-1}\mathbf{k}_1 \mod q,$$

because

$$\mathbf{y}'^t(\mathbf{PL})^{-1}\mathbf{k}_1 = \mathbf{y}'^t\mathbf{Ux} = (\mathbf{y}'^t\mathbf{U})\mathbf{x} = \mathbf{k}_2^t\mathbf{x} = \mathbf{y}^t\mathbf{PLUx} = \mathbf{y}^t\mathbf{Ax} \mod q. \tag{B4}$$

Appendix B.3 Correctness

The correctness of algorithm 2 can be seen from the above analysis (i) (ii) (iii), especially the equations B2, B3, B4.

Appendix B.4 Computational Complexity

We need $O(\frac{4m^3}{3})$ multiplications to compute the $\mathbf{T}_1$, $\mathbf{T}_2$ based on the PLU factorization at average, $O(4n^3)$ multiplications to compute $\mathbf{z}_1$, $\mathbf{z}_2$, $O(2mn)$ multiplications to compute $\mathbf{k}_1$, $\mathbf{k}_2$, $O(m^2)$ multiplications to compute $(\mathbf{PL})^{-1}$. $O(n^2/2)$ multiplications to compute $\mathbf{y}'$. $O(m^2)$ multiplications to compute $\mathbf{y}'^t(\mathbf{PL})^{-1}\mathbf{k}_1 \mod q$. So the shared key algorithm can be done after $O(\frac{4m^3}{3})$ multiplications to compute the shared key. The basic operation is multiplication in the finite field $\mathbb{Z}_q$.

Appendix C Experimental Results

We implemented the attack on a platform which is an Intel Dual-Core2, CPU 2.6Ghz, Windows 7 operating system with 4G storage memory, we use the MATLAB version 7.9 to implement it. The scheme we attack is the experiment in [3], $q = n^2$, $m = 4n\log n$ they suggested, the parameters $n = 64$, $m = 1536$, $q = 4099$ is a suggested parameter in their experiment. The result is as same as the theoretical analysis, the key can be correctly recovered. In the experiment, the most time-consuming operation in the attack algorithm is PLU decomposition, however the PLU operations can also be implemented in polynomial time. The experiment results can be seen in table C1.

We tested 10 random instances for every (n, m, q), experimental results showed that the attack performed less slowly than the theoretical results indicated, one reason was that the experiment platform was not taken into account by theoretical analysis. If we adopted other platform with object oriented language, the attack time must be more quickly.

References

1 Okunev P, Johnson C R. Necessary And Sufficient Conditions For Existence of the LU Factorization of an Arbitrary Matrix. arXiv preprint math/0506382, 2005.
2 Alama J. The rank+ nullity theorem. Formalized Mathematics, 2007, 15(3): 137-142.
3 Wang S B, Zhu Y, Ma D, et al. Lattice-based key exchange on small integer solution problem. Sci China Ser F-Inf, 2014, 57(11): article No.112111.