Global Journal of Science Frontier Research: F
Mathematics and Decision Sciences
Volume 20 Issue 6 Version 1.0 Year 2020
Type : Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

Several Lattice-Based AKEs on the SIS Problem

By Limin Zhou & Baolei Mao
Binzhou University

Abstract- In order to design lattice-based authentication key exchange (AKE)protocols with strong security, the article analyzes Wang0s work without authentication that are vulnerable to man-in-the-middle attacks and propose several AKE protocols based on the Bi-ISIS problem. Without signature etc. used to provide authentication, the management is simple, the overhead is low, and the efficiency is high, the security is directly based on the difficult assumption of the Bi-ISIS problem. Although they do not resist unknown key sharing attacks, it has security attributes such as anti-man-in-themiddle attack, session key independence, forward security, and anti-key leakage camouage attacks. The schemes is based on the difficult problem of lattice that they can resist quantum attacks.

GJSFR-F Classification: *MSC 2000: 06D50*

Strictly as per the compliance and regulations of:

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

Several Lattice-Based AKEs on the SIS Problem

Limin Zhou [α] & Baolei Mao [σ]

Abstract- In order to design lattice-based authentication key exchange (AKE)protocols with strong security, the article analyzes Wang0s work without authentication that are vulnerable to man-in-the-middle attacks and propose several AKE protocols based on the Bi-ISIS problem. Without signature etc. used to provide authentication, the management is simple, the overhead is low, and the efficiency is high, the security is directly based on the difficult assumption of the Bi-ISIS problem. Although they do not resist unknown key sharing attacks, it has security attributes such as anti-man-in-the-middle attack, session key independence, forward security, and anti-key leakage camouage attacks. The schemes is based on the difficult problem of lattice that they can resist quantum attacks.

I. Introduction

In 1976, Diffie and Hellman first proposed the concept of a public key cryptosystem and the first key exchange protocolDiffie-Hellman (DH) protocol, [1], whose security stemed from the difficulty of discrete logarithms, and it is difficult for an attacker to obtain the corresponding session key from the information communicated between the two parties. The DH algorithm has no the ability to authenticate the user′s identity and cannot resist man-in-the-middle attacks. The authenticated key exchange (AKE) protocol allows communicated parties to authenticate each other's identity, and still securely negotiate a common session key in the case of active adversaries on the channel.

After the protocol[1] was proposed, there apeared a large number of AKE protocols, whose securities depended on the difficult of large integer factorization or discrete logarithm. With the development of quantum computing, discrete logarithm and other problems are solvable with polynomial time algorithms, and cryptographic schemes based on such problems were threated. Studying a new type of public key cryptosystem that resists quantum attacks has become an important issue in cryptography. Therefore, the design of the quantum cryptosystem is an hot issue in current cryptography research. Among them, the future quantum key exchange protocol needs are the most urgent, so it has attracted a lot of attention in recent years because of its simple operation, parallelism and resistance to quantum attacks.

Author α: Department of Mathematics, Binzhou University, 256603 Shandong, China.
Author σ: Zhengzhou University, 100 Kexue Road, Zhengzhou, China.
e-mail: zhoulimin.s@163.com

Most lattice-based cryptosystem were directly based on two average-case problems with the worst-case difficult guarantee on the lattice: the SIS (Small Integer Solution ,SIS) problem [2] and the LWE (Learning with Error, LWE) problem [3][4]. The LWE problem and the SIS problem were general case difficulty problems and their difficulties were proved to be equivalent to the difficulty of lattice problems (such as GapSVP, GapSIVP) in the worst case, so that the cryptographic schemes constructed based on these problems weare difficult to break even in the worst case. In 1996, Ajtai first proposed the Hard-on-Average problem: SIS problem [2]. In 2008, Gentry et al. first proposed another Hard-on-Average problem: the ISIS (Inhomogeneous Small Integer Solution ISIS) problem [5], and proved that the general difficulty of the ISIS problem was equivalent to the difficulty of the approximate shortest linear independent vector group problem and the version of the shortest vector problem under the specific factor.

The lattice-based key exchange protocol can resist quantum attacks. In 2012, Ding et al. [6] first proposed a key exchange protocol based on the LWE problm and combined the key exchange and lattice problem, which made the lattice-based key exchange protocol stept to a new level. Subsequently, many lattice-based AKE protocols appeared [7]-[15]. In 2013, Li et al. [7]proposed an the AKE based on the LWE problem to determine the feasibility of lattice-based AKE. In 2015, Zhang et al. [8] proposed an AKE based on the RLWE (Ring-LWE, RLWE) problem [16], which consolidated the status of lattice-based key exchange. Fujioka et al. [9][10] used the key encapsulation mechanism to propose AKEs based on the (R)LWE problem and provided a new idea to construct lattice-based AKE. In 2009, Katz et al. [11] constructed the password AKE using a smooth projection function. Xu et al. [12] proposed a provably secure password AKE based on the RLWE problem. In 2017, Ding et al. [13] designed a password-based AKE protocol based on the RLWE problem. In 2019, Zhao et al.[14] generated random parameters with the smooth projective functionand calculated session key with pseudo-random function to propose a lattice-based a password AKE. In 2014, Wang et al. [15] first proposed a variant of the SIS problem: Bi-ISIS (bilateral ISIS, Bi-ISIS) problem, and designed a key exchange protocol based on the Bi-ISIS problem, which opened another new idea for seeking the lattice-based cryptosystems.

Literature [15] can only provided passive security and cannot resist man-in-the-middle attacks and son on. And it cannot provided mutual authentication, that anyone can impersonate the honest participants to destroy it. In order to achieve authentication of the protocol [15], several simple AKE protocols are constructed. Compared with the previous AKE protocols, no signature or encryption algorithm is used, their management is simple, its overhead is low, their security is high, their scalability is good, and their identity authentication is realized. With lower calculation and higher computing efficiency, the two parties achieves secure session key negotiation and key verification. It realizes the identity authentication of the two communication parties and can effectively resist man-in-the-middle attacks and some active attacks. their design is efficient with good cryptographic properties and resistance to quantum attacks.

II. Preliminaries

This section gives some related theories on lattice [3][4]..

a) Select parameters

Assume that n is the the main security parameter.The parameters are chosen the same as that in [15]: a prime $q = O(n^2)$, $m = O(n \log n), \beta \geq \sqrt{m}$, $q/\omega(\sqrt{n \log n}) > \beta \geq \sqrt{m}$, and $m \geq 2n \log n$, *e.g.* for the typical parameters

Ref

2. M. Ajtai. Generating hard instances of lattice problems. Proceedings of the Twenty- Eighth Annual ACM Symposium on Theory of Computing. ACM, 1996, pp.99-108, 1996.

$q = 2n^2 + 1$, $m = 2n \log q$, and $\beta = \sqrt{m} = 2\sqrt{n \log n}$. The Euclidean norm ($l_2$) for vectors is denoted by $\| \mathbf{x} \|_2 = \sqrt{\sum_i x_i^2}$. Choosing elements from the set X uniformly at random is denoted by $x_1, \cdots, x_k \quad_R X$. All computing is performed in Z_p.

b) Hard Random Integer Lattice

Lattice and some related definitions on lattice can be seen in [3][4]. The SIS problem was in [5]. Here only recall the Bi-ISIS problem and its hardness[15] for paper limit.

Deffinition 1.1 *(Bi-ISIS). Given an integer q, a random matrix $\boldsymbol{A} \in Z_q^{m \times m}$ with $rank(\boldsymbol{A}) = n$, two vectors $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_q^m$ and a real β, find nonzero integer vectors $x, y \in \mathbb{Z}^m \backslash \{0\}$ s.t.*

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} = \boldsymbol{u}_1 \mod q, & \| \boldsymbol{x} \| \leq \beta \\ \boldsymbol{y}^t \boldsymbol{A} = \boldsymbol{u}_2^t \mod q, & \| \boldsymbol{y} \| \leq \beta \end{cases}$$

If $u_1 = 0 \mod q$, $u_2^t = 0 \mod q$, $Bi - ISIS$ is $Bi - SIS$. Lemma 1.2 [15] give the hardness of $Bi - (I)SIS_{q,m,\beta}$.

Lemma 1.2 *The problems $Bi - (I)SIS_{q,m,\beta}$ are as hard as the problem $(I)SIS_{q,m,\beta}$.*

Definition 1.3 **(Bi-ISIS*)**. *Let n, m, q and β be the parameters as that of ISIS problem. Set $\boldsymbol{A} \in Z_q^{m \times m}$ with rank($\boldsymbol{A}$)= n, $\boldsymbol{e}_1$ is linear independent with column vectors of $\boldsymbol{A}$, $\boldsymbol{e}_2$ is linear independent with row vectors of $\boldsymbol{A}$. For vectors*

$$\boldsymbol{b}_1 \in \{\boldsymbol{A}\boldsymbol{z} + \boldsymbol{e}_1 : \ \boldsymbol{z} \in \mathbb{Z}^m, \ \boldsymbol{e}_2^t \cdot \boldsymbol{z} = 0 \mod q\}$$

$$\boldsymbol{b}_2^t \in \{\boldsymbol{z}^t \boldsymbol{A} + \boldsymbol{e}_2^t : \ \boldsymbol{z} \in \mathbb{Z}^m, \ \boldsymbol{z}^t \cdot \boldsymbol{e}_1 = 0 \mod q\}$$

the goal is to find vectors $x, \ y \in \mathbb{Z}^m$ s.t.

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}_1 = \boldsymbol{b}_1 \mod q, & \| \boldsymbol{x} \| \leq \beta \\ \boldsymbol{y}^t \boldsymbol{A} + \boldsymbol{e}_2^t = \boldsymbol{b}_2^t \mod q, & \| \boldsymbol{y} \| \leq \beta \end{cases}$$

If $e_1, \ e_2$ are unknown, $Bi - ISIS^*$ may be harder than $Bi - ISIS$ problem. CBi-ISIS/DBi-ISIS problem can be reduced to $Bi - ISIS^*$ problem [**?**].

Definition 1.4 *Given security parameters n, q, m, β, a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m \times m}$ with $rank(A) = n$. Set $D = \{z \in Z^m : \ \| z \|_2 \leq \beta\}$, $\forall x, \ y \in D$, there exists two vectors sets $\boldsymbol{U} = \{\boldsymbol{u}_1, \cdots \boldsymbol{u}_n\}$, which is linear independent with the column vectors of $\boldsymbol{A}$, and $\boldsymbol{V} = \{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ which is linear independent with the row vectors of $\boldsymbol{A}$, s.t. $\forall i \in \{1, \cdots, n\}$, $y^t \cdot u_i = 0 \mod q$, $v_i^t \cdot x = 0 \mod q$. Assume*

$$A * x := Ax + \sum_{i \in S} u_i \mod q, \quad y^t * A := y^t A + \sum_{i \in S'} v_i^t \mod q$$

where S and S' are two random subsets of $\{1, \cdots, n\}$.

Definition 1.5 CBi-ISIS problem. *Given $(A, A*x, y^t*A)$, where $x, \ y \in D$, the goal is to compute $y^t Ax$.*

Definition 1.7 DBi-ISIS problem. *Given $(A, A*x, y^t*A, y^tAx)$, the goal is to distinguish $(A, A*x, y^t*A, y^tAx)$ and $(A, A*x, y^t*A, z)$, where $x, \ y \in D$ and $z \in \mathbb{Z}_q$ are chosen uniformly at random.* Let n, $m = poly(n)$, $q = q(n)$ be integers and $\beta = poly(n)$ be a real, *s.t.* $q \geq \beta \cdot \omega\sqrt{(n \log n)}$. Set $D = \{z \in Z^m : \ \| z \|_2 \leq \beta\}$, a random matrix $A \in Z_q^{m \times n}$ with rank$(A) = n$. For any probabilistic polynomial time (PPT) adversary $\mathcal{A}$,

Ref

5. Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]. Proceedings of the fortieth annual ACM symposium on Theory of computing. ACM, 2008: 197-206.

1. if $Pr[\mathcal{A}(A, \beta, A * x, y^t * A) = y^t Ax : \ x, \ y \leftarrow_R D] < negl(n)$ holds, then call it **CBi-ISIS assumption**;
2. if $Pr[\mathcal{A}(A, \beta, A * x, y^t * A, y^t Ax) = 1 : x, \ y \leftarrow_R D]$

$$-Pr[\mathcal{A}(A, \beta, A * x, y^t * A, z) = 1 : \ x, \ y \leftarrow_R D]| < negl(n)$$

holds, then call it **DBi-ISIS assumption**, where the probabilities are all taken over the random choice of $x, \ y \leftarrow_R D$ and the random bits used by $\mathcal{A}$.

III. Lattice-Based AKEs on the SIS Problem

Based on Wang′s work [15], this section propose several lattice-based KEs on the SIS problem.

a) The basic lattice-based KE

Let n be the security parameter. The system selects m, q, a public matrix $A \leftarrow_R \mathbb{Z}_q^{m \times m}$ with $rank(A) = n, m > n$ and a real integer β, a short vector set $D = z \in Z^m : \|Z\| \leq \beta$. H is a Hash function. Assume that Alice and Bob run the protocol honestly.

1. Assume that Alice selects a temporary secret key vector $x \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|x\| \leq \beta$ and generates $V = \{v_1^t, \cdots, v_n^t\}$ which is linear independent with row vectors of A such that $< v_i, x >= 0 \mod q$, computes a temporary public key $X = A * x \mod q$, makes V public, sends X to Bob.
2. Bob selects a temporary secret vector $y \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|y\| \leq \beta$, generates $U = \{u_1, \cdots, u_n\}$ which is linear independent with column vectors of A such that $< u_i, y >= 0 \mod q$, computes a temporary public key $Y = y^t * A \mod q$, makes U public, sends Y to Alice.
3. Alice computes session key $K = H(Y \cdot x) = H(y^t Ax)$.
4. Bob computes session key $K = H(y^t \cdot X) = H(y^t Ax)$.

b) An active attack

Obviously, the protocol in section 3.1 has no authentication. It is passive safe and actively attacked. We now describe an active attack on it.

Suppose that an attacker (Tom) intercepts X which is sent to Bob by Alice, pretends to be Alice and send $X' = A * x$ to Bob. Then Tom intercepts Y which is sent to Alice by Bob, pretends to be Bob and send $Y' = y^t * A$ to Alice. Now Tom and Alice compute $K' = H(y'^t Ax)$. Alice thought that she and Bob shared K'. Alice thought that she and Bob shared K'. Tom and Bob compute $K'' = H(y^t Ax')$. Bob thought that he and Alice shared K''. The protocol is not secure. The reason why the protocol is insecure under active attack is that the messages of communication parties are not authenticated. In this way, the adversary can fake any party and generate its own message to establish a session key with the other party, so our main work is how to provide authentication for it.

c) A static (long-term) AKE

In order to resist passive attacks in section 3.1 and section 3.2, the final session key cannot be calculated only by the temporary key, but calculated by combining the static public/private keys and temporary public / private keys of both parties in communication.

This article gradually adds authentication functions to the basic KE protocol to increase its security. It can use a certificate authority to issue a certificate to bind the identity of Alice (Bob) and the $\bar{A} = A * t(\bar{B} = b^t * A)$ value selected by the user. That is, treat $\bar{A}(\bar{B})$ as a static public key certified by CA rather than a temporary private key. Either party can use the CA′s public key to verify that the user′s $\bar{A}(\bar{B})$ value is true. So that the protocol can resist passive attacks

Ref

15. S. B. Wang, Y. Zhu, D. Ma, et al. Lattice-based key exchange on small integer solution problem [J]. Science China Information Sciences, 2014, 57(11): 1-12.

1. Assume that Alice selects a static secret key vector $a \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|a\| \leq \beta$ and generates $V = \{v_1^t, \cdots, v_n^t\}$ which is linear independent with row vectors of A such that $< v_i, a >= 0 \mod q$, computes a static public key $\bar{A} = A * a \mod q$, makes V public, sends $\bar{A}$ to Bob.
2. Bob selects a static secret vector $b \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|b\| \leq \beta$, generates $U = \{u_1, \cdots, u_n\}$ which is linear independent with column vectors of A such that $< u_i, b >= 0 \mod q$, computes a static public key $\bar{B} = b^t * A \mod q$, makes U public, sends $\bar{B}$ to Alice.
3. Alice computes session key $\bar{K} = H(\bar{B} \cdot a) = H(b^t A a)$.
4. Bob computes session key $\bar{K} = H(b^t \cdot \bar{A}) = H(b^t A a)$.

Obviously, the session key generated by each static session is the same and not independent.

d) A modified static(long-term) AKE

Let both parties send some random numbers in each session, the section 3.3 can solve the problem of session key independence. we obtain a modified KE as follows.

1. Assume that Alice selects a random number $N_{\bar{A}} \in Z_p^*$, a static secret key vector $a \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|a\| \leq \beta$ and generates $V = \{v_1^t, \cdots, v_n^t\}$ which is linear independent with row vectors of A such that $< v_i, a >= 0 \mod q$, computes a static public key $\bar{A} = A * a \mod q$, makes V public, sends $\bar{A}, N_{\bar{A}}$ to Bob.
2. Bob selects a random number $N_{\bar{B}} \in Z_p^*$, a static secret vector $b \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|b\| \leq \beta$, generates $U = \{u_1, \cdots, u_n\}$ which is linear independent with column vectors of A such that $< u_i, b >= 0 \mod q$, computes a static public key $\bar{B} = b^t * A \mod q$, makes U public, sends $\bar{B}, N_{\bar{B}}$ to Alice.
3. Alice computes session key $\bar{K} = H(\bar{B} \cdot a, N_{\bar{A}}, N_{\bar{B}})$.
4. Bob computes session key $\bar{K} = H(b^t \cdot \bar{A}), N_{\bar{A}}, N_{\bar{B}})$.

e) A modified static AKE 2

If the static private keys (a or b) are leaked, the session key previously established by both parties will no longer be secure. That is, the protocol in section 3.4 does not satisfy forward security. To ensure forward security, the agreement was further modified. Let the long-term public key be $\bar{A}(\bar{B})$ and the temporary public key $X(Y)$, the last generated session key is $\bar{K} = H(b^t A a, y^t A x)$

1. Assume that $\bar{A} = A * a$ is Alice′s static key. She selects a temporary secret key vector $x \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|x\| \leq \beta$ and generates $V = \{v_1^t, \cdots, v_n^t\}$ which is linear independent with row vectors of A such that $< v_i, x >= 0 \mod q$, computes a temporary public key $X = A * x \mod q$, makes V public, sends X to Bob.
2. Assume that $\bar{B} = b^t * A \mod q$ is Bob′s static pubic key. He selects a temporary secret vector $y \leftarrow_R \mathbb{Z}^m$ $s.t.$ $\|y\| \leq \beta$, generates $U = \{u_1, \cdots, u_n\}$ which is linear independent with column vectors of A such that $< u_i, y >= 0 \mod q$, computes a temporary public key $Y = y^t * A \mod q$, makes U public, sends Y to Alice.
3. Alice computes session key $\bar{K} = H(\bar{B} \cdot a, Y \cdot x)$
4. Bob computes session key $\bar{K} = H(b^t \cdot \bar{A}, y^t \cdot X)$.

This protocol satisfies forward security, but it is vulnerable to key compromise impersonation (KCI) attack in section 3.6.

f) A key compromise impersonation(KCI) attack

After receiving Alice′ message X, if the adversary obtains a in section 3.5, he can generate a message $Y = y * A$ to Alice. Since Tom knows y and a, he can

calculate Alice′s session key $K = H(B \cdot a, Y \cdot x)$. Alice thinks that she has established $\bar{K}$ with Bob. In fact, Tom and her established it.

In order to resist KCI attack in section 3.5 and 3.6, we modify the protocol. The final session key is $\bar{K} = H(b^t Aa, y^t Ax, y^t Aa, b^t Ax)$ which is shown in section 3.7.

g) A AKE to resist KCI attack

1. Assume that $\bar{A} = A * a$ is Alice′s static key. She selects a temporary secret key vector $x \leftarrow_R \mathbb{Z}^m$ *s.t.* $\|x\| \leq \beta$ and generates $V = \{v_1^t, \cdots, v_n^t\}$ which is linear independent with row vectors of A such that $< v_i, x >= 0 \mod q$, computes a temporary public key $X = A * x \mod q$, makes V public, sends X to Bob.
2. Assume that $\bar{B} = b^t * A \mod q$ is Bob′s static pubic key. He selects a temporary secret vector $y \leftarrow_R \mathbb{Z}^m$ *s.t.* $\|y\| \leq \beta$, generates $U = \{u_1, \cdots, u_n\}$ which is linear independent with column vectors of A such that $< u_i, y >= 0 \mod q$, computes a temporary public key $Y = y^t * A \mod q$, makes U public, sends Y to Alice.
3. Alice computes session key $\bar{K} = H(\bar{B} \cdot a, Y \cdot x, Y \cdot a, B \cdot x)$.
4. Bob computes session key $\bar{K} = H(b^t \cdot \bar{A}, y^t \cdot X, y^t \cdot \bar{A}, b^t \cdot X)$.

This protocol is vulnerable to unknown key-share attacks which is shown in section 3.8.

h) An unknown key-share attack

$\hat{A}$ denotes Alice′s identity, $\hat{B}$ denotes Bob′s identity, $\hat{T}$ denotes Tom′s identity.

Suppose that when a user registers a public key, CA does not require the user prove that he knows the corresponding private key. If the adversary (Tom) registers a public key $\bar{T}$ that is the same as Alice′s public key $\bar{A}$, $\bar{T} = \bar{A}$. Tom intercepts the message $\hat{A}, \hat{B}, X = A * x$ sent by Alice to Bob. Tom changes the message $(\hat{A}, \hat{B}, X = A * x)$ to $\hat{T}, \hat{B}, X$ and sends it to Bob as Tom. Then, Tom intercepts the message $\hat{B}, \hat{T}, Y = y^t * A$ that Bob sent to himself. Tom pretends to be Bob and changes the message $(\hat{B}, \hat{T}, Y = y^t * A)$ to $\hat{B}, \hat{A}, Y$, and sends it $(\hat{B}, \hat{A}, Y)$ to Alice. Now Alice thought she and Bob shared the key$K_{\hat{A}\hat{B}}(\bar{B} \cdot a, Y \cdot x, Y \cdot a, \bar{B} \cdot x)$, but Bob and Tom negotiated a key $K_{\hat{B},\hat{T}} = H(b^t \cdot \bar{T}, y^t \cdot X, y^t \cdot \bar{T}, b^t \cdot X)$. Since $\bar{T} = \bar{A}$, get $K_{\hat{A}\hat{B}} = K_{\hat{B},\hat{T}}$, thus the protocol is unsafe.

A standard anti-unknown key attack method is to add the identities of both parties to the hash function. The method is ignored here.

IV. Conclusion

Based on the work[15], this article proposes and discusses several lattice-based AKE protocols and their advantages and disadvantages. Compared with the previous protocols, no signature or encryption algorithm was used, their management is simple with lower overhead, its better scalability, and their identity authentication is realized. With lower calculation and higher computing efficiency, the two communication parties achieve secure session key negotiation and key verification. These protocols do not rely on digital signatures to provide key authentication, so their design is efficient with good cryptographic properties and resistance to quantum attacks.

References Références Referencias

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

Notes

2. M. Ajtai. Generating hard instances of lattice problems. Proceedings of the Twenty- Eighth Annual ACM Symposium on Theory of Computing. ACM, 1996, pp.99-108, 1996.
3. O. Regev, On lattices, learning with errors, random linear codes, and cryptography. 13th Color Imaging Conference: Color Science, Systems, Technologies, and Applications. pp. 84-93, 2005.
4. O. Regev, On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), vol. 56, no.6, pp. 1-37, 2009. symposium on Theory of computing. ACM, 2009: 333-342.
5. Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]. Proceedings of the fortieth annual ACM symposium on Theory of computing. ACM, 2008: 197-206.
6. J. Ding, X. Xie, X. Lin. A simple provably secure key exchange scheme based on the learning with error problem. Cryptology ePrint Archive, Report 2012/688, 2012. (Available from: http://eprint.iacr.org) accessed on May, 1. 2012. pp.1-15, 2012.
7. Wulu Li. A key exchange scheme based on lattice[C]. Dependable, Autonomic and Secure Computing (DASC), 2013 IEEE 11th International Conference on. IEEE, 2013: 100-106.
8. J. Zhang, Z. Zhang, J. Ding, et al. Authenticated key exchange from ideal lattices [C]. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2015: 719-751.
9. A. Fujioka., K. Suzuki, K. Xagawa, et al. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism [C]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ACM, 2013: 83-94.
10. A. Fujioka., K. Suzuki, K. Xagawa, et al. Strongly secure authenticated key exchange from factoring, codes, and lattices[J]. Designs, Codes and Cryptography, 2015, 76(3): 469-504.
11. J. Katz, V. Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices [M]. Advances in Cryptology CASIACRYPT 2009. Springer Berlin Heidelberg, 2009: 636-652.
12. XU D. Q.HE D. B. Provably Secure Three-party Password Authenticated Key Exchange Protocol Based On Ring Learning With Error[J] IACR Cryptology ePrint Archive 201715(2): 360-384 IEEE 11th International Conference on. IEEE, 2013: 100-106.

13. Ding J., Alsayigh S., Lancrenon J., et al. Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World[C]. the cryptographers track at the rsa conference, 2017: 183-204.
14. ZHAO Zongqu, HUANG Lijuan, YE Qing, FAN Tao. Two party password authentication key exchange protocol based on lattice[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2019, 31(6): 833-840.
15. S. B. Wang, Y. Zhu, D. Ma, et al. Lattice-based key exchange on small integer solution problem [J]. Science China Information Sciences, 2014, 57(11): 1-12.
16. V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors overrings. Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp.1-23, May, 2010.

Notes