SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

February 2017, Vol. 60 028101:1–028101:3
doi: 10.1007/s11432-015-0721-4

Cryptanalysis of a lattice based key exchange protocol

Shaowu MAO[1,3], 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]*School of Computer Science and Technology, Hebei University, Baoding* 071002*, China;*
[3]*Huawei Technoligies Co., Ltd., Xi'an* 710077*, China*

Received September 8, 2016; accepted October 24, 2016; published online December 29, 2016

Citation Mao S W, Zhang P, Wang H Z, et al. Cryptanalysis of a lattice based key exchange protocol. Sci China Inf Sci, 2017, 60(2): 028101, doi: 10.1007/s11432-015-0721-4

A lattice is a set of points in n-dimensional space with a periodic structure. Lattice-based cryptosystem holds a great promise for post-quantum cryptography [1], as they enjoy very strong security proofs based on the worst-case hardness, relatively efficient implementations, as well as great simplicity. The first lattice-based cryptosystem was proposed by Ajtai and Dwork [2], whose security is based on the lattice problems in the worst-case. After their seminal work, several lattice-based cryptosystems have been proposed till now, such as collision-resistant hash functions [3], signature schemes [4], encryption schemes [5], and other primitives [6]. Most of lattices in these lattice-based cryptosystems are q-ary lattices. In the q-ary lattices the small integer solution (SIS) problem, inhomogeneous small integer solution (ISIS) problem and learning with errors problem (LWE) have been researched widely because of its enjoying in worst-case hardness guarantees [7].

In 2014, Wang et al. [8] proposed a lattice-based key exchange protocol based on the small integer solution (SIS) problem. In 2016, Gupta et al. introduced a man in the middle attack against the scheme. But this introduction was no novelty, because the authors of the original paper [9] already considered this aspect. In this article, we present an efficient shared key attack algorithm which runs in polynomial time against the protocol to recover the shared key, and experimental results also show that the attack algorithm succeeds to recover the shared key efficiently. This renders Wang's lattice-based key exchange protocol insecure. To the best of our knowledge, it is the first efficient cryptanalysis of the Wang et al.'s lattice-based key exchange protocol.

Notations. First, we establish some 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; Capitalized bold letter indicates a matrix, such as $\boldsymbol{A}$; $\mathbf{0}$ is a zeros matrix or zeros vector; lowercase bold letter indicates a column vector, such as $\boldsymbol{x}$; $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ is an inner product of $\boldsymbol{x}, \boldsymbol{y}$; $\boldsymbol{x}^{\mathrm{T}}$ is the transposition of $\boldsymbol{x}$; rank$(\cdot)$ is the rank in $\mathbb{Z}_q^{m\times m}$.

Description of the protocol [8]. Before we describe the key exchange protocol of Wang et al., let us first introduce some problems in their paper. In [8], they extended the SIS and ISIS problems to Bilateral SIS problem and Bilateral ISIS problem.

* Corresponding author (email: whz@whu.edu.cn)
The authors declare that they have no conflict of interest.

They denoted the corresponding problems by Bi-SIS and Bi-ISIS, respectively.

Definition 1 (Bi-SIS problem)**.** The Bi-SIS is as follows: given integers n, m, q ($m > n\log q$), a real β and a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals to n, the goal is to find two nonzero integer vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^m \setminus \{\boldsymbol{0}\}$ that satisfy

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \mod q \quad \text{and} \quad \|\boldsymbol{x}\| \leqslant \beta, \\ \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} = \boldsymbol{0} \mod q \quad \text{and} \quad \|\boldsymbol{y}\| \leqslant \beta. \end{cases}$$

Definition 2 (Bi-ISIS problem)**.** The Bi-ISIS is as follows: given integers n, m, q ($m > n\log q$), a real β and a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals to n, two vectors $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \mathbb{Z}_q^m$, the goal is to find two integer vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^m \setminus \{\boldsymbol{0}\}$ that satisfy

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}_1 \mod q \quad \text{and} \quad \| \boldsymbol{x} \| \leqslant \beta, \\ \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} = \boldsymbol{b}_2^{\mathrm{T}} \mod q \quad \text{and} \quad \| \boldsymbol{y} \| \leqslant \beta. \end{cases}$$

Lemma 1 ([8])**.** The new problems Bi-$\mathrm{SIS}_{q,m,\beta}$/Bi-$\mathrm{ISIS}_{q,m,\beta}$ are as hard as the $\mathrm{SIS}_{q,m,\beta}$/$\mathrm{ISIS}_{q,m,\beta}$ problems.

Improvement is made to provide double-side operations between square matrices and row/column vectors; however, the Bi-SIS and Bi-ISIS problems are as hard as SIS and ISIS problems, respectively.

They also extended Bi-ISIS to the following problem.

Definition 3 (Bi-ISIS* problem)**.** Given integers n, m, q ($m > n\log q$), a real β as in SIS, and a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals to n, $\boldsymbol{e}_1$ is linearly independent with column vectors of $\boldsymbol{A}$, $\boldsymbol{e}_2$ is linearly independent with row vectors of $\boldsymbol{A}$, given vectors $\boldsymbol{b}_1 \in \{\boldsymbol{A}\boldsymbol{z} + \boldsymbol{e}_1 : \boldsymbol{z} \in \mathbb{Z}^m, \langle \boldsymbol{e}_2, \boldsymbol{z}\rangle = 0 \mod q\}$ and $\boldsymbol{b}_2^{\mathrm{T}} \in \{\boldsymbol{z}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}} : \boldsymbol{z} \in \mathbb{Z}^m, \langle \boldsymbol{e}_1, \boldsymbol{z}\rangle = 0 \mod q\}$, the goal is to find a vector $\boldsymbol{x} \in \mathbb{Z}^m$ and a vector $\boldsymbol{y} \in \mathbb{Z}^m$, such that

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1 = \boldsymbol{b}_1 \mod q \quad \text{and} \quad \|\boldsymbol{x}\| \leqslant \beta, \\ \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}} = \boldsymbol{b}_2^{\mathrm{T}} \mod q \quad \text{and} \quad \|\boldsymbol{y}\| \leqslant \beta. \end{cases}$$

In [8], they said that when $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ are given, the Bi-ISIS* problem is essentially a Bi-ISIS problem. However, from our analysis, we showed that the Bi-ISIS* problem is not as hard as Bi-ISIS problem when $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$ are given.

Definition 4 (CBi-ISIS problem and DBi-ISIS problem)**.** Given the parameters n, m, q and $m > n\log q$ as in the ISIS problem, a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals to n. For any vectors $\boldsymbol{x} \in \mathbb{Z}$ with $\|\boldsymbol{x}\| \leqslant \beta$, and $\boldsymbol{y} \in \mathbb{Z}$ with $\|\boldsymbol{y}\| \leqslant \beta$, there exists two vector sets: $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ which is linearly independent with rows vectors of $\boldsymbol{A}$, and $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ which is linearly independent with column vectors of $\boldsymbol{A}$, such that $\langle \boldsymbol{v}_i, \boldsymbol{x}\rangle = 0 \mod q$ and $\langle \boldsymbol{u}_i, \boldsymbol{y}\rangle = 0 \mod q$ ($1 \leqslant i \leqslant n$). The CBi-ISIS problem and the DBi-ISIS problem are defined as follows:

Computational Bi-ISIS (CBi-ISIS) problem. Given $\boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1$ and $\boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}$, the goal is to compute $\boldsymbol{y}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{x} \mod q$.

Decisional Bi-ISIS (DBi-ISIS) problem. The goal is to distinguish between the two distributions $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1, \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}, \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{x})$ and $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1, \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}, \boldsymbol{z})$, where $\boldsymbol{z} \in \mathbb{Z}_q$ are chosen uniformly at random, $\boldsymbol{e}_1 = \sum_{i\in S} \boldsymbol{u}_i \mod q$ by using $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$, $S \subseteq \{1, \ldots, n\}$ is a random subset, $\boldsymbol{e}_2^{\mathrm{T}} = \sum_{i\in S'} \boldsymbol{v}_i^{\mathrm{T}} \mod q$ by using $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$, and $S' \subseteq \{1, \ldots, n\}$ is a random subset.

We present a simple description of the scheme proposed by Wang et al. The more details of key exchange procedure can be seen in [8]. Wang et al. provided some suggestions for the parameters: q is a prime($\approx n^2$), $m = 2n\log q$, and a concrete parameter selection in their experiment: $n = 64$, $q = 4099(\approx n^2)$, $m = 1536(\approx 2n\log q)$.

Our attack. The security of Wang et al.'s key exchange protocol is based on the hardness assumption of the CBi-ISIS problem and the DBi-ISIS problem; the definitions of CBi-ISIS and DBi-ISIS problem are described in Definition 4.

Some novel elements are used in our method. Therefore, for giving a clear description of our attack, we define some notations. We let $\Delta^{\perp}(\boldsymbol{A}) = \{\boldsymbol{t} \in \mathbb{Z}_q^m : \boldsymbol{A}\boldsymbol{t} = \boldsymbol{0} \mod q\}$, $\Delta^{\perp}(\boldsymbol{A}^{\mathrm{T}}) = \{\boldsymbol{s} \in \mathbb{Z}_q^m : \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} = \boldsymbol{0} \mod q\}$ $\Delta^{\perp}(\boldsymbol{V}) = \{\boldsymbol{t} \in \mathbb{Z}_q^m : \boldsymbol{V}\boldsymbol{t} = \boldsymbol{0} \mod q\}$, $\Delta^{\perp}(\overline{\boldsymbol{U}}^{\mathrm{T}}) = \{\boldsymbol{s} \in \mathbb{Z}_q^m : \overline{\boldsymbol{U}}^{\mathrm{T}}\boldsymbol{s} = \boldsymbol{0} \mod q\}$, where $\boldsymbol{V} = (\boldsymbol{v}_1^{\mathrm{T}} \ \cdots \ \boldsymbol{v}_n^{\mathrm{T}})^{\mathrm{T}} \in \mathbb{Z}_q^{n\times m}$, $\overline{\boldsymbol{U}} = (\,\boldsymbol{u}_1 \big| \cdots \big| \boldsymbol{u}_n\,) \in \mathbb{Z}_q^{m\times n}$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ are column vectors which are the same with Step 2 in Wang et al.'s key exchange protocol.

$\Delta^{\perp}(\boldsymbol{A}), \Delta^{\perp}(\boldsymbol{A}^{\mathrm{T}}), \Delta^{\perp}(\boldsymbol{V})$ and $\Delta^{\perp}(\overline{\boldsymbol{U}}^{\mathrm{T}})$ are four vectors space; which are generated by $\boldsymbol{A}$, $\boldsymbol{A}^{\mathrm{T}}$, $\boldsymbol{V}$ and $\overline{\boldsymbol{U}}^{\mathrm{T}}$, respectively.

For the sake of convenience, we denote the perturbation vector $\sum_{i\in S} \boldsymbol{u}_i$ and $\sum_{i\in S'} \boldsymbol{v}_i^{\mathrm{T}}$ as

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

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

Table 1 Recovering the shared key by Algorithm 1

n	m	q	DS	Time (s)	Result
128	3854	10007	2^{128}	27842.89	Success
80	3240	6421	2^{80}	8201.06	Success
64	1536	4099	2^{64}	1638.64	Success

The core idea of our attack is based on attacking the CBi-ISIS problem. We first describe the shared key attack method as in Algorithm 1.

Algorithm 1 Shared key attack

Input $\boldsymbol{A}$, $\boldsymbol{b}_1 = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1$, $\boldsymbol{b}_2^{\mathrm{T}} = \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}$, $\boldsymbol{V} = (\boldsymbol{v}_1^{\mathrm{T}} \ \cdots \ \boldsymbol{v}_n^{\mathrm{T}})^{\mathrm{T}}$ $\overline{\boldsymbol{U}} = (\,\boldsymbol{u}_1 \big| \cdots \big| \boldsymbol{u}_n\,)$.

Output The shared key.

Step1 PLU Factorization $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{L}\boldsymbol{U} \mod q$, $\boldsymbol{A}^{\mathrm{T}} = \boldsymbol{P}_1\boldsymbol{L}_1\boldsymbol{U}_1 \mod q$.

Step2 Solve $\boldsymbol{T}_1 \in \mathbb{Z}_q^{(m-n)\times m}$ satisfying $\boldsymbol{T}_1\boldsymbol{A} = \boldsymbol{0}$ through solving $\boldsymbol{U}_1\boldsymbol{T}_1^{\mathrm{T}} = \boldsymbol{0}$ with $\mathrm{rank}(\boldsymbol{T}_1) = m - n$.

Solve $\boldsymbol{T}_2 \in \mathbb{Z}_q^{m\times(m-n)}$ satisfying $\boldsymbol{A}\boldsymbol{T}_2 = \boldsymbol{0}$ through solving $\boldsymbol{U}\boldsymbol{T}_2 = \boldsymbol{0}$ with $\mathrm{rank}(\boldsymbol{T}_1) = m - n$.

Step3 Compute $\boldsymbol{T}_1\boldsymbol{b}_1 = \boldsymbol{T}_1\overline{\boldsymbol{U}}\boldsymbol{z}_1 \mod q$, then to obtain $\boldsymbol{z}_1$.

Compute $\boldsymbol{b}_2^{\mathrm{T}}\boldsymbol{T}_2 = \boldsymbol{z}_2^{\mathrm{T}}\boldsymbol{V}\boldsymbol{T}_2 \mod q$, then to obtain $\boldsymbol{z}_2$.

Step4 Compute $\boldsymbol{k}_1 = \boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}_1 - \overline{\boldsymbol{U}}\boldsymbol{z}_1 \mod q$ and $\boldsymbol{k}_2^{\mathrm{T}} = \boldsymbol{y}^{\mathrm{T}}\boldsymbol{A} = \boldsymbol{b}_2^{\mathrm{T}} - \boldsymbol{z}_2^{\mathrm{T}}\boldsymbol{V} \mod q$.

Step5 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{P}\boldsymbol{L}\boldsymbol{U}\boldsymbol{x} = \boldsymbol{k}_1 \mod q \Rightarrow \boldsymbol{U}\boldsymbol{x} = (\boldsymbol{P}\boldsymbol{L})^{-1}\boldsymbol{k}_1 \mod q$.

Solve $\boldsymbol{y}'$ satisfying $\boldsymbol{y}'^{\mathrm{T}}\boldsymbol{U} = \boldsymbol{y}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{L}\boldsymbol{U} = \boldsymbol{k}_2^{\mathrm{T}} \mod q$.

Step6 Return $\boldsymbol{y}'^{\mathrm{T}}(\boldsymbol{P}\boldsymbol{L})^{-1}\boldsymbol{k}_1 \mod q$.

Experimental results. We implemented the attack on a platform comprising an Intel Dual-Core, CPU with 2.6 GHz and Windows 7 operating system with 4 GB storage memory. We used MATLAB version 7.9 to implement it. The experiment results are shown in Table 1. Design security is denoted by DS.

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

Conlusion. As we have shown, the lattice based key exchange protocol proposed by Wang et al. is not secure because the shared key attack algorithm we presented in this work can efficiently recover the corresponding shared key in polynomial time. We proved that the shared key attack algorithm can recover the shared key correctly, and the experimental results support our view. In addition, we provide a simple attack example in the Appendix to illustrate our attack method.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61303212, 61202385, 61202386, 61303024, 61170080), State Key Program of National Natural Science of China (Grant Nos. 61332019, U1135004), National Basic Research Program of China (Grant No. 2014CB340600), Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-14-002), and Open Project of Beijing Key Lab of Trusted Computing (BJUT).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Zhang H G, Han W B, Lai X J, et al. Survey on cyberspace security. Sci China Inf Sci, 2015, 58: 110101
2 Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM, 1997. 284–293
3 Arbitman Y, Dogon G, Lyubashevsky V, et al. SWIFFTX: a proposal for the SHA-3 standard. 2008
4 Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal gaussians. In: Advances in Cryptology—CRYPTO 2013. Berlin: Springer, 2013. 40–56
5 Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Proceedings of the 11th International Conference on Topics in Cryptology: CT-RSA, San Francisco, 2011. 319–339
6 Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Advances in Cryptology—ASIACRYPT 2014. Berlin: Springer, 2014. 22–41
7 Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM J Comput, 2007, 37: 267–302
8 Wang S B, Zhu Y, Ma D, et al. Lattice-based key exchange on small integer solution problem. Sci China Inf Sci, 2014, 57: 112111
9 Gupta D S, Biswas G P. Cryptanalysis of Wang et al.'s lattice-based key exchange protocol. Perspect Sci, 2016, 8: 228–230