A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem

Jintai Ding[1,2,*], Xie Xiang[3], Xiaoding Lin[4]

1: CPS Lab
Chongqing University
2: Department of Mathematical Sciences
University of Cincinnati
3: Chinese Academy of Sciences
4: Rutgers University
* Corresponding Author
jintai.ding@gmail.com

Abstract. We use the learning with errors (LWE) problem to build a new simple and provably secure key exchange scheme. The basic idea of the construction can be viewed as certain extension of Diffie-Hellman problem with errors. The mathematical structure behind comes from the commutativity of computing a bilinear form in two different ways due to the associativity of the matrix multiplications:

$$(X^t \times A) \times Y = X^t \times (A \times Y),$$

where X, Y are column vectors and A is a square matrix. We show that our new schemes are more efficient in terms of communication complexity and computation complexity compared with key exchange schemes or key transport schemes via encryption schemes based on the LWE problem. Furthermore, we extend our scheme to the ring learning with errors (RLWE) problem, resulting in small key size and better efficiency.

1 Introduction

Lattice-based public key cryptography has become a promising potential alternative to public key cryptography based on traditional number theory assumptions. One building block of lattice-based cryptography, especially in encryption, is the learning with errors (LWE) problem. After the introduction of LWE problem by Regev [21], it has attracted a lot of attentions in theory and applications due to its usage in cryptographic constructions with good provable secure properties. In a nutshell, the (decisional) LWE problem is to distinguish polynomially many noisy inner-product samples $(\mathbf{a}, b \approx \langle \mathbf{a}, \mathbf{s} \rangle)$ from uniformly random samples.[1] An attractive property of the LWE problem is that Regev [21] shows that to solve the average-case LWE problem is at least as hard as to (quantumly) solve some worst-case hard lattice problems. Many lattice-based primitives based on LWE have been discovered, such as public-key encryption [21,14,18], (hierarchical) identity-based encryption [14,1,11], functional encryption [3,2,5,15] and fully homomorphic encryption [9,7,6].

In the constructions mentioned above, a matrix form of the LWE problem is always used (i.e., need sufficient many samples). The drawback of that is it results in large (say quadratic) key size. To further improve the efficiency, Lyubashevsky, Peikert and Regev [19] introduced the ring learning with errors (RLWE) problem, which is to distinguish polynomially many noisy ring multiplication $(a, b \approx a \cdot s)$ from uniform, where " $\cdot$" is the multiplicative operation over some ring. It's shown in [19] that to solve RLWE problem is at least as hard as to solve some worst-case problems in *ideal* lattices, instead of general lattices.

The Diffie-Hellman key exchange protocol is a fundamental construction in public key cryptography. It is simple and elegant, and it relies on a different mathematical structure from that of

[1] $\mathbf{s}$ is secret and remains the same in all the samples.

encryption scheme constructions, such as the RSA construction, since it does not require a trapdoor function. Actually, DH-like key exchange protocol guarantees forward security better than classical RSA-like one. What motivates the work in this paper is to try to build a simple key exchange protocol using the basic idea but based on the LWE problem. There are already related works in [16,17,10,13], but as far as we know there is not yet any provably secure key exchange protocols based on the LWE problem as a direct generalization of the Diffie-Hellman key exchange protocol, which is elegant in terms of its simplicity. To achieve this goal, we use the normal form of LWE problem suggested in [4] and propose a new provably secure key exchange protocol.

The key idea behind our new construction can be viewed as a way to share a secret given by the value of the bilinear function of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{Z}_q^n$, where q, n are some integers, via the bilinear form:

$$Q(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \mathbf{A} \mathbf{y},$$

where $\mathbf{A}$ is an $n \times n$ matrix in $\mathbb{Z}_q$. Surely in order to make the system provably secure, we need to introduce the small errors to achieve our goal. The main contribution of this paper is to use this simple idea to build a simple and provably secure key exchange scheme. Furthermore, we extend our construction further based on the RLWE problem. Our construction is a significant additional step in showing how versatile the LWE assumption can be.

Besides, we also give an interactive multiparty key exchange protocol. This protocol can be viewed as a generalization of our two party protocol. Although the provable security of the protocol seems plausible but we do not know how to do it, and we leave it as an open problem.

1.1 Main Contributions

The DH key exchange protocol was constructed ahead of the RSA encryption scheme, and these two system are based on two very different mathematical principles, while the DH key exchange protocol is based on the commutativity of the power maps and the hardness of the discrete logarithm problem and the RSA cryptosystems is based on special group automorphism and the hardness of prime factorization of integers. Due to versatile applications of LWE in cryptography including a very elegant encryption scheme, it is a natural question to ask if we can construct a simple and elegant key exchange just like the DH scheme which, however, is not based on the same mathematical principles as that of the LWE encryption scheme. Our paper gives a positive answer. The fundamental difference is that we use the quantities of the usual LWE constructions, which serves the purpose of hiding the plaintext, and, is, therefore, later canceled out, to serve the purpose as the exchanged key, and we rely also on the commutativity of matrix multiplication to compute bilinear maps, which was not used in the LWE constructions. Thus, from the point view of structural constructions of cryptosystems, we further demonstrate the versatility of the LWE problem, but in a way different from any previous construction before. The simplicity of the construction is very striking, though the elegance is slightly affected due to extra bits needed. This method should open possible doors to other applications, in particular, key distribution systems and new identity-based encryption systems.

More precisely, let's first recall the standard way to encrypt a message using LWE. Taking Regev's encryption for example, the public key consists of a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^m$, where $\mathbf{u}$ is a LWE sample, i.e. $\mathbf{u} = \mathbf{A}^T \mathbf{s} + \mathbf{e}$. To encrypt, the user chooses uniformly random vectors $\mathbf{x} \in \{0,1\}^m$ and error e, and computes $\mathbf{c}_1 = \mathbf{A}\mathbf{x}, c_2 = \langle \mathbf{u}, \mathbf{x} \rangle + e + m \cdot \lfloor q/2 \rfloor$. When decrypting, the user computes $c_2 - \mathbf{s}^T \mathbf{c}_1$ to remove the common part $\mathbf{s}^T \mathbf{A} \mathbf{x}$ and recover the message from the "error". Instead, our construction retrieve a shared secret from the common part for each party. More specifically, suppose Alice and Bob have secret keys $\mathbf{s}_A \in \mathbb{Z}_q^n$ and $\mathbf{s}_B \in \mathbb{Z}_q^n$. In the key exchange stage with public parameters $\mathbf{M} \in \mathbb{Z}_q^{n\times n}$, Alice and Bob send $\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + \mathbf{e}_A$ and $\mathbf{p}_B = \mathbf{M}^T\mathbf{s}_B + \mathbf{e}_B$ to each other, respectively. When receiving $\mathbf{p}_B$, Alice computes $\mathbf{s}_A^T\mathbf{p}_B$. Similarly, Bob computes $\mathbf{s}_B^T\mathbf{p}_A$. Note that $\mathbf{s}_A^T\mathbf{p}_B$ and $\mathbf{s}_B^T\mathbf{p}_A$ are very close to $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B$. Finally, we construct a way to derive a shared secret from the two values close to $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B$.

To illustrate the security of the above scheme, we need to show that the transcriptions and the extracted key are pseudorandom. First, due to the squared form of the matrix $\mathbf{M}$, the transcripts $\mathbf{p}_A$ and $\mathbf{p}_B$ are just LWE samples with independent secrets. This implies that they can be replaced by uniformly random vectors in $\mathbb{Z}_q^n$ by the LWE assumption. In order to make the extracted key look random, we additionally add noises to $\mathbf{s}_A^T\mathbf{p}_B$ and $\mathbf{s}_B^T\mathbf{p}_A$, respectively. Notice that if $\mathbf{p}_A$ and $\mathbf{p}_B$ are uniformly random, the "noisy" form of $\mathbf{s}_A^T\mathbf{p}_B$ and $\mathbf{s}_B^T\mathbf{p}_A$ are LWE samples, which is pseudorandom under LWE assumption. In the security proof, we use standard hybrid games and deal exclusively with the squared matrix $\mathbf{M}$.

Key exchange is widely used in secure Internet communications, which is, therefore, very important in practical applications. In term of practical applications, one may argue that we can always construct easily a key exchange scheme using a public key encryption scheme, and why do we need a new key exchange scheme? Surely, we can compare our scheme with a key exchange and a key transport scheme on LWE type of encryption, but this comparison surely depends on the assumption what is overhead cost and what is the real key exchange cost. We can show that there could be indeed substantial advantage in our scheme in terms of communication cost and (or) computation cost, we will illustrate the point by using our LWE based one and our RLWE based one respectively.

1.2 Organization

In Section 2, we give some basic notions and facts. The protocol based on LWE problem is given in Section 3, and the more efficient protocol based on RLWE problem is given in Section 4. In Section 5, we describe our interactive key exchange scheme. In the last section, we will present the conclusion and the discussion.

2 Preliminaries

Notations. We use bold capital letters to denote matrices, and bold lowercase letters to denote vectors. The notation $\mathbf{A}^T$ denotes the transpose of the matrix $\mathbf{A}$. A function $\mathrm{negl}(\lambda)$ is *negligible*, if it vanishes faster than the inverse of any polynomial in λ. The *statistical distance* between two distributions X, Y over some finite or countable set S is defined as $\Delta(X,Y) = \frac{1}{2}\sum_{s\in S}\big|\Pr[X = s] - \Pr[Y = s]\big|$. X and Y are statistically indistinguishable if $\Delta(X,Y)$ is negligible.

Let Λ be a discrete subset of $\mathbb{Z}^m$. For any vector $\mathbf{c} \in \mathbb{R}^m$ and any positive parameter $\sigma \in \mathbb{R}_{>0}$, let $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x}-\mathbf{c}\|^2/\sigma^2)$ be the Gaussian function on $\mathbb{R}^m$ with center $\mathbf{c}$ and parameter σ. Denote $\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in\Lambda}\rho_{\sigma,\mathbf{c}}(\mathbf{x})$ be the discrete integral of $\rho_{\sigma,\mathbf{c}}$ over Λ, and $\mathcal{D}_{\Lambda,\sigma,\mathbf{c}}$ be the discrete Gaussian distribution over Λ with center $\mathbf{c}$ and parameter σ. Specifically, for all $\mathbf{y} \in \Lambda$, we have $\mathcal{D}_{\Lambda,\sigma,\mathbf{c}}(\mathbf{y}) = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{y})}{\rho_{\sigma,\mathbf{c}}(\Lambda)}$. For notional convenience, $\rho_{\sigma,\mathbf{0}}$ and $\mathcal{D}_{\Lambda,\sigma,\mathbf{0}}$ are abbreviated as ρ_σ and $\mathcal{D}_{\Lambda,\sigma}$, respectively.

The Learning with Errors Problem We recall the learning with errors (LWE) problem, a classic hard problem on lattices defined by Regev [21].

Definition 1. *Let $n \geq 1$ and $q \geq 2$ be integers, let $\alpha \in (0,1)$. For $\mathbf{s} \in \mathbb{Z}_q^n$, let $A_{\mathbf{s},\alpha}$ be the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.*

The LWE problem is : for uniformly random $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, given a poly(n) number of samples that are either from $A_{\mathbf{s},\alpha}$ or uniformly random in $\mathbb{Z}_q^n \times \mathbb{Z}_q$, output 0 if the former holds and 1 if the latter holds.

It is known that when $\alpha q \geq 2\sqrt{n}$ and $q = \text{poly}(n)$, this decision problem is at least as hard as approximating several problems on n-dimensional lattices in the *worst-case* to within $\widetilde{O}(n/\alpha)$ factors with a quantum computer [21] or on a classical computer for a subset of these problems [20]. Very recent work by Brakerski *et al.* [8] shows the classical hardness for LWE. A simple analysis shows that for any $t \in \mathbb{Z}^+$ and $gcd(t,q) = 1$, then the LWE assumption still holds if we choose $b = \langle \mathbf{a}, \mathbf{s} \rangle + te$. The HNF-LWE assumption [4] says that the hardness preserves even if we choose the secret from the error distribution, i.e. $\mathbf{s} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$. We will exclusively use this assumption.

We give a bound of the norm of the Gaussian distribution.

Lemma 1. *For any $s \geq \omega(\sqrt{\log n})$, then we have*

$$\Pr_{x \leftarrow \mathcal{D}_{\mathbb{Z}^n,s}}[\|x\| > s\sqrt{n}] \leq 2^{-n}.$$

3 Key Exchange Protocol from LWE

Key exchange protocols are very important cryptographic protocols. The original Diffien-Hellman key exchange protocol [12] is built on the fact that the exponential maps are commutative, namely

$$g^{ab} = (g^a)^b = (g^b)^a,$$

over some multiplicative group $\mathbb{G}$ with large order p. This construction does not need trapdoor function. If we look carefully why the key exchange above works, one realize we may do the same thing using the associativity and commutativity of computing the value of bilinear form, namely,

$$\mathbf{x}^T \mathbf{A} \mathbf{y} = (\mathbf{x}^T \mathbf{A})\mathbf{y} = \mathbf{x}^T(\mathbf{A}\mathbf{y}),$$

where $\mathbf{A}$ is a $n \times n$ matrix in $\mathbb{Z}_q$ and $\mathbf{x}, \mathbf{y}$ are vectors in $\mathbb{Z}_q^n$. Here this computation can be viewed a pairing of the two vector $\mathbf{x}, \mathbf{y}$ via the corresponding bilinear form.

Surely we need to introduce small errors, namely, the idea of LWE problem, to make the scheme secure. Our basic idea is that we can use the Hermit normal form of LWE (HNF-LWE) problem to build a key exchange protocol like the Diffie-Hellman key exchange protocol. The protocol can be set up as follows.

3.1 Construction

Two parties Alice and Bob decide to do a key exchange over an open channel.

- The system first generates the public parameters q, n, α, t, which we will specify later. Samples a uniformly random matrix $\mathbf{M} \leftarrow \mathbb{Z}_q^{n \times n}$.

- Alice and Bob choose vectors $\mathbf{s}_A, \mathbf{s}_B \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$ independently. Then, Alice computes $\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + t\mathbf{e}_A \mod q$, where $\mathbf{e}_A \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$. Sends $\mathbf{p}_A$ to Bob.

- Receiving p_A, Bob first chooses error vector $e'_B \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$. Computes $K_B = \mathbf{p}_A^T \cdot \mathbf{s}_B + te'_B \mod q$. Sets $\mathsf{Signal} = 0$ if $K_B \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$; $\mathsf{Signal} = 1$ otherwise. Bob obtains the shared key $SK_B = (K_B + \mathsf{Signal} \cdot \frac{q-1}{2} \mod q) \mod t$. Finally Bob samples $\mathbf{e}_B \leftarrow \mathcal{D}_{\mathbb{Z}^n,\alpha q}$, computes $\mathbf{p}_B = \mathbf{M}^T \cdot \mathbf{s}_B + t\mathbf{e}_B \mod q$. Sends $(\mathbf{p}_B, \mathsf{Signal})$ to Alice.

- Once get $(\mathbf{p}_B, \mathsf{Signal})$, Alice samples $e'_A \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ and computes $K_A = \mathbf{s}_A^T\mathbf{p}_B + te'_A \mod q$, and obtains $SK_A = (K_A + \mathsf{Signal} \cdot \frac{q-1}{2} \mod q) \mod t$.

Correctness We now show that if Alice and Bob run the protocol honestly, they will share an identical key.

Lemma 2. *If $4(\alpha q)^2 \cdot n \cdot t \leq \frac{q-1}{4}$, then $SK_A = SK_B$ with overwhelming probability.*

Proof. The form of K_A, K_B are as follows. $K_A = \mathbf{s}_A^T(\mathbf{M}^T \cdot \mathbf{s}_B + t\mathbf{e}_B) + t\mathbf{e}'_A = \mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B + t(\mathbf{s}_A^T\mathbf{e}_B + e'_A)$. $K_B = (\mathbf{s}_A^T\mathbf{M}^T + t\mathbf{e}_A^T)\mathbf{s}_B + te'_B = \mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B + t(\mathbf{e}_A^T\mathbf{s}_B + e'_B)$. We first consider $\mathsf{Signal} = 0$, which means that $K_B \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$. Now we can rewrite $K_A = K_B + t(\mathbf{s}_A^T\mathbf{e}_B + e'_A - \mathbf{e}_A^T\mathbf{s}_B - e'_B) \mod q$. From Lemma 1, we have that

$$|t(\mathbf{s}_A^T\mathbf{e}_B + e'_A - \mathbf{e}_A^T\mathbf{s}_B - e'_B)| \leq 4t \cdot (\alpha q\sqrt{n}) \cdot (\alpha q\sqrt{n}) = 4t(\alpha q)^2 \cdot n,$$

with overwhelming probability. By the hypothesis and $K_B \mod q \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$, we know that $K_B \mod q + t(\mathbf{s}_A^T\mathbf{e}_B + e'_A - \mathbf{e}_A^T\mathbf{s}_B - e'_B) \in [-\frac{q-1}{2}, \frac{q-1}{2}]$. Therefore, $K_A \mod q = K_B \mod q + t(\mathbf{s}_A^T\mathbf{e}_B + e'_A - \mathbf{e}_A^T\mathbf{s}_B - e'_B)$, and $SK_B = (K_B \mod q) \mod t = (K_A \mod q) \mod t = SK_A$.

Moreover, we show that $SK_A = SK_B = (\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B \mod q) \mod t$ when $\mathsf{Signal} = 0$. Since $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B = K_B - t(\mathbf{e}_A^T\mathbf{s}_B + e'_B) \mod q$, $K_B \mod q \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$ and $|t(\mathbf{e}_A^T\mathbf{s}_B + e'_B)| \leq \frac{q-1}{4}$. Hence $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B \mod q = K_B \mod q - t(\mathbf{e}_A^T\mathbf{s}_B + e'_B)$.

The case of $\mathsf{Signal} = 1$ is analogous. Since $K_B + \frac{q-1}{2} \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$, then the analysis is exactly as above. In this case, the shared key $SK_A = SK_B = (\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B + \frac{q-1}{2} \mod q) \mod t$. □

Remark. We note that for the correctness of our protocol, Bob has to send a signal to Alice to tell her that the resulting K_B is in the range $[-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$ or not. The reason is to make sure that the error terms in K_B and K_A do not result different modulo q operations. The drawback of signal is that the adversary will also know the "main" part, say $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B$ or $\mathbf{s}_A^T\mathbf{M}^T\mathbf{s}_B + \frac{q-1}{2} \mod q$, lies in $[-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$. This does not harm the security, since if we can show the "main" part is (pseudo)random in $[-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$, the additional modulo t operation makes the shared key uniform in $\mathbb{Z}_t$.

Parameter Selection. A reasonable way to select the parameters is $n = \lambda$, $q = \lambda^4$,$t = 2$, $\alpha = 1/\lambda^3$. It's easy to verify that $\alpha q \geq \sqrt{n}$ and the correctness holds.

3.2 Security

We now define the passive security of a key exchange protocol. Intuitively, any PPT adversary should not distinguish a real shared key to a random one even if he gets the transcripts of the protocol. More specifically, we define the advantage of an adversary $\mathcal{A}$:

$$\mathbf{Adv}_{\mathcal{A}} = \Pr[b' \leftarrow \mathcal{A}(\text{transcripts}, K_b), b \leftarrow \{0,1\}, K_0 \text{ is real}, K_1 \text{ is random} : b = b'] - 1/2.$$

Definition 2. *We say a key exchange protocol is secure under passive adversary, if for any PPT adversary the advantage is negligible.*

We now slightly change the definition according to our construction, we do not need the adversary to distinguish the shared key, instead we want it to distinguish K_A or K_B from uniformly random in $\mathbb{Z}_q$. I.e. we prove that

$$\Pr[b' \leftarrow \mathcal{A}(\mathbf{M}, \mathbf{p}_A, \mathbf{p}_B, K_b), b \leftarrow \{0,1\}, K_0 = K_B, K_1 \leftarrow_R \mathbb{Z}_q : b = b'] - 1/2$$

is negligible (we can also replace $K_0 = K_A$).

Theorem 1. *The construction above is secure against passive PPT adversaries, if the HNF-LWE assumption holds.*

Proof. We prove the security by a series of games. The first game $\mathbf{Game}_0$ is the real game which the adversary gets the real shared key K_B, while the last game $\mathbf{Game}_4$ the adversary gets a random key. We show that the views of $\mathbf{Game}_0$ and $\mathbf{Game}_4$ are computational indistinguishable for any PPT adversaries, under the HNF-LWE assumption.

$\mathbf{Game}_0$. This is the real game between the protocol challenger and the passive adversary $\mathcal{A}$. That is the adversary obtains $\mathbf{M}, \mathbf{p}_A, \mathbf{p}_B, \mathsf{Signal}, K_B$, where $\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + t\mathbf{e}_A$, $\mathbf{p}_B = \mathbf{M}^T\mathbf{s}_B + t\mathbf{e}_B$ and $K_B = \mathbf{p}_A^T\mathbf{s}_B + te'_B$. Then $\mathcal{A}$ outputs a guess b'.

$\mathbf{Game}_1$. This game is identical to $\mathbf{Game}_0$ except that instead of setting $\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + t\mathbf{e}_A$ and $K_B = \mathbf{p}_A^T\mathbf{s}_B + te'_B$. The challenger sets $\mathbf{p}_A = \mathbf{b}_A$ and $K_B = \mathbf{b}_A^T \cdot \mathbf{s}_B + te'_B$, where $\mathbf{b} \leftarrow_R \mathbb{Z}_q^n$.

In Lemma 3, we show that under the HNF-LWE assumption, the views in $\mathbf{Game}_0$ and $\mathbf{Game}_1$ are computationally indistinguishable for any PPT passive adversaries.

$\mathbf{Game}_2$. This game is identical to $\mathbf{Game}_1$ except that instead of setting $\mathbf{p}_B = \mathbf{M}^T\mathbf{s}_B + t\mathbf{e}_B$ and $K_B = \mathbf{b}_A^T \cdot \mathbf{s}_B + te'_B$. The challenger sets $\mathbf{p}_B = \mathbf{b}_B$ and $K_B = u$, where $\mathbf{b}_B \leftarrow_R \mathbb{Z}_q^n$ and $u \leftarrow_R \mathbb{Z}_q$.

We show the views for any PPT passive adversaries in $\mathbf{Game}_1$ and $\mathbf{Game}_2$ are computationally indistinguishable, if the HNF-LWE assumption holds. The proof is given in Lemma 4.

$\mathbf{Game}_3$. This game is identical to $\mathbf{Game}_2$ except that instead of setting $\mathbf{p}_A = \mathbf{b}_A$. The challenger sets $\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + t\mathbf{e}_A$.

In Lemma 5, we prove the views in $\mathbf{Game}_2$ and $\mathbf{Game}_3$ are computationally indistinguishable, if the HNF-LWE assumption holds.

$\mathbf{Game}_4$. This game is identical to $\mathbf{Game}_3$ except that instead of setting $\mathbf{p}_B = \mathbf{b}_B$. The challenger sets $\mathbf{p}_B = \mathbf{M}^T\mathbf{s}_B + t\mathbf{e}_B$.

In Lemma 6, we prove that the views in $\mathbf{Game}_3$ and $\mathbf{Game}_4$ are indistinguishable, if the HNF-LWE assumption holds. The conclusion follows from Lemma 3,4,5,6 directly. □

Lemma 3. *Any PPT passive adversary can not distinguish* $\mathbf{Game}_0$ *and* $\mathbf{Game}_1$*, if the HNF-LWE assumption holds.*

Proof. We prove the lemma by showing that if there exists an adversary $\mathcal{A}$ who can distinguish $\mathbf{Game}_0$ and $\mathbf{Game}_1$, then we can construct another adversary $\mathcal{B}$ to distinguish the HNF-LWE samples from uniform. $\mathcal{B}$ works as follows. Once obtaining challenges $(\mathbf{A}, \mathbf{u}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$ from the HNF-LWE oracle, where $\mathbf{u}$ is either $\mathbf{As}+\mathbf{e}$ or uniformly random in $\mathbb{Z}_q^n$, $\mathcal{B}$ sets $\mathbf{M} = \mathbf{A}$, $K_B = \mathbf{u}^T\mathbf{s}_B + t\mathbf{e}'_B$ and computes $\mathbf{p}_B = \mathbf{M}^T\mathbf{s}_B + t\mathbf{e}_B$. Finally $\mathcal{B}$ sends $(\mathbf{M}, \mathbf{p}_A, \mathbf{p}_B, \mathsf{Signal}, K_B)$ to $\mathcal{A}$. $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. We note that $\mathcal{B}$ can sample $\mathbf{s}_B$ and the errors and computes Signal by himself, since $\mathbf{s}$ is independent of $\mathbf{s}_B$.

If $\mathbf{u}$ is an LWE sample, then what $\mathcal{A}$ obtains are exactly the same as in $\mathbf{Game}_0$, if $\mathbf{u}$ is uniformly random in $\mathbb{Z}_q^n$, then what $\mathcal{A}$ obtains are exactly the same as in $\mathbf{Game}_1$. This implies that if $\mathcal{A}$ can distinguish $\mathbf{Game}_0$ and $\mathbf{Game}_1$ with noticeable advantage, then $\mathcal{B}$ can distinguish HNF-LWE samples from uniformly random with the same advantage. This finishes the proof. □

Lemma 4. *Any PPT passive adversary can not distinguish* $\boldsymbol{Game}_1$ *and* $\boldsymbol{Game}_2$*, if the HNF-LWE assumption holds.*

Proof. We prove this lemma by showing that if there exists an adversary $\mathcal{A}$ distinguishes $\mathbf{Game}_1$ and $\mathbf{Game}_2$, then we can construct a PPT adversary $\mathcal{B}$ to distinguish the HNF-LWE samples from uniform. $\mathcal{B}$ works as follows. Once obtaining challenges $(\mathbf{A}, \mathbf{u}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$ and $(\mathbf{b}, u) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathbf{u}$ and u are either $\mathbf{A}^T\mathbf{s} + \mathbf{e}, \mathbf{b}^T\mathbf{s} + e$ or uniformly random in $\mathbb{Z}_q^n$ and $\mathbb{Z}_q$ respectively, $\mathcal{B}$ sets $\mathbf{M} = \mathbf{A}$ and $\mathbf{p}_A = \mathbf{b}$, let $\mathbf{p}_B = \mathbf{u}$ and $K_B = u$, and compute Signal from K_B. $\mathcal{B}$ sends $(M, \mathbf{p}_A, \mathbf{p}_B, \mathsf{Signal}, K_B)$ to $\mathcal{A}$, and outputs whatever $\mathcal{A}$ outputs. It's easy to see that if $\mathbf{u}, u$ are LWE samples, then what $\mathcal{A}$ gets are exactly the same as in $\mathbf{Game}_1$; if $\mathbf{u}, u$ are uniformly random, then what $\mathcal{A}$ gets are exactly the same as in $\mathbf{Game}_2$. Therefore, if $\mathcal{A}$ can distinguish the two games with noticeable advantage, then $\mathcal{B}$ can break the HNF-LWE problem with noticeable advantage. This complete the proof. □

Lemma 5. *Any PPT passive adversary can not distinguish* $\boldsymbol{Game}_2$ *and* $\boldsymbol{Game}_3$*, if the HNF-LWE assumption holds.*

Proof. The proof is similar to Lemma 3, except we still choose K_B uniformly from $\mathbb{Z}_q$. □

Lemma 6. *Any PPT passive adversary can not distinguish* $\boldsymbol{Game}_3$ *and* $\boldsymbol{Game}_4$*, if the HNF-LWE assumption holds.*

Proof. The proof is similar to Lemma 4, except we still choose K_B uniformly from $\mathbb{Z}_q$. □

Key Exchange Protocol with Multiple Bits. In order to get multiple shared secret bits in the protocol, one can use the matrix secret form of LWE assumption. More specifically, Alice and Bob choose secret matrix $\mathbf{S}_A, \mathbf{S}_B \in \mathbb{Z}_q^{n\times n}$ instead of $\mathbf{s}_A, \mathbf{s}_B$ (still from the error distribution). It's easy to extend the other part to get multiple shared secret bits. The security straightforwardly from the underlying HNF-LWE assumption by standard hybrid argument.

Comparisons . We now give some comparisons by directly using public key encryption scheme to do key exchange. The main idea of using PKE is as follows: for two parties A and B with key pair (pk_A, sk_A) and (pk_B, sk_B), respectively. A chooses a bit a uniformly at random, and encryption it by using B's public key $c_B = Enc(pk_B, a)$ and sends c_B to B. Similarly B choose a uniform bit b and sends $c_A = Enc(pk_A, b)$ to A. A and B decrypt the ciphertext by using their own secret key and compute $a \oplus b$. We note that, by using the PKE based key exchange, the users need to first download the public key of the party he/she wants to communicate. Therefore, it incurs more communication complexity. While in our scheme, the public parameter $\mathbf{M}$ is generated once for all, namely a public authority like NIST can generate one matrix M that any two parties can use the same M, while the security is not affected. We focus on LWE-based encryptions and estimate the complexity for 1 bit secret key. The comparisons are given in Table 1:

Table 1. Comparisons between LWE-based ones for 1-bit secret key

	Pub. Param.	Commun. Comp.	Comput. Comp.	Assumption
Reg'05 [21]	$4(n+1)n\log^2 q$	$(4n^2+6n)\log^2 q + 2\log q$	$4n^2 \log q$	$\mathsf{SIVP}_{\tilde{O}(n^3)}$
LP'12 [18]	$4n^2 \log q$	$4(n^2+n)\log q$	$6n^2$	$\mathsf{SIVP}_{\tilde{O}(n^3)}$
Ours	$n^2 \log q$	$2n \log q + 1$	$2n^2$	$\mathsf{SIVP}_{\tilde{O}(n^4)}$

Pub. Param. means the size of public parameter; Commun. Comp. means the communication complexity; Comput. Comp. means the computation complexity and is estimated by the number of multiplications in $\mathbb{Z}_q$.

We compare the efficiency of our scheme with key transport schemes based on PKE from LWE. Intuitively, in a key transport scheme, party A chooses a uniformly random bit s and encrypts it by using B's public key to encrypt it $c = Enc(pk_B, s)$ and then sends c to B. B uses its secret key to decrypt c and recover s. The session key between A and B is s. Therefore, the communication complexity and computation complexity will be half as the key exchange schemes based on PKE. From the results in Table 1, even in such a scenario, the efficiency of our scheme is still substantially better in terms of communication complexity and computation complexity.

4 Key Exchange Protocol from Ring-LWE

In this section, we show how to get a more efficient key exchange protocol from the Ring-LWE problem [19]. Consider the ring $R = \mathbb{Z}[x]/f(x)$, where $f(x) = x^n + 1$ and n is a power of 2. For an integer q, let $R_q = R/qR$. Any element in R_q is represented by a degree $n-1$ polynomial, which can also be viewed as a vector with its corresponding coefficients as its entries. For an element

$$a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1},$$

we define $\|a\| = \max|a_i|$, the ℓ_∞ norm of the vector $(a_0, a_1, ..., a_{n-1})$. Furthermore, it's easy to get that $\|x \cdot y\| \leq n\|x\| \cdot \|y\|$ for any $x, y \in R$. For convenience, we do not give the specific description of the error distribution, since we only care the norm of the element from the distribution. Denote χ (whose support is R) to be β-bounded, if $\Pr[\|x\| > \beta : x \leftarrow \chi] \leq \mathrm{negl}(n)$. We recall the definition of Ring-LWE proposed by Lyubashevsky, Peikert and Regev [19].

Definition 3. *Let $n \geq 1$ be a power of 2 and $q \geq 2$ be an integer, let $R = \mathbb{Z}[x]/f(x)$, where $f(x) = x^n + 1$, and $R = R/qR$. Let χ be β-bounded. For $s \in R_q$, let $A_{s,\chi}$ be the distribution on $R_q \times R_q$ obtained by choosing $a \leftarrow R_q$ uniformly at random, $e \leftarrow \chi$, and output $(a, a \cdot s + e \mod q)$.*

The RLWE problem is : for uniformly random $s \leftarrow R_q$, given a poly(n) number of samples that are either from $A_{s,\chi}$ or uniformly random in $R_q \times R_q$, output 0 if the former holds and 1 if the latter holds.

The $\mathrm{RLWE}_{n,q,\chi}$ assumption is that the $\mathrm{RLWE}_{n,q,\chi}$ problem is infeasible. Denote the assumption by $\mathrm{RLWE}^{(m)}_{n,q,\chi}$ when we require the indistinguishability to hold given only m samples. We state the hardness of the special case of $\mathrm{RLWE}^{(m)}_{n,q,\chi}$ described in [19] as follows.

Theorem 2 ([19]). *For the ring $R = \mathbb{Z}[X]/f(x)$, $f(x) = x^n + 1$, where n is a power of 2, and a prime integer $q = q(n) = 1 \mod 2n$, and $\beta = \omega(\sqrt{n \log n})$, there is an efficiently samplable distribution χ that outputs elements of R with norm at most β with overwhelming probability, such that if there exists an efficient algorithm that solves $\mathrm{RLWE}^{(m)}_{n,q,\chi}$, then there is an efficient quantum algorithm for solving $n^{2.5} \cdot (q/\beta) \cdot (nm/\log(nm))^{1/4}$-approximate worst-case* SVP *for ideal lattices over R.*

The HNF-RLWE assumption [4] says that the hardness preserves even if we choose the secret from the error distribution, i.e. $s \leftarrow \chi$.

4.1 Construction

We now describe the key exchange protocol based on RLWE assumption.

- The system first generates the public parameters $q, n, \chi, \beta, t, R = \mathbb{Z}[x]/f(x)$, where $f(x) = x^n + 1$ and n is a power of 2. Samples a uniformly random element $m \leftarrow R_q$.

- Alice and Bob choose elements $s_A, s_B \leftarrow \chi$ independently. Then, Alice computes $p_A = ms_A + te_A \mod q$, where $e_A \leftarrow \chi$. Sends p_A to Bob.

- Receiving p_A, Bob first chooses error vector $e'_B \leftarrow \chi$. Computes $K_B = p_A \cdot s_B + te'_B \mod q$. For $i = 0, .., n-1$, sets $\mathsf{Signal}_i = 0$ if $(K_B)_i \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$; $\mathsf{Signal}_i = 1$ otherwise. Denote $\mathsf{Signal} = (\mathsf{Signal}_0, ..., \mathsf{Signal}_{n-1})$. Bob obtains the shared key $SK_B = (K_B + \frac{q-1}{2} \cdot \mathsf{Signal} \mod q) \mod t$. Finally Bob samples $e_B \leftarrow \chi$, computes $p_B = m \cdot s_B + te_B \mod q$. Sends (p_B, Signal) to Alice.

- Once getting (p_B, Signal), Alice samples $e'_A \leftarrow \chi$ and computes $K_A = s_A p_B + te'_A \mod q$, and obtains $SK_A = (K_A + \frac{q-1}{2} \cdot \mathsf{Signal} \mod q) \mod t$.

Correctness We now show that if Alice and Bob run the protocol honestly, they will share an identical key.

Lemma 7. *If $4tn\beta^2 \leq \frac{q-1}{4}$, then $SK_A = SK_B$ with overwhelming probability.*

Proof. The form of K_A, K_B are as follows. $K_A = ms_As_B + t(s_Ae_B + e'_A) \mod q$. $K_B = ms_As_B + t(e_As_B + e'_B) \mod q$. We first consider $\mathsf{Signal}_i = 0$, which means that $(K_B)_i \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$. Now we can rewrite $(K_A)_i = (K_B)_i + \Big(t(s_Ae_B + e'_A - e_As_B - e'_B)\Big)_i \mod q$. We have that

$$|\Big(t(s_Ae_B + e'_A - e_As_B - e'_B)\Big)_i| \leq \|t(s_Ae_B + e'_A - e_As_B - e'_B)\| \leq 4tn\beta^2,$$

with overwhelming probability. By the hypothesis and $(K_B)_i \mod q \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$, we know that $(K_B)_i \mod q + (t(s_Ae_B + e'_A - e_As_B - e'_B))_i \in [-\frac{q-1}{2}, \frac{q-1}{2}]$. Therefore, $(K_A)_i \mod q = (K_B)_i \mod q + (t(s_Ae_B + e'_A - e_As_B - e'_B))_i$, and $(SK_B)_i = ((K_B)_i \mod q) \mod t = ((K_A)_i \mod q) \mod t = (SK_A)_i$.

Moreover, we show that $(SK_A)_i = (SK_B)_i = ((ms_As_B)_i \mod q) \mod t$ when $\mathsf{Signal}_i = 0$. Since $(ms_As_B)_i = (K_B)_i - (t(e_As_B + e'_B))_i \mod q$, $(K_B)_i \mod q \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$ and $|(t(e_As_B + e'_B))_i| \leq \frac{q-1}{4}$. Hence $(ms_As_B)_i \mod q = (K_B)_i \mod q + (t(e_As_B + e'_B))_i$.

The case of $\mathsf{Signal}_i = 1$ is analogous. Since $(K_B)_i + \frac{q-1}{2} \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$, then the analysis is exactly as above. In this case, the shared key $(SK_A)_i = (SK_B)_i = ((ms_As_B)_i + \frac{q-1}{2} \mod q) \mod t$. □

Parameter Selection. A reasonable way to select the parameters is $n = \lambda$, $q = \lambda^4$,$t = 2$, $\beta = \lambda$.

Theorem 3. *The construction above is secure against passive PPT adversaries, if the HNF-RLWE assumption holds.*

Proof. The proof is almost the same as in 1, we omit it here. □

Comparisons Here, we give comparisons between our scheme and other key exchange schme based on public key encryption from RLWE. We use two examples, one is the RLWE-based scheme from Lyubashevsky *et al.* [19], and the other one is the NTRU variant from Stehlé and Steinfeld [22]. Due to the property of RLWE, our scheme can agree on n bit secret key once. We note that the public parameter m can be produced once for all, therefore, it significantly reduce the communication cost. The comparisons are given in Table 2. When comparing to the key transport schemes based on PKE, where the communication and computation cost will be cut to half for encryption based schemes, the efficiency of our scheme is still better than the LPR'10 [19] scheme in communication cost (1/2) but worse in computation cost (4/3); and our scheme is slightly worse than the SS'11 [22] scheme. But we note that the assumption of the SS'11 [22] is much stronger. Therefore, to obtain same security, one needs to increase the security parameter in SS'11 [22], which results much worse efficiency. This means our scheme could still have substantial advantage in terms of practical applications.

Table 2. Comparisons between RLWE-based ones for n bit secret key

	Pub. Param.	Commun. Comp.	Comput. Comp.	Assumption
LPR'10 [19]	$4n \log q$	$8n \log q$	6	$\mathsf{Ideal\text{-}SIVP}_{\tilde{O}(n^3)}$
SS'11 [22]	$2n \log q$	$4n \log q$	4	$\mathsf{Ideal\text{-}SIVP}_{\tilde{O}(n^8)}$
Ours	$n \log q$	$2n \log q + n$	4	$\mathsf{Ideal\text{-}SIVP}_{\tilde{O}(n^{4.5})}$

Pub. Param. means the size of public parameter; Commun. Comp. means the communication complexity; Comput. Comp. means the computation complexity and is estimated by the number of multiplications in the ring R_q.

5 Interactive Multiparty Key Exchange Protocol

In this section, we describe an interactive multiparty key exchange protocol based on RLWE problem. Although the provable security of the protocol seems plausible, we still can not do it, and we leave it as an open problem.

We now describe the interactive multiparty key exchange protocol.

- For a set of k users, the system first generates the public parameters $q, n, \chi, \beta, t, R = \mathbb{Z}[x]/f(x)$, where $f(x) = x^n + 1$ and n is a power of 2. Samples a uniformly random element $m \leftarrow R_q$.

- For $i \in \{0, ..., k-1\}$, the user i chooses random $s_i \leftarrow \chi$ and $e_i^0 \leftarrow \chi$. Computes $p_i^0 = ms_i + te_i^0 \in R_q$, and sends p_i^0 to the user $i+1$. Then for $1 \leq j \leq k-2$, user $i+j \mod k$ computes $p_i^j = s_{i+j \mod k} \cdot p_i^{j-1} + te_i^j$, where $e_i^j \in \chi$, and sends p_i^j to the user $i+j+1 \mod k$.

- For the user 0, he or she first chooses $\hat{e}_0 \leftarrow \chi$ and computes $K_0 = p_1^{k-2} \cdot s_0 + t\hat{e}_0$. For $\tau = 0, .., n-1$, sets $\mathsf{Signal}_\tau = 0$ if $(K_0)_\tau \in [-\frac{q-1}{4}, \frac{q-1}{4}] \cap \mathbb{Z}$; $\mathsf{Signal}_\tau = 1$ otherwise. Denote

$\mathsf{Signal} = (\mathsf{Signal}_0, ..., \mathsf{Signal}_{n-1})$. The user 0 obtains the shared key $SK_0 = (K_0 + \frac{q-1}{2} \cdot \mathsf{Signal} \mod q) \mod t$. Finally, the user 0 broadcasts Signal.

- For users $1 \leq i \leq k-1$. they first choose $\hat{e}_i \leftarrow \chi$ and compute $K_i = p_{i+1 \mod k}^{k-2} \cdot s_i + t\hat{e}_i$ and each obtains the shared secret key $SK_i = (K_i + \frac{q-1}{2} \cdot \mathsf{Signal} \mod q) \mod t$.

Correctness We now show that if Alice and Bob run the protocol honestly, they will share an identical key.

Lemma 8. *If $2k \cdot t \cdot n^k \beta^{k+1} \leq \frac{q-1}{4}$, then all the k parties share the same secret key with overwhelming probability.*

Proof. The correctness is very similar to the RLWE base two party key exchange protocol. Let's first look at K_0, we can rewrite it in the form: $K_0 = m \prod_{i=0}^{k-1} s_i + \Delta_0$, where:

$$\Delta_0 = s_0 \prod_{i=2}^{k-1} s_i \cdot t \cdot e_1^0 + s_0 \prod_{i=3}^{k-1} s_i \cdot t \cdot e_1^1 + \cdots + s_0 \cdot s_{k-1} \cdot t \cdot e_1^{k-3} + s_0 \cdot t \cdot e_1^{k-2} + t\hat{e}_0.$$

Note that $\|\Delta_0\| \leq k \cdot t \cdot n^k \beta^{k+1}$. Similarly, we can compute $K_j = m \prod_{i=0}^{k-1} s_i + \Delta_j$ where $\|\Delta_j\| \leq k \cdot t \cdot n^k \beta^{k+1}$ and $1 \leq j \leq k-1$. Notice that since $\|\Delta_0 - \Delta_j\| \leq 2k \cdot t \cdot n^k \beta^{k+1} \leq \frac{q-1}{2}$ for $1 \leq j \leq k-1$, we can apply the same analysis on Lemma 7 to finish the remaining part of this lemma. □

6 Conclusion

In this paper, we use the LWE problem to build a new, simple and provably secure key exchange protocol. We show that our scheme have substantial advantages in practical applications when compared with similar scheme derived from the encryption schemes based on the LWE problem. We also extend the construction to the RLWE case. Our construction is a significant additional step in showing how versatile the LWE assumption can be.

The work in this paper can be attributed to the understanding that the basic idea behind the LWE problem itself can be viewed as certain form of inner product with small errors that somehow can be eliminated for certain applications. Our construction can be viewed as an extension of this idea to the case of a bilinear pairing, namely a pairing of bilinear forms with errors. In addition, the reason why the scheme works well actually depends on the associativity and the commutativity of the multiplications in both the non-commutative rings (the LWE problem) and the commutative rings (the RLWE problem). We believe that exploring further algebraic properties of the non-commutative rings could yield even more interesting cryptographic protocols, such as certain homomorphic properties over non-commutative operations over matrices.

Using the same idea, we are now in the process finishing works in building simple and provable secure identity-based encryption systems and scalable key distribution systems for large networks.

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (h) ibe in the standard model. In *Advances in Cryptology–EUROCRYPT 2010*, pages 553–572. Springer, 2010.
2. S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee. Functional encryption for threshold functions (or fuzzy ibe) from lattices. In *Public Key Cryptography*, pages 280–297, 2012.

3. S. Agrawal, D. Freeman, and V. Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. In *Advances in Cryptology–ASIACRYPT 2011*, pages 21–40. Springer, 2011.
4. B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. *Advances in Cryptology-CRYPTO 2009*, pages 595–618, 2009.
5. Xavier Boyen. Attribute-based functional encryption on lattices. In *Theory of Cryptography*, pages 122–142. Springer, 2013.
6. Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In *Advances in Cryptology–CRYPTO 2012*, pages 868–886. Springer, 2012.
7. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *ITCS*, pages 309–325, 2012.
8. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *Proceedings of the 45th annual ACM symposium on Symposium on theory of computing*, pages 575–584. ACM, 2013.
9. Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *Foundations of Computer Science (FOCS) 2011*, pages 97–106. IEEE, 2011.
10. R. Canetti, D. Dachman-Soled, V. Vaikuntanathan, and H. Wee. Efficient password authenticated key exchange via oblivious transfer. In *Public Key Cryptography*, pages 449–466. Springer, 2012.
11. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. *Advances in Cryptology–EUROCRYPT 2010*, pages 523–552, 2010.
12. W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.
13. A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama. Strongly secure authenticated key exchange from factoring, codes, and lattices. In *Public Key Cryptography*, pages 467–484. Springer, 2012.
14. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.
15. S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In *Proceedings of the 45th annual ACM symposium on Symposium on theory of computing*, pages 545–554. ACM, 2013.
16. J. Katz and V. Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In *Advances in Cryptology–ASIACRYPT 2009*, pages 636–652. Springer, 2009.
17. J. Katz and V. Vaikuntanathan. Round-optimal password-based authenticated key exchange. In *Theory of Cryptography*, pages 293–310. Springer, 2011.
18. R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In *CT-RSA*, pages 319–339, 2011.
19. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT*, pages 1–23, 2010.
20. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.
21. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93. ACM, 2005.
22. D. Stehlé and R. Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In *EUROCRYPT*, pages 27–47, 2011.