Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 398-403
doi:10.4028/www.scientific.net/AEF.6-7.398

A Latticed-based Public Key Encryption with KDM Security from R-LWE

Wu Yan Fang[1, 2, a], Huang Zheng[1], Wen Qiao Yan[2]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

[2] Dept. of School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

[a]wuyanfnaghaoting@163.com

Keywords: lattice-based cryptography, key-dependent message security, R-LWE

Abstract. Since the introduction of the ring learning with errors (R-LWE) by Lyubashevsky, Peikert and Regev, many efficient and secure applications were founded in cryptography. In this paper, we mainly present an efficient public-key encryption scheme based on the R-LWE assumption. It is very simple to describe and analyze. As well as it can achieve security against certain key-dependent message (KDM) attacks. Namely, this efficient encryption scheme can securely encrypt its own secret key. The security of this scheme follows from the already proven hardness of the R-LWE problem since the R-LWE assumption is reducible to worst-case problems on the ideal lattice. Besides, the scheme enjoys a high level efficiency and low cost since the operations of the scheme are very simple and fast. The cost of both the encryption and decryption is only polylog(n) bit per message symbol.

Introduction

The well-studied learning with errors (LWE) problem was introduced by Regev [1], which has proved that there is a quantum reduction from the worst-case lattice problem to it. Peikert subsequently showed that hardness of LWE under certain lattice assumption through a classical reduction [2] (γ-SVP to LWE). Furthermore, the LWE assumption is sufficiently flexible to allow for the design of cryptographic constructions. Many interesting cryptographic applications have been founded based on it in the last years ([1, 2, 3, 4, 5, 6]).

The LWE problem can be described as the task of recovering the secret element from the linear equations with certain errors. Informally, for a dimension n and a prime q, given many pairs of the form $\left(\mathrm{a}_i, b_i \approx \langle \mathrm{a}_i, \mathrm{s} \rangle\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathrm{a}_i \in \mathbb{Z}_q^n$ is uniform and independent element, $\mathrm{s} \in \mathbb{Z}_q^n$ is uniformly random secret and the inner product $\langle \mathrm{a}_i, \mathrm{s} \rangle \in \mathbb{Z}_q$ is perturbed by a random error term chosen from certain error distribution, the goal of the LWE problem is to recover the secret s from the equations.

However, the main drawback of the schemes based on LWE is that they are not efficient enough for practical applications since the key typically contains a random matrix defined over $\mathbb{Z}_q$ for a small q .So the space and time requirements seem bound to be at least quadratic with respect to the security parameter n . To solve this problem, an algebraic variant of LWE, called the ring learning with errors (R-LWE), was presented in the independent concurrent work [7]. The R-LWE assumption is analogue to LWE. Roughly speaking, given the noisy equations are of the form $\left(a,\ b = a \cdot s + e\right) \in R_q \times R_q$, where $a \in R_q$ is uniformly random and the product $a \cdot s$ is perturbed by some random error term, chosen from an error distribution χ , the goal is to recover the secret s from the equations. The R-LWE assumption has very strong hardness guarantees [7]. For the features of the R-LWE problem, the applications based on it are more efficient and practical, compared with ones based on LWE assumption.

Besides, the most basic task in cryptography is construct secure encryption. Many definitions of security for encryption are under the assumption that the message to be encrypted should not dependent on the secret key. However, some situations need the message depending on the secret key.

So the definition of key dependent message security was introduced by Black, Rogaway and Shrimpton [8]. KDM secure encryption is a new area which has attracted much research in recent years ([9], [10], [11], [12], [13], [14]). An example of the KDM encryption allows the adversary to obtain the ciphertexts of the message dependent on the secret keys.

Our Results and Techniques. In this paper, to motivate the efficiency as well as the security of a scheme, we mainly construct a public-key encryption scheme based on the $\text{R-LWE}_{\text{t}}^{\times}$ assumption, which is a variant of the R-LWE assumption. It is efficient and enjoys the KDM security. The construction and security proofs are simple and natural since many applications of the LWE problem can be made much more efficient through the use of the R-LWE problem. This contribution is mainly inspired by the ideas from the work of Applebaum, Cash, Peikert and Sahai [10] based on the LWE problem. The proof of the security is the also similar to it.

The $\text{R-LWE}_{\text{t}}^{\times}$ assumption is obtained by applying the invertible techniques and the scaling the noise techniques, introduced in [15] and [9] respectively. It remains hard after the subtle modification. Due to the work [15], an important observation is that the R-LWE assumption is still hard even when $A_{s,\chi}$ and $U\left(R_q \times R_q\right)$ are respectively by $A_{s,\chi}^{\times}$ and $U\left(R_q^{\times} \times R_q\right)$, where $A_{s,\chi}^{\times}$ is obtained by sampling the pair $\left(a,\ a\cdot s+e\right)$ with $\left(a,\ e\right) \leftarrow U\left(R_q^{\times}\right) \times \chi$ and $R_q^{\times}$ is the set of invertible elements of R_q. Meantime, we apply the scaling the noise techniques in [9] to the assumption to get the $\text{R-LWE}_{\text{t}}^{\times}$ assumption our scheme based on. Roughly speaking, given noisy equations in the form of $\left(a,\ b=a\cdot s+t\cdot e\right) \in R_q^{\times} \times R_q$ with $\left(a,\ e\right) \leftarrow U\left(R_q^{\times}\right) \times \chi$ and $t \in \mathbb{Z}_q^*$, the goal is still to recover the secure s from the equations. As shown in [9], the additional factor of $t \in \mathbb{Z}_q^*$ is not a problem because of the virtue of $t \in \mathbb{Z}_q^*$ and q being relatively prime.

In order to make our scheme provide security for KDM, we generate the secret key s in the noise distribution instead of the uniform one over R_q. This modification does not affect the security of the scheme. We will discuss it in the following section.

Preliminaries

Natations. Throughout the paper, we use n for the security parameter. Other parameters are functions of n. Let $\mathcal{D}$ denote a distribution over some set S. $d \leftarrow \mathcal{D}$ is used to denote that d is chosen from the distribution $\mathcal{D}$. Define $d \leftarrow U(S)$ that d is chosen from the uniform distribution over a finite S. Let the distribution $D_{\mathbb{Z}^n,r}$ denote n dimensional discrete Gaussian distribution. $\mathbb{Z}[x]$ denote the ring of polynomials over the integers. The ring $\mathbb{Z}[x]/\langle f(x)\rangle$ is the ring of all integer polynomials modulo $f\left(x\right)$, where $f\left(x\right)=x^n+1$ is a polynomial of degree n .Analogously, $\mathbb{Z}_q[x]/\langle f(x)\rangle$ denote the ring of all integer polynomials modulo both $f(x)$ and q. In our work, we define a ring as $R_q=\mathbb{Z}_q[x]/\langle f(x)\rangle$.

Lattice. Let $\text{B}=\{b_1,b_2,\ldots,b_n\} \subseteq \mathbb{R}^n$ consist of n linearly independent vectors. The n dimensional lattice Λ generated by the basis

$$\Lambda=\mathcal{L}\left(\text{B}\right)=\left\{\text{Bc}=\sum_{\text{i}=1}^{\text{n}} c_i : \text{c} \in \mathbb{Z}^n\right\}. \tag{1}$$

By mapping polynomials to the vectors of their coefficients, we can see that an ideal of a ring, (here the ring is $\mathbb{Z}[x]/\langle f(x)\rangle$), corresponds to a sub-lattice of $\mathbb{Z}^n$. So a lattice is an ideal lattice if there exists an ideal $I \subseteq R$, such that $I=\left\{a_0+a_1x+\cdots+a_{n-1}x^{n-1} :\ \text{a} \in \Lambda\right\}$.

The Gaussian distribution ($D_{\Lambda,r}$) on Λ with parameter r is proportional to $e^{-\pi\|x/r\|}$ to each point $x \in \Lambda$. The ith successive minimum $\lambda_i(\Lambda)$ is the smallest radius r such that Λ contains i linearly independent vectors of norm at most r.

There are several natural computational problems involving lattice. These problems play a fundamental role in various areas. The following standard worst-case problem is of interest. The parameter $\gamma(n)$ is the approximation factor.

The (approximate) shortest vector problem (γ-SVP): Given a basis of the lattice Λ, it is supposed to find the shortest non-zero vector $v \in \Lambda$ such that $\|v\| \le \gamma(n)\|w\|$ for all $w \in \Lambda \setminus \{0\}$ with respect to a fixed approximate factor $\gamma(n)$.

As shown in [16], this problem with a constant factor is NP-hard for all norms under randomized reductions. Using the famous best known LLL [17] algorithm, this problem with exponential (in the lattice dimension) approximate factor is solvable. The same problem restricted to the ideal lattice is called ISVP. Even though the ideal lattices have a special algebraic structure and is not consider being NP-hard, it is also believed that no algorithm is known to perform non-negligibly better for γ-ISVP than for γ-SVP.

The Variant of R-LWE. In this section, we describe the variant of the R-LWE assumption our scheme is based on and discuss its hardness. We called it $\text{R-LWE}_{\text{t}}^{\times}$.

Let n be a power of 2 and let q be a prime satisfying $q = 1 \bmod 2n$. Define a probability distribution χ over R_q. The distribution $A_{s,\chi}^{\times,t}$ is obtained by sampling the pair $(a,\ a \cdot s + t \cdot e) \in R_q^{\times} \times R_q$ with $(a,\ e) \leftarrow U(R_q^{\times}) \times \chi$ and $s \leftarrow U(R_q)$ and $t \in \mathbb{Z}_q^*$. Where $R_q^{\times}$ denote the set of invertible elements of R_q.

Definition 1: For an integer $q = q(n)$ and an error distribution χ, the problem $\text{R-LWE}_{\text{t}}^{\times}$ is defined as follows: given access to an oracle that produces samples in $R_q \times R_q$, distinguish whether the oracle outputs sample from the distribution $A_{s,\chi}^{\times,t}$ or the distribution $U(R_q \times R_q)$ with overwhelming advantage.

Due to the work [1] and [7], we can get the analogous hardness results for $\text{R-LWE}_{\text{t}}^{\times}$ since this problem also shares some nice properties of the standard LWE problem, most notably equivalence between the decision version and the search version, where the goal is to recover the secret s. Especially, there is a probability polynomial-time reduction from solving the $\text{R-LWE}_{\text{t}}^{\times}$ problem to distinguishing between $A_{s,\chi}^{\times,t}$ and $U(R_q \times R_q)$ with non-negligible advantage. So if the search problem is hard, the $\text{R-LWE}_{\text{t}}^{\times}$ distribution is pseudorandom.

Public Key Encryption

As described in instruction, the theory advances of the R-LWE make lattice-based cryptography truly efficient and practical. In this section, we present the formal description of our KDM secure public-key scheme based on the $\text{R-LWE}_{\text{t}}^{\times}$ problem described in the above section. We also give the detailed analysis, including the techniques used in the construction and the properties of the scheme.

The Construction of the Scheme. Let n denote the security parameter. Our scheme relies on appropriate parameters choices, including the prime integer $q = 1 \bmod 2n$ and a larger prime $t \in \mathbb{Z}_q^*$ such that $r \ll t$ to ensure all but negligible probability $s \in R_t$, a degree n polynomial $f(x) = x^n + 1 \in \mathbb{Z}[x]$ and the error distribution $\chi = D_{\mathbb{Z}^n,r}$ with $r \ge \omega(\sqrt{\log n})$. These parameters are public. There are polynomial-time algorithms which can output these parameters.

Key generation (1^n): Sample a ring element $s \leftarrow \chi$ and define s as the secret key. Then compute $b = a \cdot s + t \cdot e \in R_q$, where $a \leftarrow R_q, e \leftarrow \chi$ and define (a,b) as the public key. Return keys both $sk := s$ and $pk := (a,b)$.

Encryption (pk , m): To encrypt a message $m \in R_t$, given the public key (a,b), chose a sampler r from the error distribution χ, and then compute $c_1 = a \cdot \mathrm{r}$ and $c_2 = b \cdot \mathrm{r} + m$. Return the ciphertexts $c = (c_1, c_2)$.

Decryption (sk , c): Given the secret s and the ciphertexts c, compute $m = (c_2 - c_1 \cdot s) \bmod t$. Return the message m.

The correctness of the construction is apparent for

$$(c_2 - c_1 \cdot s) \bmod t = \left((a \cdot s + t \cdot e) \cdot \mathrm{r} + m - a \cdot \mathrm{r} \cdot s\right) \bmod t = m. \tag{2}$$

Note that the decryption of this scheme is complete without any decryption failures.

For technical reasons, in the formal construction the secret key s is chosen from the noise distribution χ rather than the uniform distribution $U(R_q)$ to achieve KDM security without any security loss. The security of the scheme remains from the hardness of the R-LWE$_t^{\times}$ assumption, actually from its Hermite normal form due to the following lemma.

Lemma: For $q = 1 \bmod 2n$ and arbitrary $s \in R_q$ and the error distribution χ, there is a deterministic polynomial-time transformation T, which maps $A_{s,\chi}^{\times,t}$ to $A_{s_1,\chi}^{\times,t}$ with $s_1 \leftarrow \chi$ and maps $U(R_q^{\times} \times R_q)$ to $U(R_q^{\times} \times R_q)$.

Proof: The transformation T is given access to distribution $\mathcal{D}$ over $R_q^{\times} \times R_q$. Here the distribution is $A_{s,\chi}^{\times,t}$ or $U(R_q^{\times} \times R_q)$. Next we prove it in two steps.

The first step is that the transformation T obtains a pair $(\overline{a},\ \overline{b}) \in R_q^{\times} \times R_q$ by drawing from the distribution $\mathcal{D}$. When the distribution $\mathcal{D}$ is $A_{s,\chi}^{\times,t}$, the pair $(\overline{a},\ \overline{b})$ satisfies $\overline{b} = \overline{a} \cdot s + t \cdot s'$, where s' is chosen from χ.

The second step is to transform samples from $\mathcal{D}$ into ones form a different distribution. For a sample $(\overline{a}, \overline{b})$, the transformation T will turn it to be $(a', b') \in R_q^{\times} \times R_q$ by computing $a' = -\overline{a}^{-1} \cdot a$ and $b' = b + a' \cdot \overline{b}$.

We can note that $a' \in R_q^{\times}$ is uniform because $\overline{a} \in R_q^{\times}$ is invertible modulo q and $a \in R_q^{\times}$ is uniform. On the one hand, if $\mathcal{D}$ is the distribution $U(R_q^{\times} \times R_q)$, then $(a', b') \in R_q^{\times} \times R_q$ is also a sample from $U(R_q^{\times} \times R_q)$. On the other hand, if $\mathcal{D} = A_{s,\chi}^{\times,t}$, then $b = a \cdot s + t \cdot e \in R_q$ with $(a,e) \leftarrow U(R_q^{\times}) \times \chi$. Therefore, we get $b' = b + a' \cdot \overline{b} = a \cdot t \cdot s' + t \cdot e = a \cdot s_1 + t \cdot e$, where $s_1 = t \cdot s'$. We can see (a', b') is from the distribution $A_{s_1,\chi}^{\times,t}$ as desired.

The Pseudorandomness and Efficiency. As shown in [7], the R-LWE$_t^{\times}$ problem has two classical features, efficiency and pseudorandomness. That is, our scheme can be efficiently generated by "cheap" operation such as modular addition and multiplication. Compared with some schemes based on the traditional problems or the LWE problem, our scheme can achieve the same security at lower overhead. In this scheme, the cost of both the encryption and decryption is only polylog(n) bit per message symbol. So this scheme is obviously more efficient than ones ([10], [11]) based on the LWE problem and the DDH problem respectively. This result stems from the fact an element in the ring can encode n samples from $\mathbb{Z}_q$. So the overhead in this scheme can be reduced by a factor of

approximating n . As well as our scheme enjoys the properties of low complexity and pseudorandomness. We can observe that all the size of the keys and ciphertexts is $O(n \log n)$. And they actually are the R-LWE instances. So they are all pseudorandom. If the adversary is forced to work without the knowledge of any signed message, key recovery from the public information (such as the public key and the ciphertexts in this scheme) is equivalent to solve the R-LWE problem.

The Security of the Scheme. The features of the KDM security in our scheme are similar to the work [10]. Namely, this scheme can securely encrypt any liner function of secret key. Consider the ciphertext $c_2 = b \cdot \mathrm{r} + s = (a \cdot \mathrm{r} + 1) + t \cdot e\mathrm{r}$, which is the encryption of the secret key $s \in R_q$. We can define $a_1 = a \cdot \mathrm{r} + 1$ and $e_1 = e \cdot \mathrm{r}$. Then the ciphertext $c = (a_1 - 1, a_1 \cdot s + t \cdot e_1)$ is also exactly an R-LWE instance, which is computationally indistinguishable from the uniform ones. This case can extend to any liner function of secret key. So we can get the following theorem. The proof is straightforward as well as the outline of the proof is analogous to the methodology introduced in [10]. Here, it is omitted.

Theorem: For parameters mentioned in the formal construction, this scheme is KDM-secure under the R-LWE$_t^{\times}$ assumption.

Summary

We construct a public-key encryption based on the R-LWE$_t^{\times}$ problem, which is reducible to the worst-case problems on ideal lattice. So the scheme is simple and efficient. Besides, our scheme enjoys key dependent message security.

Acknowledgement

This work is supported by National Natural Science Foundation of China (Grant Nos. 61170270, 61100203, 60903152, 61003286, 61121061) and the Fundamental Research Funds for the Central Universities (Grant Nos.BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, 2011RCZJ15, and 2012RC0612).

References

[1] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: STOC, pp. 84–93 (2005).

[2] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem, in: STOC (2009).

[3] S. Agrawal, D. Boneh, and X. Boyen, Efficient lattice (H)IBE in the standard model, in: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010).

[4] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, Bonsai trees, or how to delegate a lattice basis, in: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010).

[5] C. Gentry, C. Peikert and V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: Proc. of STOC, pp. 197–206. ACM, New York (2008).

[6] C. Peikert, B. Waters, Lossy trapdoor functions and their applications, in: STOC, pp. 187–196 (2008).

[7] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. in: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010).

[8] J. Black, P. Rogaway, T. Shrimpton, Encryption-scheme security in the presence of key-dependent messages, in: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 62–75. Springer, Heidelberg (2003).

[9] Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In Proc. of CRYPTO, volume 6841 of LNCS, pages 505–524. Springer, 2011.

[10] B. Applebaum, D. Cash , C. Peikert and A. Sahai, Fast cryptographic primitives and circular-secure encryption based on hard learning problems, in: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009).

[11] D. Boneh, S. Halevi , M. Hamburg, R. Ostrovsky, Circular-secure encryption from decision Diffie-Hellman, in: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008).

[12] T. Malkin, I. Teranishi, M. Yung, Efficient circuit-size independent public key encryption with kdm security. in: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 507–526. Springer, Heidelberg (2011).

[13] J. Camenisch, N. Chandran and V. Shoup, A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks, Cryptology ePrint Archive, Report 2008/375 (2008).

[14] D. Hofheinz, D. Unruh, Towards key-dependent message security in the standard model, in: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 108–126. Springer, Heidelberg (2008).

[15] D. Stehle, R. Steinfeld, Making NTRU as Secure as Worst-case Problems over Ideal Lattice, EUROCRYPT (2010). Berlin Heidelberg:Springer-Verlag, LNCS, 2011, 6630:27-47

[16] S. Khot, Hardness of approximating the shortest vector problem in lattices. J ACM 52(5):789–808 , 2005.

[17] A. Lenstra, H. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, Math Ann 261(4):515–534, 1982.