SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2014, Vol. 57 112111:1–112111:12
doi: 10.1007/s11432-014-5147-z

Lattice-based key exchange on small integer solution problem

WANG ShanBiao[1], ZHU Yan[2*], MA Di[3] & FENG RongQuan[1]

[1]*School of Mathematical Sciences, Peking University, Beijing* 100871*, China;*
[2]*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing* 100083*, China;*
[3]*Department of Computer and Information Science, University of Michigan-Dearborn, MI* 48128*, USA*

Received September 17, 2013; accepted January 20, 2014; published online September 15, 2014

Abstract In this paper, we propose a new hard problem, called bilateral inhomogeneous small integer solution (Bi-ISIS), which can be seen as an extension of the small integer solution problem on lattices. The main idea is that, instead of choosing a rectangle matrix, we choose a square matrix with small rank to generate Bi-ISIS problem without affecting the hardness of the underlying SIS problem. Based on this new problem, we present two new hardness problems: computational Bi-ISIS and decisional problems. As a direct application of these problems, we construct a new lattice-based key exchange (KE) protocol, which is analogous to the classic Diffie-Hellman KE protocol. We prove the security of this protocol and show that it provides better security in case of worst-case hardness of lattice problems, relatively efficient implementations, and great simplicity.

Keywords cryptography, lattices, small integer solutions, key exchange protocol, secure communications

Citation 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(12), doi: 10.1007/s11432-014-5147-z

1 Introduction

With the rapid development of new computing technologies, such as cloud computing, grid computing, as well as quantum information technology, the computing power grows more powerful and brings new challenges for the traditional cryptography. To meet these challenges, lattices have emerged in recent years as a rich platform on which to construct various cryptographic primitives, such as one-way functions and collision-resistant hash functions [1–3], oblivious transfer [4], public key encryption schemes [5–11], signatures [11–15], identity-based encryption [12,13,16,17], and fully homomorphic encryption schemes [18–22]. Lattices are attractive in modern cryptography, because lattice-based constructions can enjoy very strong security proofs based on worst-case hardness assumptions (that appear to resist quantum and subexponential attacks), relatively efficient implementations, as well as great simplicity [12,23]. Most of lattice-based cryptographic constructions are based directly upon one of the two average-case problems that have been shown to enjoy worst-case hardness guarantees: the small integer solution (SIS) problem and learning with errors problem [7,10,11,16,17,22].

*Corresponding author (email: zhuyan@ustb.edu.cn)

In modern cryptography, key exchange (KE) protocols are not only important tools for building practical cryptosystems, but also basic cryptographic protocols for secure communication. In 1976, Diffie and Hellman published a famous cryptographic protocol (Diffie-Hellman KE) in the groundbreaking paper "New Directions in Cryptograph." The Diffie-Hellman protocol allows users to exchange keys without a Trusted Authority, even if an opponent is monitoring that communication channel. Although the Diffie-Hellman protocol itself is an anonymous (non-authenticated) key-agreement protocol (insecure against man-in-the-middle attack), it provides the basis for a variety of authenticated protocols and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes.

As mentioned above, various lattice-based cryptographic schemes have been proposed in recent years. However, review of the literature clearly shows that current research in this area still lacks an effective solution for lattice-based KE protocol, which is as fast, easy to understand, and simple to implement as Diffie-Hellman KE, and secure against quantum computing attacks. In view of the fundamental position of Diffie-Hellman KE, our paper will focus on the construction of such a lattice-based KE protocol.

In this paper, we propose a new KE protocol over the SIS problem and its variants. The SIS problem is defined by parameters $q = q(n) \in \mathbb{Z}, m = m(n) \in \mathbb{Z}$, and $\beta = \beta(n) \in \mathbb{R}$, where the integer n is the primary security parameter; given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the goal is to find a nonzero vector $\mathbf{z} \in \mathbb{Z}^m$, such that $\mathbf{Az} = \mathbf{0} \mod q$ and $\|\mathbf{z}\|_2 \leqslant \beta$. The SIS problem dates back to Ajtai's pioneering work [1], which showed that for appropriate parameters, the SIS problem is at least as hard as approximating several worst-case lattice problems, such as the (decisional) shortest vector problem (known as GapSVP), to within a polynomial factor in the lattice dimension. Ajtai's result was tightened in follow-up works (e.g., [24]), leading to a somewhat satisfactory understanding of the hardness of the SIS problem. The hardness of the SIS problem has been the foundation for one-way functions [1] and collision-resistant hash functions [2], identification schemes [25–27], and digital signatures [11–15].

However, the above-mentioned SIS problem is not suitable for constructing the (as Diffie-Hellman) KE protocol directly. In this paper, we introduce a new variant of SIS problem, called bilateral (or double-sides) small integer solution (Bi-SIS). Based on this variant of SIS, we present a new lattice-based KE (KE) protocol, which enjoys some good properties such as simple, easy to implement, and good performance. Our contributions can be summarized as follows:

1. Define a new kind of hard problem, called bilateral small integer solution (Bi-SIS), as well as its inhomogeneous version (Bi-ISIS). We also define computational Bi-ISIS (CBi-ISIS) and decisional Bi-ISIS (DBi-ISIS) problems and review the hardness of these problems. These problems contain similar relations between the discrete logarithm (DL), computational Diffie-Hellman (CDH), and decision Diffie-Hellman (DDH) problems.

2. Construct a new lattice-based KE protocol based on our new problems. This new construction can be considered as a lattice-based version of classic Diffie-Hellman KE protocol. We prove the security of this protocol and show that it provides better security based on the worst-case hardness of lattice problems, relatively efficient implementations, and great simplicity.

On the one hand, our prototype implementation of the proposed KE protocol shows that it is very efficient because the main computation is multiplication between matrices and vectors. On the other hand, it is easy to understand that the worst-case security guarantee provided by our protocol is at the expense of the increasing of storage space, because the users in our protocol have to store a big matrix to generate lattice space.

The rest of the paper is organized as follows. The preliminaries and the definitions of the SIS problem are provided in Section 2. We define the bilateral SIS (ISIS) problem and analyze its hardness in Section 3. We define the CBi-ISIS and DBi-ISIS problem and analyze its hardness in Section 4. We present the construction of our KE protocol and analyze its security in Section 5. The performance analysis and experiments are shown in Section 6. The paper concludes in Section 7.

2 Preliminaries

The main security parameter throughout the paper is n. By convention, vectors are in column form and

we use bold lower-case letters to denote them (e.g., $\mathbf{x}$). Matrices are denoted by bold capital letters (e.g., $\mathbf{A}$), and $\mathbf{A}^{\mathrm{T}}$ is the transposition of $\mathbf{A}$. We use the Euclidean (l_2) norm for vectors throughout the paper, for example, $\|\mathbf{x}\| = \sqrt{\sum_i x_i^2}$. We use $x_1, \cdots, x_k \leftarrow_R X$ to denote the process of choosing elements from the set X uniformly at random. A function $negl : \mathbb{N} \longrightarrow \mathbb{R}$ is called *negligible*, if for every polynomial $poly(n)$ there exists a constant $n_0 \in \mathbb{N}$, such that $negl(n) < poly(n)^{-1}$, for all $n > n_0$.

2.1 Definition of lattices

A lattice in the n-dimensional Euclidean space $\mathbb{R}^n$ is the set

$$\mathcal{L}(\mathbf{b}_1, \cdots, \mathbf{b}_k) = \left\{ \sum_{i=1}^{k} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$

of all integral combinations of k linearly independent (column) vectors $\mathbf{b}_1, \cdots, \mathbf{b}_k \in \mathbb{R}^n$. The integers k and n are called the rank and dimension of the lattice. A basis can be represented by the matrix $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_k] \in \mathbb{R}^{n \times k}$ having the basis vectors as columns. Using matrix notation, the lattice generated by a matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$ can be defined as $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^k\}$, where $\mathbf{Bx}$ is the usual matrix–vector multiplication. In particular, any lattice admits multiple different bases.

The shortest vector problem (SVP), whose goal is to find the shortest nonzero vector in a lattice, is one of the most basic hard problems on lattices. To extend this problem, GapSVP_γ and SIVP_γ are two standard (worst-case hard) approximation problems on lattices, where γ denotes the approximation factor. GapSVP is the decisional version of SVP and SIVP can be seen as an extension of SVP. For space limitations, we omit their formal definitions, which can be found in many works, such as in [12,23].

2.2 Definition of q-ary lattices

We assume that $q \in \mathbb{Z}$ is a modulus. Here, we define two kinds of modular lattices, called q-ary lattices. This kind of lattices are particularly important in lattice-based cryptography. We define a q-ary lattice $\mathcal{L}$ is an integer lattice that satisfies $q\mathbb{Z}^n \subseteq \mathcal{L} \subseteq \mathbb{Z}^n$. It is easy to know whether an integer vector $\mathbf{x}$ is in $\mathcal{L}$ is totally determined by $\mathbf{x} \mod q$. Given two integers, q and $m > n$ (e.g., $m = O(n \log n)$, $q = O(n^2)$), and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we define the following two types of m-dimensional q-ary lattices:

$$\begin{aligned} \Lambda_q(\mathbf{A}) &= \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{v} = \mathbf{A}^{\mathrm{T}}\mathbf{z} \pmod q, \text{ for all } \mathbf{z} \in \mathbb{Z}^n\}, \\ \Lambda_q^{\perp}(\mathbf{A}) &= \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{Av} = \mathbf{0} \pmod q\}. \end{aligned}$$

These two lattices are usually used in lattice-based constructions. We were able to generate $\Lambda_q(\mathbf{A})$ by the rows of $\mathbf{A}^{\mathrm{T}}$, and $\Lambda_q(\mathbf{A})$ corresponds to the linear code generated by $\mathbf{A}$. Also, $\Lambda_q^{\perp}(\mathbf{A})$ consists of all integer vectors that are orthogonal modulo q to the row vectors of $\mathbf{A}$, and it also corresponds to the linear code whose parity matrix is $\mathbf{A}$.

2.3 Finding SISs in q-ary lattices

First, in this subsection, we describe definitions of the SIS and ISIS problems in the l_2 norm, then give some related results. It is well-known that the SIS problem is equivalent to finding some short nonzero vector in $\Lambda_q^{\perp}(\mathbf{A})$, and this problem is defined as follows.

Definition 1 ($\mathrm{SIS}_{q,m,\beta}$)**.** Assume that a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is known, the goal of SIS problems is to calculate a vector $\mathbf{z} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$, such that $\mathbf{Az} = \mathbf{0} \pmod q$ and $\|\mathbf{z}\| \leqslant \beta$.

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, we can define a new variant of the SIS problem, which is called the inhomogeneous SIS (denoted by ISIS) problem. The ISIS problem is equivalent to the problem of decoding an arbitrary integer point $\boldsymbol{t} \in \mathbb{Z}^m$ to within distance β on the lattice $\Lambda_q^{\perp}(\mathbf{A})$. Hence, we have the definition of ISIS problem as follows:

Definition 2 ($\mathrm{ISIS}_{q,m,\beta}$)**.** Assume that a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a random syndrome $\mathbf{u} \in \mathbb{Z}_q^n$ are known, the goal of ISIS problem is to find a vector $\mathbf{z} \in \mathbb{Z}^m$, such that $\mathbf{Az} = \mathbf{u} \pmod q$ and $\|\mathbf{z}\| \leqslant \beta$.

When we pick some appropriate parameters, the SIS (and 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.

Proposition 1 [12, Proposition 4.7]**.** Given any poly-bounded $m, \beta = poly(n)$, as well as any prime $q \geqslant \beta \cdot \sqrt{\omega(n \log n)}$, the $\mathrm{SIS}_{q,m,\beta}$ and $\mathrm{ISIS}_{q,m,\beta}$ problems in the average case are as hard as approximating the problems SIVP_γ and GapSVP_γ in the worst case to within certain $\gamma = \beta \cdot \widetilde{O}(\sqrt{n})$ factors.

3 Bilateral SIS/ISIS problem and its hardness

In this section, we make an extension to the SIS (ISIS) problems and obtain a new kind of hard problems. Our variants of SIS and ISIS are very flexible in cryptographic constructions.

3.1 Definitions of bilateral SIS/ISIS problems

Technically, in the definition of our new problem, the parameters are the same as the SIS problem except the matrix $\mathbf{A}$. We choose a square matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank n, instead of a rectangle $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ in the original SIS problem. For any square matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank n, there is a submatrix $\mathbf{A'} \in \mathbb{Z}_q^{n\times m}$, such that the rows of $\mathbf{A'}$ are linear independent and belong to $\mathbf{A}$. Thus, we have $\Lambda_q(\mathbf{A}) = \Lambda_q(\mathbf{A'})$ and $\Lambda_q^\perp(\mathbf{A}) = \Lambda_q^\perp(\mathbf{A'})$. $\mathbf{A}$ is square with rank n, so that both row rank and column rank of $\mathbf{A}$ is n, which is less than m.

The benefit of our improvements is to provide double-sides operations between square matrices and row/column vectors. That is, given a square matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$, we can extend the (inhomogeneous) SIS problem to solve the equation $\mathbf{Ax} = \mathbf{u}_1 \pmod q$ and the equation $\mathbf{y}^{\mathrm{T}}\mathbf{A} = \mathbf{u}_2^{\mathrm{T}} \pmod q$. We call it Bilateral SIS (ISIS) problem and denote the corresponding problems by Bi-SIS and Bi-ISIS, respectively.

Definition 3 (Bi-SIS problem)**.** The Bi-SIS (in the l_2 norm) is as follows: given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals n, and a real β, the goal is to find two nonzero integer vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m \backslash \{\mathbf{0}\}$, such that

$$\begin{cases} \mathbf{Ax} = \mathbf{0} \pmod q \quad \text{and} \quad \|\mathbf{x}\| \leqslant \beta, \\ \mathbf{y}^{\mathrm{T}}\mathbf{A} = \mathbf{0}^{\mathrm{T}} \pmod q \quad \text{and} \quad \|\mathbf{y}\| \leqslant \beta. \end{cases} \tag{1}$$

Definition 4 (Bi-ISIS problem)**.** The Bi-ISIS (in the l_2 norm) is as follows: given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank equals n, two vectors $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}_q^m$, and a real β, the goal is to find a vector $\mathbf{x} \in \mathbb{Z}^m$ and a vector $\mathbf{y} \in \mathbb{Z}^m$, such that

$$\begin{cases} \mathbf{Ax} = \mathbf{u}_1 \pmod q \quad \text{and} \quad \|\mathbf{x}\| \leqslant \beta, \\ \mathbf{y}^{\mathrm{T}}\mathbf{A} = \mathbf{u}_2^{\mathrm{T}} \pmod q \quad \text{and} \quad \|\mathbf{y}\| \leqslant \beta. \end{cases} \tag{2}$$

Similarly, we denote probability ensembles over Bi-SIS instances and Bi-ISIS instances as $\mathrm{Bi\text{-}SIS}_{q,m,\beta}$ and $\mathrm{Bi\text{-}ISIS}_{q,m,\beta}$, respectively.

3.2 Hardness analysis of Bi-SIS/Bi-ISIS problems

In this subsection, we give the hardness analysis of our new Bi-SIS/Bi-ISIS Problems. First of all, we show that the Bi-SIS/Bi-ISIS problem is equivalent to the SIS/ISIS problem.

Lemma 1. There is a polynomial time reduction from $\mathrm{SIS}_{q,m,\beta}/\mathrm{ISIS}_{q,m,\beta}$ to $\mathrm{Bi\text{-}SIS}_{q,m,\beta}/\mathrm{Bi\text{-}ISIS}_{q,m,\beta}$.

Proof. Suppose the input to a SIS problem is $(q(n), \mathbf{A}, \beta(n))$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is uniformly random. Our goal is to find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$, such that $\mathbf{Az} = \mathbf{0} \pmod q$. Generally, we have $m > n$, and without loss of generality we can assume that the n rows of $\mathbf{A}$ are linear independent over

integers. Let $\{\mathbf{a}_1, \cdots, \mathbf{a}_n\}$ be the rows of $\mathbf{A}$, $\mathbf{A}_1$ be the matrix, whose first n rows are the rows of $\mathbf{A}$, and the remainder $(m-n)$ rows are the same vector $\mathbf{a}_n$, then we have $\mathbf{A}_1 \in \mathbb{Z}_q^{m\times m}$ with rank equals n.

Now $(q(n), \mathbf{A}_1, \beta(n))$ is a Bi-SIS instance. Suppose the solution of this Bi-SIS problem $(q(n), \mathbf{A}_1, \beta(n))$ is $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$, such that $\mathbf{A}_1\mathbf{x} = \mathbf{0} \pmod q$ and $\mathbf{y}^{\mathrm{T}}\mathbf{A}_1 = \mathbf{0}^{\mathrm{T}} \pmod q$, where $\|\mathbf{x}\| \leqslant \beta, \|\mathbf{y}\| \leqslant \beta$. Then, we get $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod q$ and $\|\mathbf{x}\| \leqslant \beta$. Therefore, we find a solution of the original SIS problem. This shows that there is a polynomial time reduction from Bi-SIS$_{q,m,\beta}$ to SIS$_{q,m,\beta}$. Similarly, there is a polynomial time reduction from Bi-ISIS$_{q,m,\beta}$ to ISIS$_{q,m,\beta}$.

Lemma 2. There is a polynomial time reduction from Bi-SIS$_{q,m,\beta}$/Bi-ISIS$_{q,m,\beta}$ to SIS$_{q,m,\beta}$/ISIS$_{q,m,\beta}$.

Proof. Suppose the input to a Bi-SIS problem is $(q(n), \mathbf{A}, \beta(n))$, where $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ is uniformly random with rank equal to n. Our goal is to find nonzero integer vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}, \|\mathbf{x}\| \leqslant \beta, \|\mathbf{y}\| \leqslant \beta$, such that $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod q$ and $\mathbf{y}^{\mathrm{T}}\mathbf{A} = \mathbf{0} \pmod q$. On the one hand, we consider how to find a nonzero integer vector $\mathbf{x}$, such that $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod q$. Since $m > n$ and $rank(\mathbf{A}) = n$, we can assume without loss of generality that the first n rows of $\mathbf{A}$ are linear independent over integers. Let $\mathbf{A}_1$ be the first n rows of $\mathbf{A}$, then $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times m}$. Now $(q(n), \mathbf{A}_1, \beta(n))$ is a SIS instance. The solution of this SIS problem $(q(n), \mathbf{A}_1, \beta(n))$ is a solution of the original Bi-SIS problem. On the other hand, we consider to find a nonzero integer vector $\mathbf{y}$, such that $\mathbf{y}^{\mathrm{T}}\mathbf{A} = \mathbf{0} \pmod q$. Observe that $(\mathbf{y}^{\mathrm{T}}\mathbf{A})^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}}\mathbf{y}$. Therefore, we can use the same method as in the above discussion. This shows that there is a polynomial time reduction from Bi-SIS$_{q,m,\beta}$ to SIS$_{q,m,\beta}$. Similarly, there is a polynomial time reduction from Bi-ISIS$_{q,m,\beta}$ to ISIS$_{q,m,\beta}$.

From Lemma 1 and 2, we conclude that our new problem Bi-SIS/Bi-ISIS is as hard as the SIS/ISIS problem. We have the following theorem.

Theorem 1. Our new problems Bi-SIS$_{q,m,\beta}$/Bi-ISIS$_{q,m,\beta}$ are as hard as problems SIS$_{q,m,\beta}$/ISIS$_{q,m,\beta}$.

According to Proposition 1 and Theorem 1, we have the following proposition which relates the hardness of the Bi-SIS/Bi-ISIS problem to hardness of lattice problems.

Proposition 2. Given any poly-bounded $m, \beta = poly(n)$, as well as any prime $q \geqslant \beta \cdot \sqrt{\omega(n \log n)}$, the Bi-SIS$_{q,m,\beta}$ and Bi-ISIS$_{q,m,\beta}$ problems in the average case are as hard as approximating the problems SIVP and GapSVP in the worst case to within certain $\gamma = \beta \cdot \widetilde{O}(\sqrt{n})$ factors.

3.3 Extension of Bi-ISIS

We extend the Bi-ISIS to the following problem:

Definition 5 (Bi-ISIS*)**.** Let n, m, q and β be the parameters as in ISIS, $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ is a matrix such that $rank(\mathbf{A}) = n$, $\mathbf{e}_1$ is linear independent with column vectors of $\mathbf{A}$, $\mathbf{e}_2$ is linear independent with row vectors of $\mathbf{A}$. Given vectors $\mathbf{b}_1 \in \{\, \mathbf{A}\mathbf{z} + \mathbf{e}_1 : \mathbf{z} \in \mathbb{Z}^m, \mathbf{e}_2^{\mathrm{T}} \cdot \mathbf{z} = 0 \mod q \,\}$ and $\mathbf{b}_2^{\mathrm{T}} \in \{\, \mathbf{z}^{\mathrm{T}}\mathbf{A} + \mathbf{e}_2^{\mathrm{T}} : \mathbf{z} \in \mathbb{Z}^m, \mathbf{z}^{\mathrm{T}} \cdot \mathbf{e}_1 = 0 \mod q \,\}$, the goal is to find a vector $\mathbf{x} \in \mathbb{Z}^m$ and a vector $\mathbf{y} \in \mathbb{Z}^m$, such that:

$$\begin{cases} \mathbf{A}\mathbf{x} + \mathbf{e}_1 = \mathbf{b}_1 \pmod q \quad \text{and} \quad \|\mathbf{x}\| \leqslant \beta, \\ \mathbf{y}^{\mathrm{T}}\mathbf{A} + \mathbf{e}_2^{\mathrm{T}} = \mathbf{b}_2^{\mathrm{T}} \pmod q \quad \text{and} \quad \|\mathbf{y}\| \leqslant \beta. \end{cases} \tag{3}$$

We observe that when $\mathbf{e}_1$ and $\mathbf{e}_2$ are given, the above Bi-ISIS* problem is essentially a Bi-ISIS problem. When $\mathbf{e}_1$ and $\mathbf{e}_2$ are unknown, the Bi-ISIS* problem may be much harder to solve than the Bi-ISIS problem. Based on the hardness of Bi-ISIS problem, it is reasonable to make the assumption that Bi-ISIS* problems are hard.

4 New hard problems and assumptions

We continue to define new hard problems over lattices and their complexity assumptions. Our new problems/assumptions are very analogous to the CDH/DDH problems/assumptions in the form. Given a finite cyclic group $\mathbb{G}$ and a random generator g, the CDH and DDH assumptions are defined as follows:

• **CDH assumption**: this assumption claims that given two elements g^a and g^b, it is computationally hard to compute g^{ab}.

• **DDH assumption**: under this assumption, distinguishing g^{ab} from a random value when given g^a and g^b is computationally hard.

These assumptions, considered as the "standard" assumption, have been widely used in the modern cryptography. Our goal is to extract the CDH/DDH-like assumption from Bi-ISIS* problem. To do it, we combine two branches of Bi-ISIS*, $\mathbf{b}_1 = \mathbf{A}\mathbf{x}+\mathbf{e}_1 \pmod q$ and $\mathbf{b}_2^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}\mathbf{A}+\mathbf{e}_2^{\mathrm{T}} \pmod q$, into an equation $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} = z \pmod q$, where $z \in \mathbb{Z}_q$. Also, we consider $\mathbf{b}_1$ and $\mathbf{b}_2$ as two cryptographic commitments for two random variables $\mathbf{x}$ and $\mathbf{y}$. Hence, using this method, we can integrate two random variables $\mathbf{x}$ and $\mathbf{y}$ to a random integer in $\mathbb{Z}_q$.

4.1 Definitions of new problems and assumptions

Given an instance of Bi-ISIS with parameters n, q, m, β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ of rank n, let $D = \{\mathbf{z} \in \mathbb{Z}^m : \|\mathbf{z}\| \leqslant \beta\}$. For any vectors $\mathbf{x} \in D$ and $\mathbf{y} \in D$, there exists two vector sets $\mathbf{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ which is linear independent with column vectors of $\mathbf{A}$ and $\mathbf{V} = \{\mathbf{v}_1^{\mathrm{T}}, \ldots, \mathbf{v}_n^{\mathrm{T}}\}$ which is linear independent with row vectors of $\mathbf{A}$, such that for each index i, $\mathbf{y}^{\mathrm{T}} \cdot \mathbf{u}_i = \mathbf{0} \mod q$ and $\mathbf{v}_i^{\mathrm{T}} \cdot \mathbf{x} = \mathbf{0} \mod q$. From now on, we define the following notation:

$$\mathbf{A} * \mathbf{x} = \mathbf{A}\mathbf{x} + \sum_{i\in S} \mathbf{u}_i \mod q,$$

where $S \subseteq \{1, \ldots, n\}$ is a random subset. Similarly, $\mathbf{y}^{\mathrm{T}} * \mathbf{A}$ is defined as:

$$\mathbf{y}^{\mathrm{T}} * \mathbf{A} = \mathbf{y}^{\mathrm{T}}\mathbf{A} + \sum_{i\in S'} \mathbf{v}_i^{\mathrm{T}} \mod q,$$

where $S' \subseteq \{1, \ldots, n\}$ is a random subset. We define the CBi-ISIS problem and the DBi-ISIS problem as follows:

• **Computational Bi-ISIS (CBi-ISIS) problem**: given $\mathbf{A} * \mathbf{x}$ and $\mathbf{y}^{\mathrm{T}} * \mathbf{A}$, where $\mathbf{x}, \mathbf{y} \in D$, the goal is to compute $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \pmod q$.

• **Decisional Bi-ISIS (DBi-ISIS) problem**: the goal is to distinguish between the two distributions $(\mathbf{A}, \mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}, \mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x})$ and $(\mathbf{A}, \mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}, z)$, where $\mathbf{x}, \mathbf{y} \in D$ and $z \in \mathbb{Z}_q$ are chosen uniformly at random.

Let $\mathbf{e}_1 = \sum_{i\in S} \mathbf{u}_i$ and $\mathbf{e}_2^{\mathrm{T}} = \sum_{i\in S'} \mathbf{v}_i^{\mathrm{T}}$, then we have $\mathbf{A} * \mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{e}_1 \mod q$ and $\mathbf{y}^{\mathrm{T}} * \mathbf{A} = \mathbf{y}^{\mathrm{T}}\mathbf{A} + \mathbf{e}_2^{\mathrm{T}} \mod q$, which is an instance of Bi-ISIS*(Subsection 3.3). Obviously, if there is an algorithm that solves the Bi-ISIS* problem, we can use this algorithm to solve both CBi-ISIS and DBi-ISIS problems. Therefore, both problems can reduce to the Bi-ISIS* problem.

To our knowledge, there is no efficient algorithm that can solve CBi-ISIS/DBi-ISIS problems other than an efficient Bi-ISIS* algorithm. From the discussions in Section 3.2, we know Bi-ISIS* is at least as hard as lattice problems for appropriate parameters (e.g., $q = n^2, m = n\log q = 2n\log n$, and $\beta = \sqrt{m}$). Therefore, based on the hardness of Bi-ISIS* problems (actually, the ISIS problem), we make the following assumptions.

Definition 6 (CBi-ISIS assumption)**.** Let n, $m = poly(n), q = q(n)$ be integers and $\beta = poly(n)$ be a real, such that $q \geqslant \beta \cdot \sqrt{\omega(n\log n)}$, and let $D = \{\mathbf{z} \in \mathbb{Z}^m : \|\mathbf{z}\| \leqslant \beta\}$, $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ be a random matrix with rank n. Then, for any probabilistic polynomial time (PPT) algorithm $\mathcal{A}$, the following holds:

$$\Pr[\mathcal{A}(\mathbf{A}, \beta, \mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}) = \mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} : \mathbf{x}, \mathbf{y} \leftarrow_R D] < negl(n),$$

where the probability is taken over the random choice of $\mathbf{x}, \mathbf{y} \leftarrow_R D$ and the random bits used by $\mathcal{A}$.

Definition 7 (DBi-ISIS assumption)**.** Let n, $m = poly(n), q = q(n)$ be integers and $\beta = poly(n)$ be a real, such that $q \geqslant \beta \cdot \sqrt{\omega(n\log n)}$, and let $D = \{\mathbf{z} \in \mathbb{Z}^m : \|\mathbf{z}\| \leqslant \beta\}$, $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ be a random matrix with rank n. Then, for any PPT algorithm $\mathcal{A}$, the following holds:

$$|\Pr[\mathcal{A}(\mathbf{A}, \beta, \mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}, \mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x}) = 1] - \Pr[\mathcal{A}(\mathbf{A}, \beta, \mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}, z) = 1]| < negl(n),$$

where the probability is taken over the random choice of $\mathbf{x} \leftarrow_R D, \mathbf{y} \leftarrow_R D$, and $z \leftarrow_R \mathbb{Z}_q$ and the random bits used by $\mathcal{A}$.

A direct application of our new hardness assumptions is to construct KE protocols. We propose a two-party KE protocol in Section 5.

4.2 Establishing parameters

In this subsection, we discuss how to choose parameters. It is necessary to choose proper parameters to guarantee the hardness assumption to ensure the security of cryptographic protocol. In the definition of CBi-ISIS/DBi-ISIS assumption, we have parameters n, m, q, and β, where n is the security parameter and $m = m(n), q = q(n)$, and $\beta = \beta(n)$ are functions of n.

We start from how to choose the matrix $\mathbf{A}$. The following theorem states that for appropriate parameters, the ISIS (Bi-ISIS) problem admits a small solution with high probability.

Lemma 3 [12, Lemma 4.1]**.** Let q be prime and let $m \geqslant 2n\log q$. Then, for all but an at most q^{-n} fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the subset-sums of the columns of $\mathbf{A}$ generate a random element in $\mathbb{Z}_q^n$, that is, for every $\mathbf{u} \in \mathbb{Z}_q^n$ there is a vector $\mathbf{z} \in \{0,1\}^m$, such that $\mathbf{Az} = \mathbf{u}$.

This theorem gives a proper relationship between n and m. Note that in this theorem the generated matrix is $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ rather than $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$. Also, the rows of this random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ are linear independent with high probability. Hence, we can obtain a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ with rank n by the following process: first, choose a matrix $\mathbf{A}' \in \mathbb{Z}_q^{n\times m}$ randomly, then with high probability that the rank of $\mathbf{A}'$ is n by Lemma 3. Next, we can generate each row of $\mathbf{A}$ by a random linear combination of the rows of $\mathbf{A}'$. In this situation, with high probability the ISIS (Bi-ISIS) problem (with such an input $\mathbf{A}$) admits a small solution of length less than $\sqrt{m}$. Therefore, we can choose $\beta = \sqrt{m}$.

To guarantee the hardness of Bi-ISIS, we should choose parameters according to Proposition 2 where $m = poly(n)$ and $\beta = poly(n)$; q is any prime, such that $q \geqslant \beta \cdot \sqrt{\omega(n\log n)}$.

In summary, we can choose parameters satisfying the following conditions: q is prime, $q/\sqrt{\omega(n\log n)} > \beta \geqslant \sqrt{m}$, and $m \geqslant 2n\log q$. For example, we can set $q = n^2, m = 2n\log q = 4n\log n$, and $\beta = \sqrt{m} = 2\sqrt{n\log n}$.

5 Lattice-based KE protocol

KE protocols generate a common secret key between parties that communicate over an insecure network. The most famous KE protocol is the Diffie-Hellman KE protocol [28], in which Alice and Bob fix a finite cyclic group $\mathbb{G}$ and a generator g. They respectively pick random a, b and exchange g^a and g^b. The protocol's result is that they obtain the shared secret key g^{ab}. The left subfigure of Figure 1 illustrates this protocol. The security of the protocol relies on the DDH assumption: distinguish between the two distributions (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c), where g is a generator of some multiplicative group of order p and $a, b, c \in \mathbb{Z}_p$ are chosen uniformly at random. Over the past several years, DDH has been successfully used to simplify many cryptographic schemes, such that DDH is called a cryptographic gold mine [29].

In this section, we present a secure lattice-based KE protocol and prove its security under the new DBi-ISIS assumption. With our current state of knowledge, our KE protocol is the first lattice-based KE protocol.

5.1 Our lattice-based KE protocol

In the following, we adopt the above-mentioned notations and assumptions. We use suitable parameters $m = m(n), q = q(n), \beta = \beta(n)$, and $\mathbf{A} \in \mathbb{Z}_q^{m\times m}$ as in Section 4.2, where the rank of matrix $\mathbf{A}$ is n and $n \ll m$. Our KE protocol is constructed under the CBi-ISIS/DBi-ISIS assumptions. More exactly, our protocol relies on *associative property*: for all vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m$, the equation

$$(\mathbf{y}^{\mathrm{T}} * \mathbf{A}) \cdot \mathbf{x} = \mathbf{y}^{\mathrm{T}} \cdot (\mathbf{A} * \mathbf{x}) = \mathbf{y}^{\mathrm{T}}\mathbf{Ax} \tag{4}$$

holds, where $(\mathbf{y}^{\mathrm{T}} * \mathbf{A}) \cdot \mathbf{x}$ is the inner product between $(\mathbf{y}^{\mathrm{T}} * \mathbf{A})$ and $\mathbf{x}$. This property, which is similar to $(g^a)^b = g^{ab} = (g^b)^a$ in DH, is important for our construction.

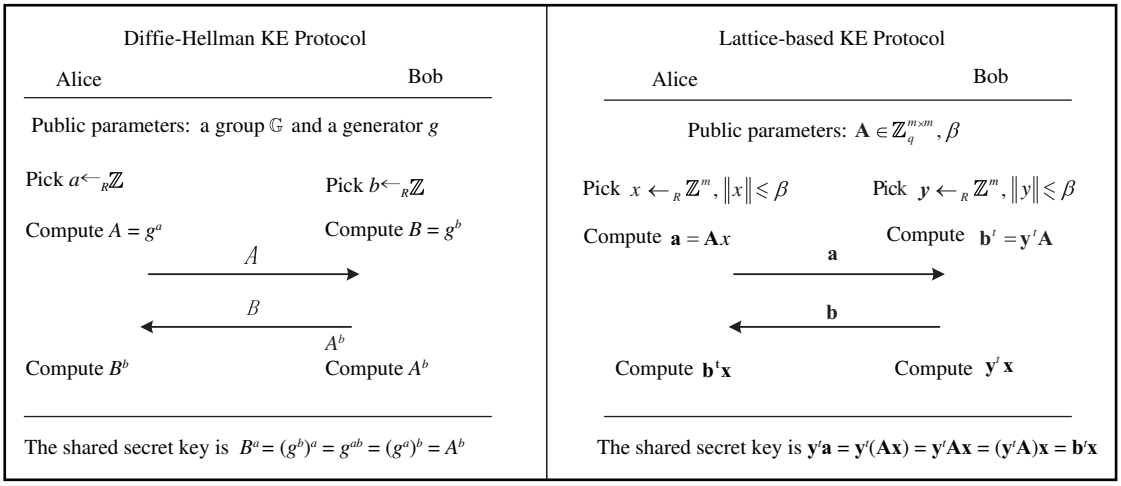

Figure 1 The Diffie-Hellman KE protocol (left) and our lattice-based KE protocol (right).

We describe our basic KE protocol as follows:

1. Setup: Alice and Bob agree on a random matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times m}$ and a real number β.

2. Initialize: Alice picks a random $\mathbf{x} \in \mathbb{Z}^m$, such that $\|\mathbf{x}\| \leqslant \beta$, generates $\mathbf{V} = \{\mathbf{v}_1^{\mathrm{T}}, \ldots, \mathbf{v}_n^{\mathrm{T}}\}$ which is linear independent with rows vectors of $\mathbf{A}$, such that $\langle \mathbf{v}_i, \mathbf{x} \rangle = 0 \mod q$. Alice keeps $\mathbf{x}$ private and makes $\mathbf{V}$ public. Bob picks a random $\mathbf{y} \in \mathbb{Z}^m$, such that $\|\mathbf{y}\| \leqslant \beta$, generates $\mathbf{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ which is linear independent with column vectors of $\mathbf{A}$, such that $\langle \mathbf{u}_i, \mathbf{y} \rangle = 0 \mod q$. Alice keeps $\mathbf{y}$ private and makes $\mathbf{U}$ public.

3. Alice uses $\mathbf{U}$ to compute $\mathbf{a} = \mathbf{A} * \mathbf{x} \mod q$, and sends it to Bob.

4. Bob uses $\mathbf{V}$ to compute $\mathbf{b}^{\mathrm{T}} = \mathbf{y}^t * \mathbf{A} \mod q$, and sends it to Alice.

5. Alice computes $K_1 = \mathbf{b}^{\mathrm{T}} \cdot \mathbf{x} = \mathbf{y}^t\mathbf{A}\mathbf{x} \mod q$.

6. Bob computes $K_2 = \mathbf{y}^{\mathrm{T}} \cdot \mathbf{a} = \mathbf{y}^t\mathbf{A}\mathbf{x} \mod q$.

According to the associative property (see Eq. (4)), both Alice and Bob are now in possession of the same integer $K = K_1 = K_2 = \mathbf{y}^t\mathbf{A}\mathbf{x} \pmod q$. This can serve as their shared secret key.

In the right subfigure of Figure 1, we demonstrate the execution of our two-party KE protocol. In comparison with the left subfigure, it is easy to find that our KE protocol works similar to the Diffie-Hellman KE protocol. Although our basic construction is not perfect for various attacks, it lays the foundation of more secure and effective constructions just as the Diffie-Hellman KE protocol. It is conceivable that our protocol will play an important role in lattice-based cryptography just as the Diffie-Hellman KE protocol's role in traditional cryptography.

5.2 Security analysis

Theorem 2. Our lattice-based KE protocol is secure against the passive (or eavesdropper) adversary under the DBi-ISIS assumption.

Proof. For the sake of clarity, we give a security analysis from the computational perspective in the following. Let A, B denote Alice and Bob, notations are as above. We consider our KE protocol as a simple interactive proof system, which can be expressed by

$$\langle A(\mathbf{x}), B(\mathbf{y}) \rangle (\mathbf{A}, \beta) = (K_1, K_2),$$

where $\langle A(\mathbf{x}), B(\mathbf{y}) \rangle (\mathbf{A}, \beta)$ denote the interactive process between A and B, A takes as input a secret $\mathbf{x}$, B takes as input a secret $\mathbf{y}$, $\mathbf{A}$ and β are public inputs, K_1 is the output of A, and K_2 is the output of B. An eavesdropper can obtain the information $(\mathbf{a}, \mathbf{b})$. Hence, we denote the view of an eavesdropper in an execution of the protocol as

$$View(\langle A(\mathbf{x}), B(\mathbf{y}) \rangle (\mathbf{A}, \beta)) = (\mathbf{a}, \mathbf{b}).$$

We consider the security of our protocol from the following aspects:

1. Considering a passive (or eavesdropper) adversary $\mathcal{S}$, his goal is to compute the shared secret key K. The success probability of this attack is computed as

$$\begin{aligned}&\Pr[\mathcal{S}(\mathbf{A},\beta,View(\langle A(\mathbf{x}),B(\mathbf{y})\rangle(\mathbf{A},\beta)))=K:\mathbf{x},\mathbf{y}\leftarrow_R D]\\ &=\ \Pr[\mathcal{S}(\mathbf{A},\beta,(\mathbf{a},\mathbf{b}))=K:\mathbf{x},\mathbf{y}\leftarrow_R D]\\ &=\ \Pr[\mathcal{S}(\mathbf{A},\beta,\mathbf{A}*\mathbf{x},\mathbf{y}^{\mathrm{T}}*\mathbf{A})=\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x}:\mathbf{x},\mathbf{y}\leftarrow_R D]<negl_1(n),\end{aligned}$$

where $negl_1(n)$ is a negligible function of n. The last inequality holds in terms of the CBi-ISIS assumption in Definition 6.

2. Considering a passive (or eavesdropper) adversary $\mathcal{S}'$, his tougher goal is to guess A's and B's secrets. The success probability of this attack is computed as

$$\begin{aligned}&\Pr[\mathcal{S}'(\mathbf{A},\beta,View(\langle A(\mathbf{x}),B(\mathbf{y})\rangle(\mathbf{A},\beta)))=(\mathbf{x},\mathbf{y}):\mathbf{x},\mathbf{y}\leftarrow_R D]\\ &=\ \Pr[\mathcal{S}'(\mathbf{A},\beta,(\mathbf{a},\mathbf{b}))=(\mathbf{x},\mathbf{y}):\mathbf{x},\mathbf{y}\leftarrow_R D]<negl_2(n),\end{aligned}$$

where $negl_2(n)$ is a negligible function of n. The last inequality follows from the hardness of Bi-ISIS* problem in Definition 5.

3. Considering a participant (A or B) is corrupted by the adversary, without loss of generality, we assume that A^* is the corrupted participant. In this situation, the adversary denoted by $\mathcal{S}_{A^*}$ has access to the secret of A^* which we denote by $\mathbf{x}^*$. The adversary's goal is to compute B's secret. The success probability of this attack is computed as

$$\begin{aligned}&\Pr[\mathcal{S}_{A^*}(\mathbf{A},\beta,View(\langle A^*(\mathbf{x}^*),B(\mathbf{y})\rangle(\mathbf{A},\beta)))=\mathbf{y}:\ \mathbf{x}^*,\mathbf{y}\leftarrow_R D]\\ &=\ \Pr[\mathcal{S}_{A^*}(\mathbf{A},\beta,(\mathbf{a}^*,\mathbf{b}))=\mathbf{y}:\mathbf{x}^*,\mathbf{y}\leftarrow_R D]\\ &=\ \Pr[\mathcal{S}_{A^*}(\mathbf{A},\beta,\mathbf{b}=\mathbf{y}^{\mathrm{T}}*\mathbf{A})=\mathbf{y}:\mathbf{y}\leftarrow_R D]<negl_3(n),\end{aligned}$$

where the equation holds because $\mathbf{x}^*$ and $\mathbf{y}$ are two independent random variants, $negl_3(n)$ is a negligible function of n, and the last inequality follows from hardness of the ISIS problem in Proposition 1.

Finally, as the key security in the Diffie-Hellman protocol is guaranteed by the DDH assumption, the security of the shared key in our protocol is also guaranteed by the DBi-ISIS assumption. This means that the shared key $K=\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x}$ is indistinguishable from z which is chosen uniformly at random. That is, for all adversaries $\mathcal{S}''$, we have

$$|Pr[\mathcal{S}''(\mathbf{A},\beta,\mathbf{A}*\mathbf{x},\mathbf{y}^{\mathrm{T}}*\mathbf{A},\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x})=1]-Pr[\mathcal{S}''(\mathbf{A},\beta,\mathbf{A}*\mathbf{x},\mathbf{y}^{\mathrm{T}}*\mathbf{A},z)=1]|<negl_4(n),$$

where $negl_4(n)$ is a negligible function of n and the last inequality follows from hardness of the DBi-ISIS problem in Definition 7.

Similar to the classic Diffie-Hellman KE protocol, our protocol by itself does not provide authentication of the communicating parties and thus is vulnerable to the man-in-the-middle attack. This problem has been studied for a long history and there are many reports on how to resist the man-in-the-middle attack by introducing other cryptography tools [30–34]. A method to authenticate the communicating parties to each other is generally needed to prevent this type of attack. Hence, our basic protocol can be improved into an *authenticated KE protocol* that is secure against the man-in-the-middle attack through the entity authentication methods, such as the signature-based methods in Refs. [34,35].

6 Performance analysis and experiments

The performance of a cryptographic construction is directly related to the length of parameters. In terms of Subsection 4.2, we choose parameters $q=O(n^2), m=O(n\log n)$, and $\beta=O(\sqrt{m})$ for a given security 'strength' n, such that the CBi-ISIS/DBi-ISIS assumption holds.

We first analyze the communication complexity of our lattice-based KE protocol for typical parameters $q=n^2$ and $m=2n\log q=4n\log n$. According to the above definition, the storage overheads of $\mathbf{A}$ is

Table 1 The comparison between Bi-ISIS and DH on communication

Protocol	Type	Variant	Length	Size
Bi-ISIS	Storage	$\mathbf{A} \in \mathbb{Z}_q^{m\times m}$	$m^2 \cdot \lvert q\rvert$	$16n^2 \log^3 n$
	Exchange	$\mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A} \in \mathbb{Z}_q^m$	$m \cdot \lvert q\rvert$	$8n \log^2 n$
	Shared key	$\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \in \mathbb{Z}_q$	$\lvert q\rvert$	$2 \log n$
DH	Storage	$g \in \mathbb{Z}_p^*$	$\lvert p\rvert$	$k = \log p$
	Exchange	$g^a, g^b \in \mathbb{Z}_p^*$	$\lvert p\rvert$	$k = \log p$
	Shared key	$g^{ab} \in \mathbb{Z}_p^*$	$\lvert p\rvert$	$k = \log p$

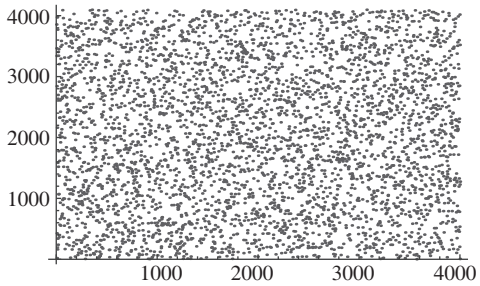

Figure 2 The distribution of $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \pmod q$ in DBi-ISIS.

$m^2 \cdot |q| = 16n^2 \log^3 n$ bits and the communication overheads of the vectors $\mathbf{A} * \mathbf{x}, \mathbf{y}^{\mathrm{T}} * \mathbf{A}$ is $m \cdot |q| = 8n \log^2 n$ bits during each exchange step. The shared secret key is $|q| = 2 \log n$ bits. By comparison, the overhead of the DH protocol is $|p| = \log p$ bits for each integer, where p is a large prime. The main security parameter of the DH protocol is the length of the modulus p denoted by $k = |p|$ (then $p \approx 2^k$). We list the overhead in Table 1. If we set $k = n$, from Table 1, we can see that the storage overheads of our protocol are much more larger than the DH protocol, while the communication overhead of our protocol is approximately the same as that of DH.

We point out that the security strength provided by our lattice-based protocol is stronger than that of the DH protocol [36,37]. In fact, the security parameter n of our lattice-based KE protocol is the dimension of the underlying lattice. When n is several hundreds large, modern computation capability is not capable of handling the underlying lattice problems [38,39]. In contrast, when the security parameter k of the DH is several hundreds large, the underlying DL problem is considered to be insecure. Actually, lattice-based constructions enjoy very strong security that appears to resist against quantum attacks, but traditional constructions based on DL cannot provide this kind of security.

Next, We analyze the computation complexity of our protocol. The main computation in our protocol is multiplication between matrices and vectors, so that the complexity of computing $\mathbf{A} * \mathbf{x}$ or $\mathbf{y}^{\mathrm{T}} * \mathbf{A}$ is $O(m^2|q|^2) = O(n^2 \log^4 n)$, where m is the length of vectors, $|q|^2$ denotes the computational overheads of multiplication of two integers in $\mathbb{Z}_q$, and $|q| = 2 \log n$. Similarly, the complexity of computing $\mathbf{b}^{\mathrm{T}}\mathbf{x}$ or $\mathbf{y}^{\mathrm{T}}\mathbf{a}$ is $O(m|q|^2) = O(n \log^3 n)$. On the other hand, it is well-known that 1024-bit DH keys are equivalent in strength to 80-bit symmetric keys [40,41]. Hence, set $|p| = 1024$ bits. The complexity of exponential operation in $\mathbb{Z}_p^*$ is $O(|p|^3)$. When $n = 80$,

- the complexities of $\mathbf{A} * \mathbf{x}/\mathbf{y}^{\mathrm{T}} * \mathbf{A}$ and $\mathbf{b}^{\mathrm{T}}\mathbf{x}/\mathbf{y}^{\mathrm{T}}\mathbf{a}$ are 1.6×10^8 and 1.6×10^5, respectively.
- the complexity of g^x/g^y is 1.1×10^9.

Therefore, the runtime of our KE protocol is faster than that of the DH protocol. More importantly, our protocol is easy to implement because all operations can be realized in central processor unit (CPU) with 16-bit or 32-bit word size. This means that it does not require the implementations of large integer (1024-bit or 2048-bit) arithmetic used in the DH protocol. Therefore, it can be used to develop the next generation of security products and services in cloud and data center [42,43].

Finally, we illustrate the distribution of $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \pmod q$ in Figure 2, from which it is very easy to detect that the distribution is uniform [44–46]. In this experiment, we choose parameters $n = 64, q = 4099(\approx n^2)$,

and $m = 1536(\approx 2n \log q)$ and compute the value $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \pmod q$ for 4000 randomly chosen small vectors $\mathbf{x}$ and $\mathbf{y}$. From this figure, we can see that the distribution of $\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{x} \pmod q$ is close to the uniform distribution over $\mathbb{Z}_q$.

7 Conclusion

In this paper, we propose some new hard problems and assumptions that are related to the SIS problem on lattices. Based on these problems and assumptions, we construct a new secure two-party lattice-based KE protocol. This protocol enjoys some good properties such as simple, easy to implement, and good performance. Therefore, it has great potential for a new security foundation in the quantum era by replacing the traditional Diffie-Hellman KE.

Acknowledgements

We are indebted to anonymous reviewers for their valuable suggestions. This work was supported by the National 973 Program (Grant No. 2013CB329606) and the National Natural Science Foundation of China (Grant Nos. 61170264, 61370187 & 61472032).

References

1 Ajtai M. Generating hard instances of lattice problems. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996. 99–108
2 Goldreich O, Goldwasser S, Halevi S. Collision-free hashing from lattice problems. ECCC, 1996, 3: 236–241
3 Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In: The 43rd Annual IEEE Symposium on Foundations of Computer Science. Vancouver: IEEE Press, 2002. 356–365
4 Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. Advances in Cryptology–CRYPTO 2008. Berlin/Heidelberg: Springer, 2008. 554–571
5 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 Press, 1997. 284–293
6 Regev O. New lattice-based cryptographic constructions. J ACM, 2004, 51: 899–942
7 Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2005. 84–93
8 Peikert C, Waters B. Lossy trapdoor functions and their applications. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2008. 187–196
9 Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009. 333–342
10 Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. Topics in Cryptology–CT-RSA 2011. Berlin/Heidelberg: Springer, 2011. 319–339
11 Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller. Advances in Cryptology–EUROCRYPT 2012. Berlin/Heidelberg: Springer, 2012. 700–718
12 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2008. 197–206
13 Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis. Advances in Cryptology–EUROCRYPT 2010. Berlin/Heidelberg: Springer, 2010. 523–552
14 Boyen X. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. Public Key Cryptography–PKC 2010. Berlin/Heidelberg: Springer, 2010. 499–517
15 Lyubashevsky V. Lattice signatures without trapdoors. Advances in Cryptology–EUROCRYPT 2012. Berlin/Heidelberg: Springer, 2012. 738–755
16 Agrawal S, Boneh D, Boyen X. Efficient lattice (h)ibe in the standard model. Advances in Cryptology–EUROCRYPT 2010. Berlin/Heidelberg: Springer, 2010. 553–572
17 Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. Advances in Cryptology–CRYPTO 2010. Berlin/Heidelberg: Springer, 2010. 98–115
18 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009. 169–178

19 Gentry C. Toward basing fully homomorphic encryption on worst-case hardness. Advances in Cryptology–CRYPTO 2010. Berlin/Heidelberg: Springer, 2010. 116–137

20 Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. Advances in Cryptology–CRYPTO 2011. Berlin/Heidelberg: Springer, 2011. 505–524

21 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. In: The 52nd Annual IEEE Symposium on Foundations of Computer Science. California: IEEE Press, 2011. 97–106

22 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM Press, 2012. 309–325

23 Micciancio D, Regev O. Lattice-based cryptography. Post-Quantum Cryptography. Berlin/Heidelberg: Springer, 2009. 147–191

24 Micciancio D, Regev O. Worst-case to average-case reductions based on gaussian measures. SIAM J Comput, 2007, 37: 267–302

25 Micciancio D, Vadhan S P. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. Advances in Cryptology–CRYPTO 2003. Berlin/Heidelberg: Springer, 2003. 282–298

26 Lyubashevsky V. Lattice-based identification schemes secure under active attacks. Public Key Cryptography–PKC 2008. Berlin/Heidelberg: Springer, 2008. 162–179

27 Kawachi A, Tanaka K, Xagawa K. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. Advances in Cryptology–ASIACRYPT 2008. Berlin/Heidelberg: Springer, 2008. 372–389

28 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory, 1976, 22: 644–654

29 Boneh D. The decision diffie-hellman problem. Algorithmic Number Theory. Berlin/Heidelberg: Springer, 1998. 48–63

30 Bellare M, Rogaway P. Entity authentication and key distribution. Advances in Cryptology–CRYPTO'93. Berlin/Heidelberg: Springer, 1994. 232–249

31 Diffie W, Van Oorschot P C, Wiener M J. Authentication and authenticated key exchanges. Designs Codes Cryptogr, 1992, 2: 107–125

32 Bird R, Gopal I, Herzberg A, et al. Systematic design of two-party authentication protocols. Advances in Cryptology–CRYPTO'91. Berlin/Heidelberg: Springer, 1992. 44–61

33 Blake-Wilson S, Menezes A. Entity authentication and authenticated key transport protocols employing asymmetric techniques. Security Protocols. Berlin/Heidelberg: Springer, 1998. 137–158

34 Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proceedings of the 30th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1998. 419–428

35 Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels (full version). Cryptology ePrint Archive, Report 2001/040, 2001. http://eprint.iacr.org/040

36 Hu H G, Hu L, Feng D G. On a class of pseudorandom sequences from elliptic curves over finite fields. IEEE Trans Info Theory, 2007, 53: 2598–2605

37 Hu H G, Feng D G. On quadratic bent functions in polynomial forms. IEEE Trans Info Theory, 2007, 53: 2610–2615

38 Nguyen P Q, Vidick T. Sieve algorithms for the shortest vector problem are practical. J Math Crypt, 2008, 2: 181–207

39 Ajtai M, Kumar R, Sivakumar D. A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2001. 601–610

40 Su D, Lü K W. Paillier's trapdoor function hides $\Theta(n)$ bits. Sci China: Info Sci, 2011, 54: 1827–1836

41 Su D, Lü K W. A new hard-core predicate of paillier's trapdoor function. Advances in Cryptology–INDOCRYPT. Berlin/Heidelberg: Springer, 2009, 2009. 263–271

42 Zhu Y, Ahn G-J, Hu H X, et al. Dynamic audit services for outsourced storages in clouds. IEEE Trans Services Comput, 2013, 6: 227–238

43 Zhu Y, Ahn G-J, Hu H X, et al. Role-based cryptosystem: A new cryptographic RBAC system based on role-key hierarchy. IEEE Trans Info Forensics and Security, 2013, 8: 2138–2153

44 Hu H G, Gong G. New sets of zero or low correlation zone sequences via interleaving techniques. IEEE Trans Info Theory, 2010, 56: 1702–1713

45 Gong G, Tor H, Hu H G. A three-valued walsh transform from decimations of helleseth-gong sequences. IEEE Trans Info Theory, 2012, 58: 1158–1162

46 Gong G, Tor H, Hu H G, et al. On the dual of certain ternary weakly regular bent functions. IEEE Trans Info Theory, 2012, 58: 2237–2243