Multiplicative Learning with Errors and Cryptosystems

Gu Chunsheng
School of Computer Engineering
Jiangsu Teachers University of Technology
Changzhou, China, 213001
guchunsheng@gmail.com

Abstract: We introduce a new concept, called multiplicative learning with errors (MLWE), which is a corresponding multiplicative version of the additive learning with errors (LWE), and show the equivalence between the decisional version and the search version for MLWE such that p is a product of sufficiently large smoothing prime factors. Then we construct the MLWE-based private-key and public-key encryption schemes, whose securities are based on the worst-case hardness assumption of the MLWE problem. Finally, we discuss how to extend the LWE on additive group to the LWE on general abelian group.
Keywords: Multiplicative Learning with Errors, Private-Key Encryption, Public-key Encryption, LWE on Abelian Group.

1. Introduction

Since Diffie and Hellman introduce public-key cryptography, very few convincingly secure asymmetric public-key cryptosystems have been discovered despite considerable research efforts. Now standard cryptographic assumptions are mainly based on the polynomial hardness problems such as factoring, discrete logarithm or various lattice problems, respectively. Recently, Regev [Reg05] proposes a different class of cryptosystems based on learning with errors (LWE). The LWE problem is a generalization of the well-known 'learning parity with noise' problem to larger modulus. In the search version of LWE, the goal is to solve for an unknown vector s on Z_p^n which is often chosen uniformly at random, given any desired m=poly(n) independent 'noisy random inner products' $(a_i, b_i =< a_i, s > + e_i) \in Z_p^n \times Z_p$, $i \in [m]$, where $a_i \in Z_p^n$ and each e_i the error distribution X. In the decisional version, the goal is merely to distinguish between noisy inner products as described above and uniformly random samples from $Z_p^n \times Z_p$. Moreover, Regev presents an elementary reduction from the search version to decision version for the LWE problem when the modulus p is a prime and p=poly(n).

The multiplicative learning with error (MLWE) problem is a multiplicative version of the LWE problem. It is parameterized by a dimension n, a modulus p, and an error distribution X over Z_p, where X is often considered as a Gaussian-like distribution that is relatively concentrated around 0. In the search version of MLWE, the goal is to solve for an unknown

vector *s* on some subset of Z_p^n which is often chosen uniformly at random, given any desired *m*=poly(*n*) independent 'noisy random exponential inner products' $(a_i, b_i = (a_i \wedge^r s) \times e_i = \prod_{j=1}^n a_{i,j}^{s_j} \times e_i \in Z_{p^*}^n \times Z_{p^*}$, $i \in [m]$,where $a_i \in Z_{p^*}^n$, e_i the error distribution *X*. In the decisional version, the goal is to distinguish between noisy random exponential inner products and uniformly random samples from $Z_{p^*}^n \times Z_{p^*}$.

Our main contribution in this paper is to generalize the LWE problem defined on additive group to the LWE on general abelian group, and construct the new private/public key cryptosystems when there is a norm on abelian group. To demonstrate this extension, we firstly introduce the multiplicative learning with error (MLWE), which is defined on the multiplicative group modulus *p,* and construct the MLWE-based private/public key cryptosystems. We then discuss how to extend the LWE on additive group to the LWE on general abelian group.

The organization of this paper is following: Section 2 introduces the related work, Section 3 gives the notational presentation and definitions, Section 4 proves the hardness of MLWE, Section 5 presents the private (public) key cryptosystem, and Section 6 discusses the LWE generalization on the abelian group.

2 Related Work

Since Regev presents the concept of LWE, many works (e.g. [KTX07], [PVW08], [AGV09], [PW08], [PVW08], [GPV08], [ACPS09], [Pei08a], [Pei09], [KS09], [KS09]) have focused on improving and designing various cryptographic primitive under the hardness of LWE.

Our work is inspired by [Reg05], but differs from it substantially in both the different problem and most of the details. Regev defines the additive learning with error, whereas we generalize LWE on the additive group to the LWE for general abelian group, and demonstrate this difference through the multiplicative learning with error. Moreover, based on the hardness of MLWE, we construct a private (public) key cryptosystem. To our knowledge, the leaning with error problem on the abelian group does not obtain the attention for researchers. We believe this contribution is of independently interest.

3. Preliminaries

Let $[p] = \{1, 2, ..., p\}$, $-[p] = \{-1, -2, ..., -p\}$, $Z_p = \{\lceil -p/2 \rceil, ..., \lfloor (p-1)/2 \rfloor\}$, $Z_{p^*} = \{a \mid \gcd(a, p) = 1, and\ a \in Z_p\}$. Let $x, y \in Z^n$ be two column vectors, define $x^c = (x_1^c, ..., x_n^c)$, $x / c = (x_1 / c, ..., x_n / c)$, $x \oplus y = (x_1 \oplus y_1, ..., x_n \oplus y_n)$, and $x * y^{-1} = (x_1 \times y_1^{-1}, ..., x_n \times y_n^{-1})$, where c is a non-zero constant.

Assume $X, Y \in Z_p^{m \times n}$, $X \wedge^r Y^T = (a_{i,j})$ where $a_{i,j} = \prod_{k=1}^n x_{i,k}^{y_{j,k}}$. $X \wedge^l Y^T = (a_{i,j})$

where $a_{i,j} = \prod_{k=1}^{n} y_{j,k}^{x_{i,k}}$. $X * Y = (a_{i,j})$ where $a_{i,j} = x_{i,j} y_{i,j}$. $Y^{-1} = (a_{i,j})$ where $a_{i,j} = y_{i,j}^{-1}$. $kX + c = (a_{i,j})$ where $a_{i,j} = kx_{i,j} + c$. $g^X = (a_{i,j})$ where $a_{i,j} = g^{x_{i,j}}$.

Let $\lambda(p)$ be the Carmichael's λ-function for p, $\varphi(p)$ be Euler's φ-function for p.

Definition 2.1 (Learning With Error LWE$_{p,s,X}$ [Reg05]). Suppose $n > 1$, p be a positive integer and consider a list of equations with errors $< a_i, s > + e_i = b_i (\mathrm{mod}\ p)$, $i \in [m]$, $m \le poly(n)$ where a_i, s are chosen independently from the uniform distribution on Z_p^n, e_i is independently drawn from the error distribution X and $b_i \in Z_p$. Let LWE$_{p,s,X}$ denote the problem of recovering s from such equations, A$_{p,s,X}$ the probability distribution generated by LWE$_{p,s,X}$.

Definition 2.2 (**Multiplicative Learning With Error MLWE$_{p,s,X}$**). Assume n, m, p be positive integers, $a_i, i \in [m]$ are chosen independently from the uniform distribution on $Z_{p^*}^n$, s is chosen independently from the uniform distribution on $Z_{\varphi(p)}^n$, $b_i = (a_i \wedge^r s) \times e_i \mod p$, where each e_i is independently drawn from the error distribution X on Z_p. Let MLWE$_{p,s,X}$ denote the problem of recovering s from such equations with errors, MA$_{p,s,X}$ the probability distribution generated by MLWE$_{p,s,X}$.

Remark: We notice this problem is not equivalent to LWE$_{p,s,X}$. For example, let $p = 29$, A, s, e, b be an input instance for MLWE$_{p,s,X}$, A_1, e_1, b_1 be the discrete logarithm $\log_2$ of A, e, b. It is easy to see that the error distribution e_1 on $Z_{\varphi(p)}$ is different from the one of e on Z_p.

$$A = \begin{pmatrix} 3 & 7 & 4 & 11 \\ 6 & 9 & 17 & 24 \\ 5 & 26 & 20 & 18 \\ 16 & 3 & 2 & 13 \end{pmatrix}, \quad s = \begin{pmatrix} 5 \\ 10 \\ 23 \\ 11 \end{pmatrix}, \quad e = \begin{pmatrix} 3 \\ 2 \\ -1 \\ 5 \end{pmatrix}, \quad b = (A \wedge^r s) * e = \begin{pmatrix} 10 \\ 4 \\ 12 \\ 3 \end{pmatrix} \mod 29,$$

$$A_1 = \log_2 A = \begin{pmatrix} 5 & 12 & 2 & 25 \\ 6 & 10 & 21 & 8 \\ 22 & 19 & 24 & 11 \\ 4 & 5 & 1 & 18 \end{pmatrix}, e_1 = \log_2 e = \begin{pmatrix} 5 \\ 1 \\ 14 \\ 22 \end{pmatrix}, b_1 = A_1 s + e_1 = \begin{pmatrix} 23 \\ 2 \\ 7 \\ 5 \end{pmatrix} \mod 28.$$

4. Hardness of MLWE

Theorem 4.1 Let $n>1$ be an integer, $p=p_1...p_t$ for distinct primes $p_i=poly(n)$. There is a probabilistic polynomial time reduction from solving the search $MLWE_{p,s,X}$ problem with overwhelming probability to distinguishing $MA_{p,s,X,e}$ from $U(Z_{p^*}^n \times Z_{p^*})$ for arbitrary $s \in Z_{\lambda(p)}^n$ with overwhelming probability.

Proof: This Lemma is similar to Lemma 3.6 of [Pei09]. But the method of proof is different from the one of [Pei09], since $\lambda(p_i)=p_i-1$ is not prime. Assume D to be an efficient distinguisher that distinguishes $MA_{p,s,X}$ from U for modulus p_1. Given input samples $(a_i, b_i = a_i \wedge^r s \times e_i), i \in [m]$ generated by the distribution $MA_{p,s,X}$. The goal is to solve s from (a_i, b_i). Due to $p_1=poly(n)$, we can compute the order of $a_{i,j}$. Without loss of generality, let the order of $a_{i,j}$ be p_1-1. Firstly, choose m random $r_i \in Z_{p_1-1}$, and for any $k \in Z_{p_1-1}$, factor $k=xy \bmod(p_1-1)$ such that $x \neq 1, y \neq 1$ and $\gcd(y, p_1-1)=1$ except with $k=0 \bmod(p_1-1)$. Then, compute $a_{i,1}^{'}=a_{i,1}^{x+r_i}$, $a_{i,j}^{'}=a_{i,j}$, $j>1$, $b_i^{'}=b_i \times a_{i,1}^{r_i y}$. Finally, call D with the parameters $(a_i^{'}, b_i^{'})$. If $D((a_i^{'}, b_i^{'}))=1$, then $s_1=k$, otherwise $s_1 \neq k$. If $s_1=xy$, then $s_1+r_i y=(x+r_i)y$, namely $(a_i^{'}, b_i^{'}) \in MA_{p_1,s,X}$. If $s_1 \neq xy$, the probability that $(s_1+r_i y)/(x+r_i)=(s_1+r_j y)/(x+r_j)$ is at most $1-1/(6\ln\ln(p_1-1))+1/(p_1-1)$. When $(s_1-xy)(r_i-r_j)=0 \bmod(p_1-1)$, $s_1 \neq xy$, and $r_i \neq r_j$, the probability of $\gcd(r_i-r_j, p_1-1)>1$ is at most $1-1/(6\ln\ln(p_1-1))$. Moreover, the probability of $r_i=r_j$ is $1/(p_1-1)$. So, the probability that $(s_1+r_i y)/(x+r_i)=(s_1+r_j y)/(x+r_j)$ and $s_1 \neq xy$ for all (r_i, r_j) is at most $(1-1/(6\ln\ln(p_1-1))+1/(p_1-1))^{m-1}$ and negligible. In other words, if $s_1 \neq xy$, there does not exist an integer z such that $z=(s_1+r_i y)/(x+r_i) \bmod(p_1-1)$ for all i with overwhelming probability. In this case, $b_i^{'}$ is uniformly random by applying the fact the

order of $a_{i,1}$ is $p_1 - 1$ and $\gcd(y, p_1 - 1) = 1$, namely, $r_i^{'} = r_i y \in U(Z_{p_1-1})$. Hence, we can decide whether $k = s_1$ by using D and $1 \le s_1 \le p_1 - 1 = poly(n)$. If all $1 \le k < p_1 - 1$ is not equal to s_1, then $s_1 = 0 \bmod (p_1 - 1)$, for the input samples are from the distribution $MA_{p_1,s,X}$. So, we can add a random number to s_1, then decide s_1. Finding all other coordinates is similar for modulus p_1 and $p_2, ..., p_t$. Finally, we recover $s \in Z_{\lambda(p)}^n$ via the Chinese remainder theorem.■

Lemma 4.1 (Decisional Average-case to Worst-case). If there is a distinguisher that distinguishes $MA_{p,s,X}$ from U for a non-negligible fraction of all possible s, then there is an efficient algorithm that for all s accepts with probability exponentially close to 1 on inputs from $MA_{p,s,X}$ and rejects with probability exponentially close to 1 on inputs from U.

Lemma 4.2 (Search Average-case to Worst-case). If there exists an efficient algorithm that solves $MLWE_{p,s,X}$ for a non-negligible fraction of all possible s, then there exists an efficient algorithm that for all s solves $MLWE_{p,s,X}$ with probability exponentially close to 1.

Proof: The proofs of Lemma 4.1, 4.2 directly follow the adaptive one of Lemma 4.1 of [Reg05]. ■

5. Encryption Schemes

In this section, we present a private-key encryption scheme and a public-key encryption scheme based on the decisional MLWE problem, respectively. By using Theorem 3.1, we know their securities depend on the hardness of the MLWE problem.

5.1 Private-Key Encryption Scheme

Let n be the security parameter. $m = n^c$ where $c > 0$ is a constant, $p = poly(n)$ is a prime, $q = \lfloor \sqrt{p} \rfloor$.

Key Generation Algorithm: On input 1^n, choose a uniformly random secret key $s \in Z_p^n$.

Encryption Algorithm: On input a secret key $s \in Z_p^n$ and a message $y \in \{0,1\}^m$. Choose $A \in_R Z_{p^*}^{m \times n}$ uniformly at random and an error vector $e \in_R (-[q-1]) \cup [q-1]$ where $|e_i| \in [q-1]$, output the ciphertext $c = (A, (A^{\wedge r} s) * e * q^y \bmod p)$.

Decryption Algorithm: On input a secret key $s \in Z_p^n$ and a ciphertext $c = (A, b)$. The decryption algorithm computes $x = b * (A^{\wedge r} s)^{-1} \bmod p$ and it deciphers as follows: if

$-(q-1) \le x_i \le q-1$, then it deciphers $y_i = 0$, otherwise it deciphers $y_i = 1$.

Correctness: The decryption algorithm computes $x = b * (A^{\wedge r}\ s)^{-1} = e * q^y$. Thus, if $y_i = 0$, then $-(q-1) \le x_i \le q-1$. If $y_i = 1$, $q \le x_i = (e_i \times q) \bmod p \le p - q$. We here use the absolutely least residue for modulo p.

Efficiency. The size of ciphertext $c = (A, b)$ has $mn \lg p + m \lg p$ bits. The expansion of ciphertext is $(mn \lg p + m \lg p)/m = n \lg p + \lg p$ for each message bit.

Proposition 5.1 (Security). The symmetric encryption scheme is semantically secure assuming that the $\mathrm{MLWE}_{p,s,U}$ problem is hard.

5.2 Public-key Encryption Scheme

Let n be the security parameter. $m = 2n$, $p = p_1 \ldots p_t > 2^{4n \lg n + 12n}$ such that $p_i = poly(n)$ are distinct primes, $q = \lambda(p)$.

Key Generation: Select $A \in Z_{p^*}^{m \times n}$ uniformly at random, $S \in Z_q^{m \times n}$, $E \leftarrow U_{[s]}^{m \times m} \bigcup U_{-[s]}^{m \times m}$, where $s = \left\lfloor 8\sqrt{n} \right\rfloor$. Output the secret key $sk = (S)$, and the public key $pk = (A, B)$ where $B = (A^{\wedge r}\ S^T) * E * M \bmod p$, $M' = diag(m_1, m_2, \ldots, m_m)$, M is obtained by replacing all 0 entries in M' with 1, and $m_i = \left\lfloor p^{1/2} \right\rfloor, i \in [m]$.

Encryption: Take as input a public key $pk = (A, B)$ and a message $y \in \{0,1\}^m$. Choose a vector $x \in \{0,1\}^m$ uniformly at random and output the ciphertext $C = (C_1, C_2, C_3) = ((x^{\wedge l}\ A) \bmod p, (x^{\wedge l}\ B) \bmod p, x \oplus y)$.

Decryption: Take as input a secret key $sk = (S)$ and a ciphertext $C = (C_1, C_2, C_3)$. Compute $c = C_2 * (C_1^{\wedge r}\ S^T)^{-1}$, and output $x_i = 0$ if $|c_i| < p^{1/2}$ modulo p and $x_i = 1$ otherwise. Finally, decrypt the message $y = C_3 \oplus x$.

Correctness. Since $c = C_2 * (C_1^{\wedge r}\ S^T)^{-1} = (m_1^{x_1} \prod e_{i,1}^{x_i}, m_2^{x_2} \prod e_{i,2}^{x_i}, \ldots, m_m^{x_m} \prod e_{i,m}^{x_i}) \bmod p$, and $|\prod e_{i,j}^{x_i}| \le \prod (\sqrt{n} \times 8\sqrt{n}) = 2^{2n \lg n + 6n} < p^{1/2}$, $j \in [m]$. Thus, if $x_i = 0$, then

$|c_i| < p^{1/2}$, if $x_i = 1$, then $|c_i| \geq p^{1/2}$.

Efficiency. The size of public key $pk = (A, B)$ has $O(m^2 \lg p) = O(n^3 \lg n)$ bits. The size of secret key $sk = (S)$ is $O(mn \lg p) = O(n^2 \lg n)$ bits. The size of ciphertext $C = (C_1, C_2, C_3)$ is $O(m \lg p) = O(n^2 \lg n)$ bits. The expansion of ciphertext is $O(n^2 \lg n / n) = O(n \lg n)$ for each message bit.

Proposition 5.2 (Security). The public key encryption scheme is secure assuming that the $\text{MLWE}_{p,s,U}$ problem is hard when p is a product of sufficiently large smoothing prime factors.

6. Extension

In fact, the LWE is the additive group defined on Z_p^n, the MLWE is the multiplicative group defined on $Z_{p^*}^n$. So, we can easily generalize the LWE on additive group to the LWE on general abelian group. Assume that G is an abelian group, $\bullet$ operator of G. Then, the LWE on G is defined as follows: given any desired m=poly(n) independent 'noisy random inner products' $(a_i, b_i = \prod_{j=1}^{n} a_{i,j}^{s_j} \bullet e_i) \in G^n \times G$, $i \in [m]$, where $a_i \in G^n$ and each e_i the error distribution X on G, $a_{i,j}^{s_j} = a_{i,j} \bullet a_{i,j} \ldots \bullet a_{i,j}$, that is, $a_{i,j}$ operates s_j times. In the search version of LWE, the goal is to solve for an unknown vector s on G^n which is often chosen uniformly at random. In the decisional version, the goal is merely to distinguish between noisy inner products as described above and uniformly random samples from $G^n \times G$. It is easy to verify that the LWE on the abelian group can be used to construct the public key cryptosystem if there is a norm for the group elements in G. So, we believe that it is very interesting to study the hardness of LWE on the general abelian group.

References

[ACPS09] B. Applebaum, D. Cash, C. Peikert, A. Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In *CRYPTO 2009*: 595-618.

[AD97] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th Annual ACM Symp. on Theory of Computing (STOC)*, pages 284–293, 1997.

[AGV09] A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In *Proc. of 6th IACR Theory of Cryptography Conference (TCC)*, pages 474–495, 2009.

[AP09] J. Alwen and C. Peikert. Generating shorter bases for hard random lattices. In *STACS*,

pages 75–86, 2009.

[FGKRS09] D. Freeman, O. Goldreich, E. Kiltz, A. Rosen and G. Segev **.** More Constructions of Lossy and Correlation-Secure Trapdoor Functions**.** *Cryptology ePrint Archive:* Report 2009/590

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *STOC*, pages 25–32, 1989.

[GKPV10] Shafi Goldwasser, Yael Kalai, Chris Peikert and Vinod Vaikuntanathan. Robustness of the Learning with Errors Assumption. In *Proceedings of ICS '10 (Innovations in Computer Science)*, 2010.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. 40th ACM Symp. on Theory of Computing (STOC)*, pages 197–206, 2008.

[KS09] A. R. Klivans and A. A. Sherstov. Cryptographic hardness for learning intersections of halfspaces. *Journal of Computer and System Sciences*, 75(1):2–12, 2009.

[KTX07] A. Kawachi, K. Tanaka, and K. Xagawa. Multi-bit cryptosystems based on lattice problems. In *Public Key Cryptography – PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 315–329, Berlin, 2007. Springer.

[Pai99] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Advances in Cryptology - Eurocrypt '99*, *Lecture Notes in Computer Science* volume 1592, pages 223–238. Springer-Verlag, Berlin, 1999.

[Pei08a] C. Peikert. Limits on the hardness of lattice problems in *lp* norms. *Computational Complexity*, 17(2):300–351, 2008. Preliminary version in CCC'07.

[Pei08b] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *ECCC*, report No. 100, 2008.

[Pei09] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proc. 41st ACM Symp. on Theory of Computing (STOC)*, Pages 333-342, 2009.

[PVW08] C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *Advances in cryptology—CRYPTO '08*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, Berlin, 2008.

[PW08] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *Proc. 40th ACM Symp. on Theory of Computing (STOC)*, pages 187–196, 2008.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. 37th ACM Symp. on Theory of Computing (STOC)*, pages 84–93, 2005.

[RS09] Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. In TCC, pages 419–436, 2009.