Fundamental Journal of Mathematics and Mathematical Sciences
Volume 9, Issue 2, 2018, Pages 67-79
This paper is available online at http://www.frdint.com/
Published online June 6, 2018

LATTICE-BASED STS PROTOCOLS ON SIS PROBLEM

LIMIN ZHOU* **and JUNSUO ZHOU**

Information Security Institute
ZhouKou Normal University
Henan 466000
P. R. China
e-mail: zhoulimin.s@163.com

The Seventh Middle School of Zibo
Shandong 255499
P. R. China

Abstract

In this paper, we first propose two simple lattice-based station to station (STS) protocols on small integer solution (SIS). The basic lattice-based STS on SIS utilizes signature to provide resisting key compromise impersonation and perfect secrecy as well as preventing unknown key-share attacks with encryption. The modified lattice-based STS provides implicit key confirmation. We analyze their securities under the DBi-ISIS assumption and indicate that they enjoy better efficient implementations and great simplicity in addition to resisting quantum attack.

Keywords and phrases: lattice-based protocols, hard random integer lattice.

2010 Mathematics Subject Classification: 06D50.

This work is partially supported by the National Natural Science Foundation of China (NSFC).

*Corresponding author

Received April 7, 2018; Accepted April 19, 2018

1. Introduction

Diffie-Hellman key exchange (DH-KE) protocol was only secure against a passive adversary and subjected to many attacks, e.g., man-in-the-middle attack, active attack, et al. To meet this case, one variant of DH-KE was authenticated key exchange (AKE) [1] which guaranteed that nobody can establish the shared session except for the participants involved in AKE.

Now, we step into the era of quantum computer. Most of the AKEs are broken by quantum computers because quantum computers can solve almost all traditional mathematical problems which AKEs depended on. Thus, it is necessary to find mathematical problems which cannot be solved by quantum computers and can be used to design cryptographic systems. Recently, lattice as a technique to resist quantum attack has attracted much attention to establish cryptographic primitives. Lattice problem includes two big basic average-case hard problems: the learning with error problem (LWE) [2, 6, 7] and the small integer solution problem (SIS) [4] which guarantees worst-case harness for cryptosystems to resist quantum attack. Regev et al. first proposed the LWE problem [2, 7] and demonstrated that solving the average-case LWE problem was at least as hard as solving quantum some worst-case hard lattice problem. In 2008, Gentry et al. [4] first defined the general Inhomogeneous Small Solution (ISIS) problem and showed that solving the average-case ISIS problem was at least as hard as to quantumly solve the worst-case hard approximation SIVP problems. As a direction application, there exists several public key cryptosystems [4, 16] based on the SIS problem.

Recently, a number of lattice-based public key cryptosystems [2, 4, 5, 12-16] appeared. However, until 2012, Ding et al. [8] first proposed a key exchange protocol whose security solely relied on the hardness of the LWE problem. In 2013, Li et al. proposed first two KEs [11] based on the new variant of LWE and SIS problem. In 2014, Wang et al. first proposed Bilateral Inhomogeneous Small Integer Solution (Bi-ISIS) problem [9] and a KE relied on the Bi-ISIS problem. These lattice-based KEs [8, 11, 9] showed that cryptography have made a big step on the relation between lattice and KE. Thus, it makes perfect sense to design AKE based on lattice. There are several papers focusing on designing AKEs from lattices [17-21]. In 2009,

Katz et al. [17] proposed the first password-based AKE based on the LWE problem. In 2014, Zhang et al. [10] proposed an AKE protocol based on the Ring Learning With Errors (Ring-LWE) [10]. Zhang's AKE relied directly and solely on the hardness of Ring-LWE and was simple without using other cryptographic primitives, e.g., signature/MAC et al. to reduce additional overhead including computing and space storage.

Motivated by [8-11] and [17-21] as mentioned above, we try to build lattice-based AKEs. Especially, based on Wang's work [9], we first propose two simple lattice-based station-to-station (STS) AKEs which solely rely on the SIS problem. The basic lattice-based STS on SIS utilizes signatures to provide resisting key compromise impersonation [1], perfect secrecy [1] and avoid unknown key-share attacks [22] with encryption. To modify the basic lattice-based STS to get another lattice-based STS which provides implicit key confirmation. Since the main calculation operation of the two lattice-based STS are only usual matrix-vector multiplication (not exponential operation) that they enjoy small calculation, better efficient implementations and great simplicity.

2. Preliminaries

Notations. Assume that n is the main security parameter in this paper. Bold lower-case letters denote vectors in the column form, e.g., $\boldsymbol{x}$. Bold capital letters denote matrices, e.g., $\boldsymbol{A}$ and the transposition of $\boldsymbol{A}$ is A^t. The Euclidean (l_2) norm for vectors, denoted by $\| \boldsymbol{x} \|_2 = \sqrt{\sum_i x_i^2}$, is used. That choosing elements from the set X uniformly at random are denoted by $x_1, \cdots, x_k \leftarrow_R X$.

2.1. Hard random integer lattice

The definition of lattice can be seen in [2, 7].

2.2. The ISIS/SIS problem and Bi-ISIS/Bi-SIS problem

One of the average-case problems on lattice is the SIS (ISIS) problem [4]. The parameters of Bi-SIS (Bi-ISIS) problem [9] are the same as that of SIS (ISIS) problem.

Definition 1.1 ($\mathrm{ISIS}_{q,m,\beta}$) [4]**.** Given an integer q, a random matrix $\boldsymbol{A} \in \mathbb{Z}^{n\times m}$, a random vector $\boldsymbol{u} \in Z^n$, a real β, find a nonzero integer vector $z \in \mathbb{Z}^m$, s.t., $\boldsymbol{A}z = \boldsymbol{u} \bmod q$ and $\| z \|_2 \le \beta$. If $u = 0 \bmod q$, then the $\mathrm{ISIS}_{q,m,\beta}$ problem is the $\mathrm{SIS}_{q,m,\beta}$ problem.

Definition 1.2 (Bi-ISIS) [9]**.** Given a prime q, a matrix $\boldsymbol{A} \in Z^{m\times m}$ chosen randomly with rank $(\boldsymbol{A}) = n$, two vectors $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_q^m$ and a real β, the goal is to find nonzero integer vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}^m \setminus \{0\}$ such that

$$\begin{cases} \boldsymbol{A}\boldsymbol{x} = \boldsymbol{u}_1 \bmod q, \| \boldsymbol{x} \| \le \beta, \\ \boldsymbol{y}^t \boldsymbol{A} = \boldsymbol{u}_2^t \bmod q, \| \boldsymbol{y} \| \le \beta. \end{cases}$$

If $\boldsymbol{u}_1 = 0 \bmod q$, $\boldsymbol{u}_2^t = 0 \bmod q$, then Bi-ISIS is the Bi-SIS. $\text{Bi - SIS}_{q,m,\beta}$ / $\text{Bi - ISIS}_{q,m,\beta}$ denotes the probability ensembles over Bi - SIS /Bi - ISIS instance. Lemma 1.3 and Proposition 1.4 gave the hardness of $\text{Bi - SIS}_{q,m,\beta}$ and $\text{Bi - ISIS}_{q,m,\beta}$.

Lemma 1.3 [9]**.** *The problems* $\textit{Bi - SIS}_{q,m,\beta}$ */* $\textit{Bi - ISIS}_{q,m,\beta}$ *are as hard as the problems* $\textit{SIS}_{q,m,\beta}$ */* $\textit{ISIS}_{q,m,\beta}$, *respectively*.

Proposition 1.4 [9]**.** *Given any poly-bounded* m, $\beta = poly(n)$, $q \ge \beta \cdot \omega(\sqrt{n \log n})$, *the Bi -* $\textit{SIS}_{q,m,\beta}$ *and* $\textit{ISIS}_{q,m,\beta}$ *problems in average case are as hard as approximating the problem SIV* P_γ *and GapSVP, in the worst case within certain* $\gamma = \beta \cdot \tilde{O}(\sqrt{n})$.

Definition 1.5 (Bi - ISIS^*) [9]**.** 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 linearly independent with column vectors of $\boldsymbol{A}$, $\boldsymbol{e}_2$ is linearly independent with row vectors of $\boldsymbol{A}$. For vectors

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

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

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

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

If $\boldsymbol{e}_1, \boldsymbol{e}_2$ are unknown, Bi - ISIS* may be harder than Bi - ISIS problem. CBi-ISIS / DBi-ISIS problem can be reduced to Bi - ISIS* problem [9].

Definition 1.6 [9]**.** Given security parameters n, q, m, β, a random matrix $\boldsymbol{A} \in \mathbb{Z}_q^{m \times m}$ with rank $(\boldsymbol{A}) = n$. 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 linearly independent with the column vectors of $\boldsymbol{A}$, and $\boldsymbol{V} = \{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ which is linearly independent with the row vectors of $\boldsymbol{A}$, s.t., $\forall i \in \{1, \cdots, n\}$, $y^t \cdot u_i = 0 \bmod q$, $v_i^t \cdot x = 0 \bmod q$. Assume

$$A * x : Ax + \sum_{i \in S} u_i \bmod q, \; y^t * A \coloneqq y^t A + \sum_{i \in S'} v_i^t \bmod q,$$

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

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

DBi-ISIS problem. Given $(A, A * x, y^t * A, y^t Ax)$, the goal is to distinguish $(A, A * x, y^t * A, y^t Ax)$ 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 $D = \{z \in Z^m : \|z\|_2 \leq \beta\}$, random matrix $A \in Z_q^{m \times m}$ with

rank $(A) = n$. For any probabilistic polynomial time (PPT) adversary $\mathcal{A}$,

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 $\mathcal{A}$.

2.3. Select parameters

Here the parameters are chosen the same as that in [9]: 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 $q = 2n^2 + 1$, $m = 2n \log q$, and $\beta = \sqrt{m} = 2\sqrt{n \log n}$.

3. Lattice-based STS Protocols on SIS

Based on Wang's work [9], we first propose lattice-based STS AKE protocols on SIS problem. The basic lattice-based STS is the combination of lattiec-based KE [9] and a secure interactive identification scheme, in which s_A, s_B act as random challenges. The signatures on random challenges provides mutual authentication.

3.1. The basic lattice-based STS

First, the system selects a public matrix $\boldsymbol{A} \leftarrow_R \mathbb{Z}_q^{m \times m}$ and a real β. Assume that two participants, Alice and Bob, run the protocol honestly.

1. Assume that Alice selects a secret key vector $s_A \leftarrow_R \mathbb{Z}^m$, s.t., $\|s_A\| \leq \beta$ and

generates $\boldsymbol{V} = \{\boldsymbol{v}_1^t, \cdots, \boldsymbol{v}_n^t\}$ which are linearly independent with rows vectors of $\boldsymbol{A}$ such that $< v_i, s_A >= 0 \bmod q$. Alice keeps s_A secret, computes $p_A = A * s_A \bmod q$, sends $(cert(Alice), p_A)$ to Bob and makes V public.

2. Bob selects a secret vector $s_B \leftarrow_R \mathbb{Z}^m$, s.t., $\|s_B\| \leq \beta$, generates $\boldsymbol{U} = \{\boldsymbol{u}_1^t, \cdots, \boldsymbol{u}_n\}$ which are linearly independent with column vectors of $\boldsymbol{A}$, such that $< u_i, s_B >= 0 \bmod q$, computes

$$K = s_B^t \cdot p_A \bmod q,\ p_B = s_B^t * A \bmod q,$$

$$t_B = sig_B(p_B \| p_A),\ c_B = enc_K(t_B)$$

and sends $(cert(Bob), p_B, c_B)$ to Alice.

3. Alice computes $K = p_B \cdot s_A \bmod q$, decrypts c_B with K to get t_B. Then she utilizes ver_B to verify t_B. If t_B is invalid, Alice refuses it and stops; otherwise, she accepts it and computes

$$t_A = sig_A(p_A \| p_B),\ c_A = enc_K(t_A)$$

sends c_A to Bob.

4. Bob utilizes K to decrypt c_A to get t_A. If t_A is invalid, he refuses it and stops; otherwise, he accepts it.

The basic lattice-based STS achieves forward secrecy [22] since the shared secret $K = s_B^t A s_B \bmod q$ is the ephemeral key. Signatures guarantee resisting key compromise impersonation [22] (since the adversary cannot know privates key of sig_A, sig_B), thus revealing long-term key p_A or p_B does nothing for an adversary to forge a signature (not sig_A, sig_B).

Encryption is necessary to prevent unknown key-share attacks [22]. Assume that there is no encryption involved in signatures. Since p_A, p_B are public keys and anyone can sign them with their own private signature keys. For an example, one

adversary Eve can replace $t_A = sig_A(p_A \| p_B)$ with $t_E = sig_E(p_A \| p_B)$ because Eve knows p_A, p_B. As a result, Alice and Bob complete the basic lattice-based STS. However, Bob ensures that he shares $K = s_B^t A s_B \bmod q$ with Eve, but Alice believes that she shares $K = s_B^t A s_B \bmod q$ with Bob. (If Alice and Bob exchange p_A, p_B using their own certificates, Eve can still replace Alice's certificate with Eve's certificate). Although Eve can operate the attack, he can not know $K = s_B^t A s_B \bmod q$. Therefore, without encryption involved with exchanged key $K = s_B^t A s_B \bmod q$, our basic lattice-based STS suffers from unknown key-share attacks.

If add Alice's (Bob's) identity ID (Alice) (ID (Bob)) to Bob's (Alice's) signature $sig_B(sig_A)$, unknown key-share attacks can be avoided. Such protocol can achieve stronger entity authentication because ID (Alice) and ID (Bob) which are involved in signatures guarantee parties' explicit indication. Obviously, it is not necessary for encryption involved in the protocol. Thus we get a modified lattice-based STS shown in Section 4.1.

4. A Modified Lattice-Based STS (ML-STS)

This is an AKE with certificate that is signatured by a Trust Authoritie (TA). Every user has a certificate, e.g., $Cert(Alice) = (ID(Alice), ver_A, sig_{TA}(Alice, ver_A))$, where ver_A is Alice's verification algorithm and her signature algorithm is denoted by sig_A; ID(Alice) denotes Alice's identification; sig_{TA} is TA's signature algorithm.

4.1. ML-STS Protocol

First, the system selects a public matrix $\boldsymbol{A} \leftarrow_A \mathbb{Z}_q^{m \times m}$ and a real β. Assume that two participants, Alice and Bob, run the protocol honestly.

1. Assume that Alice selects a secret key vector $s_A \leftarrow_R \mathbb{Z}^m$, s.t., $\|s_A\| \le \beta$ and

generates $\boldsymbol{V} = \{\boldsymbol{v}_1^t, \cdots, \boldsymbol{v}_n^t\}$ which are linearly independent with rows vectors of A such that $< v_i, s_A >= 0 \bmod q$. Alice keeps s_A secret and makes $\boldsymbol{V}$ public. She computes $p_A = A * s_A \bmod q$ and sends $(Cert(Alice), p_A)$ to Bob.

2. Bob selects a secret vector $s_B \leftarrow_R \mathbb{Z}^m$, s.t., $\|s_B\| \leq \beta$, generates $\boldsymbol{U} = \{\boldsymbol{u}_1^t, \cdots, \boldsymbol{u}_n\}$ which are linearly independent with column vectors of A, such that $< u_i, s_B >= 0 \bmod q$, computes

$$p_B = s_B^t * A \bmod q,\ K = s_B^t \cdot p_A \bmod q,$$

$$t_B = sig_B(ID(Alice) \| p_B \| p_A)$$

and sends $(Cert(Bob), p_B, t_B)$ to Alice.

3. Alice utilizes ver_B to verify t_B. If t_B is invalid, Alice refuses and stops; otherwise, she accepts it and computes

$$K = p_B \cdot s_A \bmod q,\ t_A = sig_A(ID(Bob), p_A, p_B)$$

sends t_A to Bob.

4. Bob utilizes ver_A to verify t_A. If t_A is invalid, he refuses and stops; otherwise, he accepts it.

4.2. Security analysis

ML-STS protocol can resist active attacks and passive attacks because signatures are involved in this protocol.

Theorem 4.2.1. *Our ML-STS protocol is secure against one passive adversary and one active adversary under the DBi-ISIS assumption.*

Proof. Assume that the adversary, Eve, intercepts p_A and replaces it with p'_A. Then Eve gets p_B and $t_B = sig_B(ID(Alice) \| p_B \| p'_A)$ and wants to replace p_B with p'_B, which implies that Eve must also replace $sig_B(ID(Alice) \| p_B \| p'_A)$ with

$t_B = sig_B(ID(Alice) \| p'_B \| p_A)$. Unfortunately, Eve does not know Bob' sig_B so that he could not calculate the signature on $ID(Alice) \| p'_B \| p_A$. Similarly, Eve does not know Alice's sig_A so that he can not replace $sig_A(ID(Bob) \| p_A \| p'_B)$ with $sig_A(ID(Bob) \| p'_A \| p_B)$. In summary, the signature can prevent man-in the-middle attack.

If one adversary is passive, the session will stop when Alice and Bob accept each other. Namely, the two parties successfully recognize each other and compute the session key *K*. Under the hardness of DBi-ISIS problem, one active adversary can get no information on key *K*. In short, an active adversary is detected and a passive adversary does nothing under the hardness of DBi-ISIS problem.

Theorem 4.2.2. *ML-STS protocol achieves implicit key authentication under the hardness of DBi-ISIS problem.*

Proof. Assume that Alice has accepted the protocol and the adversary is passive. Since ML-STS protocol is securely interactive, Alice can ensure that she really communicates with her intended participant: Bob. If Bob and Alice execute the protocol honestly, Alice can ensure that Bob computes a key *K* and no one can work out *K* except for Bob.

Why Alice thought that Bob can work out *K*? Because Alice receives Bob's signature on p_A and p_B, thus Alice can infer that Bob knows p_A, p_B. Assume that Bob executes honestly, then Alice can deduce that Bob knows s_B. Thus if Bob knows p_A, s_B, then he can calculate *K*.

Similarly, if Bob has already accepted it, then Bob can ensure that he communicates with his intended party: Alice, who can work out *K* and no one can work out *K* except for Alice. When Bob accepts it, he can ensure that honest Alice has already accepted it. But when Alice accepts it, she does not know whether honest Bob would accept it subsequently since Alice does not know whether Bob has received information from the last step of the session.

In short, Alice and Bob cannot confirm whether the other party has worked out the session key *K*.

5. Conclusion

In this paper, we first propose two simple lattice-based STS protocols which solely rely on the DBi-ISIS problem. The basic lattice-based STS utilizes signatures to achieve resistance to key compromise impersonation, perfect secrecy and prevent unknown key-share attacks with encryption. But the basic lattice-based STS cannot enjoy mutual key identification. ML-STS with signatures provides implicit key confirmation. Since all the calculation operations of the two lattice-based STS only depend on usual matrix-vector multiplication that they capture small calculation, better efficient implementations and great simplicity.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] Hugo Krawczyk, HMQV: A high-performance secure Diffie-Hellman protocol, CRYPTO, 2005, pp. 546-566.

[2] O. Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, 2005.

[3] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem, Proceedings of the forty-first annual ACM symposium on Theory of computing, ACM 2009, pp. 333-342.

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

[5] C. Gentry, Fully homomorphic encryption using ideal lattices, STOC 9 (2009), 169-178.

[6] B. Applebaum, D. Cash and C. Peikert et al., Fast cryptographic primitives and circular-secure encryption based on hard learning problems, Advances in Cryptology, CRYPTO, Springer, Berlin, Heidelberg, 2009, pp. 595-618.

[7] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, JACM 56(6) (2009), 34.

[8] J, Ding and X. Lin, A simple provably secure key exchange scheme based on the learning with errors problem, IACR Cryptology ePrint Archive, 2012, p. 688.

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

[10] J. Zhang, Z. Zhang and J. Ding et al., Authenticated key exchange from ideal lattices, 2014.

[11] Li Wulu, A key exchange scheme based on lattice, Dependable, Autonomic and Secure Computing (DASC), 2013 IEEE 11th International Conference on IEEE, 2013, pp. 100-106.

[12] V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, Springer-Verlag, 2010, pp. 1-23.

[13] D. Stehle and R. Steinfeld, Making NTRU as secure as worst-case problems over ideal lattices, Advances in Cryptology, EUROCRYPT 2011, Springer, Berlin, Heidelberg, 2011, pp. 27-47.

[14] E. Orsini and J. Van de Pol, N. P. Smart, Bootstrapping BGV ciphertexts with a wider choice of p and q, Public-Key Cryptography-PKC, Springer, Berlin, Heidelberg, 2015, pp. 673-698.

[15] R. Hiromasa, M. Abe and T. Okamoto, Packing messages and optimizing bootstrapping in GSW-FHE, Public-Key Cryptography-PKC, Springer, Berlin, Heidelberg, 2015, pp. 699-715.

[16] V. Lyubashevsky and D. Wichs, Simple lattice trapdoor sampling from a broad class of distributions, Public-Key Cryptography-PKC, Springer, Berlin, Heidelberg, 2015, pp. 716-730.

[17] Jonathan Katz and Vinod Vaikuntanathan, Smooth projective hashing and password-based authenticated key exchange from lattices, ASIACRYPT, 2009, pp. 636-652.

[18] Joppe W. Bos, Craig Costello, Michael Naehrig and Douglas Stebila, Post-quantum key exchange for the TLS protocol from the ring learning with errors problem, Cryptology ePrint Archive, Report 2014/599, 2014.

[19] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa and Kazuki Yoneyama, Strongly secure authenticated key exchange from factoring, codes and lattices, PKC, 2012, pp. 467-484.

[20] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa and Kazuki Yoneyama, Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism, ASIACCS, 2013, pp. 83-94.

[21] Chris Peikert, Lattice cryptography for the internet, Cryptology ePrint Archive, Report 2014/070, 2014.

[22] Katz Jonathan and Yehuda Lindell, Introduction to modern cryptography: principles and protocols, CRC Press, 2007.