New cryptographic constructions using generalized LWE

Jintai Ding

No Institute Given

Abstract. We present first a generalized LWE problem, which is essentially to extend the original LWE to the case of matrices. Then we use this new version of LWE problem, which we call matrix LWE problem to build new cryptographic schemes, which include a new key distribution scheme, a new key exchanges scheme and a new simple identity-based encryption scheme.

1 Introduction

The Learning with Errors (LWE) problem, introduced by Regev in 2005 [4], and its extension, Ring Learning with Errors (RLWE) problem have attracted a lot of attentions in theory and applications due to its usage in cryptographic constructions with some good provable secure properties. The main claim is that they are as hard as certain worst-case lattice problems and hence the related cryptographic constructions. Recently they have been used to construct homomorphic encryption schemes [9].

LWE problem can be described as follows.

First, we have a parameter n, a prime modulus q , and an "error" probability distribution κ on the finite field F_q with q elements.

Definition 1. *Let $\Pi_{S,\kappa}$ on F_q be the probability distribution obtained by selecting an element A in F_q^n randomly and uniformly, choosing $e \in F_q$ according to κ, and outputting $(A, < A, S > +e)$, where + is the addition that is performed in F_q.*

An algorithm that solves LWE with modulus q and error distribution κ, if, for any S in F_q^n , with an arbitrary number of independent samples from $\Pi_{S,\kappa}$, it outputs S (with high probability).

To achieve the provable security of the related cryptographic applications of the LWE problem, once choose q to be specific polynomial functions of n, namely q is replaced by a polynomial functions of n, which we will denote as $q(n)$ and κ to be certain discrete version of normal distribution with the standard deviation $\sigma = \alpha q \geq \sqrt{n}$.

In the original encryption scheme based on the LWE problem, one can only encrypt one bit a time and therefore the system is rather inefficient and it has a large key size. To further improve the efficiency of the cryptosystems based on the LWE problem, a new problem, which is a LWE problem based on a quotient ring of the polynomial ring $F_q[x]$ [6], was proposed. This is called the ring LWE (RLWE) problem. The RLWE problem is further used in homomorphic encryption schemes. In the cryptosystems based the RLWE problem, their security is reduced to hard problems on a subclass of ideal lattices instead of general lattices. One then may ask, is it possible to reformulate the problem such that the security is still based on general lattices instead of ideal lattices but with still good efficiency. This is the original motivation of this work.

1.1 Our contribution

We first reformulate a matrix version of LWE problem and build a similar encryption scheme, which is much more efficient in terms of computation per bit encrypted.

Then we use this new version of LWE problem, which we call matrix LWE problem to build new cryptographic schemes, which include a new key distribution scheme, a new key exchanges scheme and a new simple identity-based encryption scheme.

1.2 Matrix version of LWE and an new encryption scheme

Again, we assume that F_q is represented by integers between $-(q-1)/2$ and $(q-1)/2$.

We propose a new matrix version of LWE, which is based on the LWE. We propose to replace A, a vector in the original LWE problem, with a matrix A of size $m \times n$, and S also with a matrix of size $n \times l$, such that they are compatible to do matrix multiplication $A \times S$ (or $S \times A$). We also replace e with a compatible matrix of size $m \times l$. We will work on the same finite field with q elements.

To simplify the exposition, we will in this paper only present in details the case where A and S are both square matrices of the same size $n \times n$. But they do not have to be. A and S are randomly chosen to follow uniform distribution.

Definition 2. *Let $\Pi_{S,\kappa}$ over F_q be the probability distribution obtained by selecting an $n \times n$ matrix A, whose each entry are selected in F_q^n randomly, independently, and uniformly, choosing e as a $n \times n$ matrix over F_q according to an error distribution κ, and outputting $(A, A \times S + e)$, where $+$ is the addition that is performed in F_q.*

An algorithm that solves matrix LWE with modulus q and error distribution κ, if, for any S in $F_q^{n\times n}$, with one (or arbitrary number of) independent sample(s) from $\Pi_{S,\kappa}$, it outputs S (with high probability).

Remark 3. RLWE can be viewed as a special case of MLWE, since there is nutural embedding of the ring $F_q[x]/x^n + 1$ into the ring of $n \times n$ matrices.

We also know that if one can solve RLWE with small secret namely the elements s small, then one can solve it with uniform secret [7]. We will then use the MLWE with a small secret to build our cryptosystem.

To build an encryption scheme, we choose $q \approx n^3$, we choose again κ to be a distribution such that each component are independent, and each component follow the same discrete distribution as in the case of LWE, namely a discrete normal distribution over F_q center around 0 with standard deviation approximately $\sqrt{n}$.

With such a setting, we can build an encryption scheme as in the case of RLWE.

- We select an $n \times n$ matrix S, whose each entry is selected in the elements of $\{-t, ..., 0, ..., t\}$ of F_q^n randomly, independently, and uniformly, where t is small.
- In the setting of MLWE, we will output A and
$$E = A \times S + e,$$
which are the **public key** of our encryption scheme.
- A message m in represented as nxn matrix with binary entries of $0, 1$.
- a sender chooses a $n \times n$ matrix B like S, namely whose each entry is selected in the elements of $\{-t', ..., 0, ..., t'\}$ of F_q^n randomly, independently, and uniformly with t' small , and the message is encrypted as
$$(B \times A + e_1, B \times E + e_2 + m(q/2)),$$
where e_1 and e_2 are error matrices following the same distribution as e.
- To decrypt, one computes
$$(BE + e_2 + m(q/2) - (BA + e_1)S),$$
here everything is done in F_q. Then we divide them by $q/2$ performed as a real number division and round them to 0 or 1, which gives us the plaintext m.

The reason we could decrypt is that:

$$\begin{aligned} BE + e_2 + m(q/2) - BAS &= B \times (A \times S + e) + e_2 + m(q/2) - (BA + e_1) \times S \\ &= B \times e + e_2 + -e_1 \times S + m(q/2) \end{aligned}$$

$B \times e + e_2 + -e_1 \times S$ can be viewed as a error terms, which is determined by the distribution of the following randomly variable:

$$\sum_1^n a_1 x_i + x + \sum_1^n b_i y_i,$$

where a_i has a uniform distribution from $-t', -t' + 1, ..., 0, 1, ..., t'.$, b_i has a uniform distribution from $-t, -t+1, ..., 0, 1, ..., t$, and x_i, x and y_i has a distribution over with standard deviation $\sqrt{n}$. Therefore, this random variable is much more concentrated around zero that the normal distribution with standard deviation

$\sqrt{t'^2n^2 + n + t^2n^2}$. If $t', t << n$, the decryption process will surely return the right answer.

On key point of this new method is that on average, we can do the encryption much faster in terms of per bit speed because we can use fast matrix multiplication to speed up the computation process.

We can also use the same idea in Ring-LWE (RLWE) [6] to do encryption, where we have

$$E = A \times S + te,$$

t is small positive integer and the entries of S is also small.

We encrypt a message as

$$(BA + te_1, BE + te_2 + m).$$

Then we decrypt by computing

$$(BE + te_2 + m - B(AS + te_1))(mod \ \ t).$$

This works because

$$\begin{aligned} BE + te_2 + m - (BA + t_1e_1)S &= B \times (A \times S + te) + te_2 + m - (BA + te_1) \times S \\ &= tB \times e + te_2 + -te_1 \times S + m \end{aligned}$$

Remark 4. For the MLWE problem, we surely need to choose the distribution more carefully when we need to obtain the provable security of the scheme.

1.3 MLWE for scalable key distribution

Over a large network, key distribution among the legitimate users is a critical problem. Often, in the key distribution protocols, a difficult problem is how to construct a protocol, which is truly efficient and scalable. For example, in the case of the constructions of [1], large number of user can collaborate to drive the master key and break the system. Here we will build a truly scalable key distribution system with a trusted central server.

We work again over the finite field F_q, whose elements are represented by $-(q-1)/2, ..., 0, ..., (q-1)/2$. We choose $q \approx n^3$, we choose again κ to be an error distribution for a random such that each component are independent, and each component follow the same discrete distribution as in the case of LWE, namely a discrete normal distribution over F_q center around 0 with standard deviation approximately $\sqrt{n}$.

We have a central server, which will select a symmetric randomly chosen matrix S as a master key, whose entries are in F_q.

For each user, its ID is given as a symmetric matrix A_i and the index i with small entries, namely entries are chosen from the elements $-t', ..., 0, ..., t'$, where t' is small.

For each user, the central server distribute securely a secret:

$$E_i = A_iS + te_i,$$

where e_i is a matrix (not symmetric) selected following the error distribution.

To obtain the unique key shared between the $i-th$ user and the j-th user, where we assume that $i < j$, the $j-th$ user computes

$$E_i \times A_j = A_i S A_j + t e_i A_j,$$

and the $i-th$ user computes

$$(E_j \times A_i)^t = (A_j S A_i)^t + t(e_j A_i)^6.$$

Because A_i, A_j and S symmetric, we have that

$$A_i S A_j = (A_j S A_i)^t,$$

the $i-th$ user derives

$$A_i S A_j + t e_j^t A_i$$

But $e_i A_j$ and $e_j A_i$ are both small since t, t' e_i, e_j, A_i and A_j are all small. This allows us to get a common key for i and j by certain rounding techniques and therefore build a key distribution algorithm.

Here, we will propose the following simple rounding method.

Each user will collect all the entries that are in the range of $(-(q-1)/4, (q-1)/4)$. Each will publish the list of the positions of the entries that are selected. Then each will choose the intersection of the two sets to be the set selected and will compute the residue of the nonzero entries modular t. That will be the shared key between these two users.

Here, we can also choose e_i, e_j, A_i and A_j be vectors and using transposes. In this case, we will each time get one common number at most.

Also we can build a version with none symmetric matrices, in this case, the central serve needs to compute more matrices like $A_i S + e$ and $A_i^t S + e$. Then it is possible, we can do the same kind of key distribution.

On the other hand the RLWE problem can be viewed as a specialized commutative version of matrix-based LWE since an element in the ring can be view as a homomorphism on the ring. We can use RLWE to build a key distribution in the same way.

why scalable

why secure

1.4 A new key exchange protocol

The idea above can be easily adapted into a key-exchange protocol like the Diffie-Hellmann key exchange protocol.

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

Alice and Bob will first select a random and symmetric $n \times n$ matrix S over F_q, where $q \approx n^3$ and the error distribution κ to be a distribution such that each component are independent, and each component follow the same discrete distribution as in the case of LWE, namely a discrete normal distribution over F_q center around 0 with standard deviation approximately $\sqrt{n}$.

Then each party chooses its own secret E_i a $n \times n$ symmetric matrix with randomly chosen entry of small entries namely entries are chosen from the elements $-t', ..., 0, ..., t'$, where t' is small, and e_i following the error distribution κ, for i=A,B.

Then each pary computes

$$M_i = E_i S + e_i.$$

Then both parties exchange M_i, but certainly keep E_i and e_i secret.

Alice computes:

$$K_A = M_B E_A = E_B S E_A + e_B E_A.$$

Then Bob computes:

$$K_B = E_B \times M_A^t = E_B S E_A + E_B e_1.$$

Since e_i and E_i are small, K_A and K_A are close, we can derive from them a shared secret to be the exchanged key as in the case of above.

Security analysis

1.5 Identity-based encryption

There are several versions of identity-based encryption schemes. But they all look rather complicated. What we realize is that if we select the matrix to be commutative, then we can easily build a identity-based encryption scheme. In this case, we will realize that the structure will be very similar to the case of ideal lattice. Therefore,in stead, we will use RLWE to build a simple Identity-based encryption scheme.

We will need first choose parameter properly n, q and κ properly for the RLWE problem in order to build an simple and efficient identity-based encryption scheme easily using similar idea as above.

This constructions is also based on the encryption scheme of RLWE [6], namely, we assume that we have a ring with a porperly defined learning with error problem, where A and

$$E = A \times S + e,$$

, e is the error element following the distribution of κ, are given and the problem is to find the secret S.

We also know that can build a public key encryption systems, where A (small) and E serve as the public key, and the secret S serves as the private key.

To build a identity-based encryption scheme, the central server will first select a secret S in R as the master key controlled by a central server, where S is randomly chosen following uniform distribution.

The central server will also select a random M in R following uniform distribution and make sure that M has an inverse. if not, we will try again till we find one. Then the central serve will computer

$$M_1 = MS + e,$$

where e follows the error distribution κ.

Then the central server will publicize M and M_1 as the master public key.

For each user, the central server will assign an ID as I_i, where I_i should be in the form of a randomly chosen small elements in S.

Each member is given a secret key:

$$S_i = SI_i + M^{-1}e_i,$$

where e_i follows the error distribution κ.

Anyone can use the ID namely I_i and the master public key to build the public key

$$A_i = MI_i$$

and

$$B_i = I_iM_1 = I_iMS + I_ie = MSI_i + I_ie,$$

as the public key to encrypt a message.

Since I_i and e is small, we have I_ie is small.

Now we have that

$$S_iM - B_i = S_iM - B_i = MSI_i + MM^{-1}e_i - MSI_i + I_ie = e - I_ie_i,$$

which is small.

Therefore S_i is a solution to a ring LWE, where S_i is a secret key. There it can be use to decrypt a message.

This therefore gives an identity based encryption scheme.

Here we used very much the fact that in ring-LWE that the multiplication is commutative.

References

1. Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, Moti Yung: Perfectly-Secure Key Distribution for Dynamic Conferences. CRYPTO 1992: 471-486
2. A. Blum, A. Kalai, and H. Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM, 50(4):506519, 2003.
3. Johannes Buchmann, Daniel Cabarcas, Jintai Ding, Mohamed Saied Emam Mohamed: Flexible Partial Enlargement to Accelerate Grbner Basis Computation over F2. AFRICACRYPT 2010: 69-81
4. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 56(6):34, 2009. Preliminary version in STOC05.
5. Oded Regev, The Learning with Errors Problem (Invited Survey), CCC, pp.191-204, 2010 25th Annual IEEE Conference on Computational Complexity, 2010
6. Vadim Lyubashevsky, Chris Peikert, Oded Regev, On ideal lattices and learning with errors over rings In Eurocrypt 2010
7. Kristin Lauter and Michael Naehrig and Vinod Vaikuntanathan, Can Homomorphic Encryption be Practical?, Cryptology ePrint Archive, Report 2011/405, 2011, http://eprint.iacr.org,

8. Zvika Brakerski, Vinod Vaikuntanathan, Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011: 505-524, LNCS, Springer, 2011
9. Zvika Brakerski, Vinod Vaikuntanathan, Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106