Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 186 (2021) 309–315

Procedia Computer Science

www.elsevier.com/locate/procedia

14th International Symposium “Intelligent Systems”

Homomorphic Encryption within Lattice-Based Encryption System

Victor Kadykov[a], Alla Levina[a,*], Alexander Voznesensky[b]

[a]ITMO University, 49 Kronverkskiy Pr., St. Petersburg, Russia

[b]Saint Petersburg Electrotechnical University ”LETI”, St.Petersburg, 5 Professora Popova str., 197376, Russian Federation

Abstract

In 2009 a system of fully homomorphic encryption was constructed, in the future, many works were done based on it. In this work, will be performed an analysis of the possibility to use the ideal lattices for constructing homomorphic operations over ciphertexts.

This paper represents the analysis of an encryption system based on the primitive of a union in ideal lattices space. The advantage of this approach consists in the possibility of segregated analysis of encryption security and homomorphic properties of the system.

The work will be based on the method of analyzing generalized operations over ciphertext using the concept of the base reducing element. It will be shown that some encryption systems can be supplemented by homomorphism between opentext and ciphertext. Thus such systems can be decomposed by encryption and homomorphic parts which would affect each other but although can be analyzed separately. Different systems (probably within one class) can be represented via an identical transform of sets. Separated from the cryptographic scheme the underlying math can be used to analyze only the homomorphic part, particularly under some simplifications. The building of ideal-based ciphertext laying on the assumption that ideals can be extracted further, it will be shown in the paper what the ”remainder theorem” can be one of the principal ways to do this.

Keywords: Homomorphic encryption; Fully Homomorphic Encryption; NTRU; ideal lattices; ”remainder theorem”; information security.

1. Introduction

Starts from 1978 after privacy homomorphism [6] was discovered, obtaining a homomorphic encryption system becomes a necessary task. Much work had been done, but only 20s century related progress is having to draw the line in constructing Fully Homomorphic Encryption (FHE) scheme which happens in the year 2009 [3]. Construction of the scheme was performed with the use of ideal lattices. As it can be seen ideal primitive remains the main flow in the direction of FHE-schemes even for today’s [1]. Therefore it’s necessary to keep work on theory and assume that ideal lattices might be the only primitive where FHE is possible [8].

Before, in the period due to 2000, many security aspects were considered such as place of probabilistic property within the encryption system. Many works state that the deterministic system is breakable in polynomial time using computations in quantum architecture [2, 5, 9]. Therefore probabilistic and homomorphic property co-existing is at

* Corresponding author.
E-mail address: alla_levina@mail.ru

1877-0509
10.1016/j.procs.2021.04.149

must. This requirement raises one of the major flows in this work introducing the statement of base reducing element wich union both probabilistic and homomorphic properties within a lattice-based system.

Also, it can be assumed that ideal lattices will become perspective within modern (quantum) computations [1]. In such a case, NTRU-based systems are the most remarkable systems with the use of ideal lattices. Besides, the homomorphic properties of NTRU were discovered recently [7], and, prior to the first assumptions in this work, a more simple model of congruential encryption system [4] is used which underlies the construction of NTRU-based systems and uses ideal lattices as well.

Thus the paper covers the probabilistic part and ideal lattices in the base reducing element statement which is taken from the assumption of a congruential encryption system.

As a result, analyzing the NTRU system within homomorphic lattice-based encryption allows complementing it with algebraic operations. Using a method with base reducing elements results in the discovery of reduced ciphertext's property. Also, differences between the homomorphic and non-homomorphic workflows of NTRU pulls out differences in parameters choosing related to the security parameter which was done basing on the work [10].

For future work, it can be suggested assuming methods with base reducing elements and reduced ciphertext in the construction of FHE.

This work organized as follows: Section 1 brings forward the introduction, Section 2 describes a theory that leads to the definition of the base reducing element used in the paper, Section 3 presents an application part that uses material from the theoretical section. Subsections include: generally used and sets-related definitions in section 2.1; relations between remainder theorem and ciphertext construction in section 2.2; homomorphic relations in ciphertext structure which uses statements from theory above. In the applicable part: analysis of congruential encryption system in section 3.1, NTRU in section 3.2, homomorphic system parameters related to FHE over integers in section 3.3. Section 4 presents the conclusion.

2. Theoretical background

2.1. Basic definitions

Let's introduce definitions of meaningful $p \in P$ and probabilistic parts $u \in U$ that are sampled from the message set $c \in C$ and set of random integers $r \in R$ respectively:

$$\mathrm{R} = \{r \in \mathbb{Z}\},\ \mathrm{U} = \{u \mid \forall r < 2^N :\ u = \mathcal{S}_{R_N}(r)\};$$

$$\mathrm{C} = \{c \in \mathbb{Z}\},\ \mathrm{P} = \{p \mid \forall c < 2^N :\ p = \mathcal{S}_{P_N}(c)\};$$

where $S_{A_N}(B)$ - corresponding function that sampling set A from set B with bit-length N.

All of the elements that will be described further can be represented from the image below (Fig. 1), which is describes relations between sets in the transform process obtaining the ciphertext.

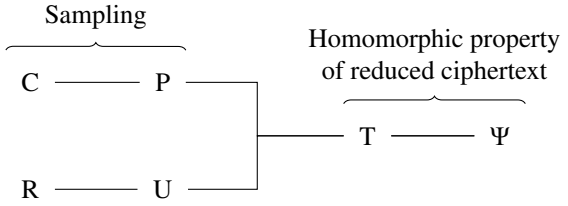

Figure 1. Workflow scheme of encryption with the use of base reducing elements construct

Assume that C and R are ideals generally such that ciphertext Ψ can be constructed using them with secret q in some lattice space $\mathcal{L}$ which possess correctness property for a decryption process.

$$\Psi = \{\psi \in \mathcal{L} \mid \mathrm{P}, \mathrm{U} \lhd \mathcal{L}, p : \psi \leftarrow Enc_q(c) : \text{choose } r, \psi \leftarrow f(k, u, p)\}; \tag{1}$$

$$Dec_q(Enc_q(c)) = c;$$

For homomorphic encryption needed homomorphic operations, such operations over ciphertext Ψ makes homomorphic to algebraic operations over opentext C with endless operations capability for FHE.

$$\psi_1 \leftarrow Enc_q(c_1), \psi_2 \leftarrow Enc_q(c_2), \psi_3 \leftarrow Eval(f, \psi_1, \psi_2) : Dec_q(\psi_3) = f(c_1, c_2);$$

Since Ψ is a ring which consist of two operations $\{\oplus, \otimes\}$ each transformation between $\mathrm{P} \rightarrow \Psi$, $\Psi \rightarrow \mathrm{P}$, $\Psi \rightarrow \Psi$ consist of composition of ring operations for *Enc*, *Dec* and *Eval* respectively. Therefore P and U must share the same ring operations and also be ideals relative to the same set Ψ. This relative showed in (1) and marked as symbol $\lhd$.

Taking into account the properties of ideals it can be showen that power of each set P either U is less then formed set Ψ. Also to preserve possibility of decryption its needed for each meaningful value to has its own disjoint probabilistic set within current key, i. e. $|\mathrm{P}| \cdot |\mathrm{U}| \leq |\Psi|$. In general case meanful and propabilistic parts can be represented with set of elements $\mathrm{P} = \{\mathrm{P}_1, \mathrm{P}_2, ...\}$, $\mathrm{U} = \{\mathrm{U}_1, \mathrm{U}_2, ...\}$. In such case both parts must be combined in the same way using ring operation $\{\oplus, \otimes\}$. Then their own powers satisfies the relation:

$$|\mathrm{P}| = |\mathrm{P}_1| \cdot |\mathrm{P}_2| \cdot ... \; ; \; |\mathrm{U}| = |\mathrm{U}_1| \cdot |\mathrm{U}_2| \cdot ... \; ; \quad |\Psi| \geq |\mathrm{P}| \cdot |\mathrm{U}|; \tag{2}$$

As it can be seen, ciphertext transformation either encryption or decryption processes are products of group operation, it can be define as composition of functions:

$$h = h_1 \circ h_2 \circ ... \circ h_N, h \in \{\oplus, \otimes\}, \text{ where } N \text{ is evaluation length.}$$

As it state in introduction to satisfy security requirements it necessary to make combination from both meaningful and probabilistic part. Such combinations will be denotes as $h(p, u)$ which in case of many elements may be represented as:

$$h(p, u) = h(p_1, p_2, ..., u_1, u_2, ...) \tag{3}$$

with at least one non-zero p-element and at least one non-zero u-element.

Before encryption scheme will be obtained it is necessary to investigate a way it will be constructed.

2.2. Encryption method

The building of ideal-based ciphertext laying on the assumption that ideals can be extracted further. The use of the "remainder theorem" can be one of the principal ways to do this. For arbitrary lattice using it countable property it can be always estimate remainder by defining countable subset and finding non-countable part with shortest norm. For example, in Euclidian space for arbitrary i, j, k and $q \in \mathbb{Z}$:

$$i = jq + k \tag{4}$$

There are two ways of extraction of the meaningful part from the ciphertext. The use of a remainder can be considered as the first way and the use of a quotient as the other, symbolically it can be written with notation referenced to a modulo operation:

$$j = i \bmod q; \tag{5}$$

$$k = (i - i \bmod q)/q = \lfloor i/q \rfloor; \tag{6}$$

Using mod operation has a specific point of view in the context. It can be represented as the cutting of dismissive information pieces. The probabilistic information part is the only such dismissive part is. Thus it becomes a nested reduction of random U from the ciphertext to obtain opentext P. This uses the key material q reduced to scalar in lattice space. Although notations (3, 4) do not establish direct comply with a meaningful part either propabilistic part or a way of extractions, the ideals specified as rings with two group operations the equation (4) is ideally suites for combining both parts.

$$a \otimes q \oplus b \leftarrow h(q, p, u) \tag{7}$$

where $a \leftarrow h(p,u)$, $b \leftarrow h(p,u)$ and q is additional secret value used to extract left either right part from the upper structure. Also each part can be formed in the similar way of $h(q,u,p)$ using its own secret and its own values. Also values can be taken from multiple parts (3) giving rise to several levels of nesting, e.g:

$$a = h_{a_1}(p_1, p_2, ..., u_1, u_2, ...) \otimes q_a \oplus h_{a_2}(p_1, p_2, ..., u_1, u_2, ...) \leftarrow h(q_a, p, u);$$

$$b = h_{b_1}(p_1, p_2, ..., u_1, u_2, ...) \otimes q_b \oplus h_{b_2}(p_1, p_2, ..., u_1, u_2, ...) \leftarrow h(q_b, p, u),$$

Without loss of generality it can be shown that for any nesting structure the resulting relationship is isomorphic to form:

$$h(h_{q_1}, h_{q_2}, ...) = h_1(p,u) \otimes q_1 \oplus h_2(p,u) \otimes q_2 \oplus ... \oplus h_N(p,u) \otimes q_N; \tag{8}$$

$$h(h_{q_1}, h_{q_2}, ...) = \sum_{i=1}^{N} h_i(p,u) \otimes q_i; \tag{9}$$

Each h_{q_n} element which uses combining method (7) above will be called as base reducing element with their own characteristic q_n, total nesting level N and with $q_N = 1$ for the last element.

The main advantage of such construction is easy way to count upper bound of security strength which can be determined the ratio of sets power before and after injection secret material regardless of the combination method of $h(u,p)$. Thus considering relation (2):

$$\frac{|\Psi|}{|\mathrm{P}| \cdot |\mathrm{U}|} = \left| \frac{h(q,p,u)}{h(p,u)} \right| = |\mathrm{Q}| = |\mathrm{Q}_1| \cdot |\mathrm{Q}_2| \cdot ...,$$

where Q is set that containing key material:

$$\mathrm{Q} = \{\mathrm{Q}_1, \mathrm{Q}_2, ...\}, q \in \mathrm{Q}, q_1 \in \mathrm{Q}_1, ...$$

With analog to h-operator definition, it can be viewed from a point of decryption process using one of the methods from (5,6). As a result, it brings to the extraction of specific part separately from the form (9). Thus if the ciphertext is in some combination of $h(q,p,u)$ then each meaningful can be extracted using one of base reducing element characteristics, e. g.:

$$u \leftarrow d(q, h(q,p,u)) = d_q,$$

where $d \in$ {binary mod operation from (5) or floor operation from (6)}

With no loss of generalization for nested levels it can be construct decryption chain for final form (9) that handles ordered sequence for base reducing elements, that is:

$$h_{enc} = \{h_{q_1}, h_{q_2}, ..., h_{q_N}\}(u,p);$$
$$h_{dec} = \{d_{q_N}, d_{q_{N-1}}, ..., d_{q_1}\}(\psi), \text{ for } q_1 < q_2 < ... < q_N;$$

such that

$$u \leftarrow h_{dec}(h_{enc}(u,p))$$

Finally, it should be carried out under theoretical assumptions above, how a homomorphic scheme is viewed using nested combinations of base reducing elements.

2.3. Homomorphic property

Homomorphic operations can be formed as product of (3):

$$h_f(\psi_1, \psi_2) = h_f^*(q, h_f(p_1, p_2), h_f(u_1, u_2)) \leftarrow Eval(f, \psi_1, \psi_2)$$

With full form (9) there are parts of noise k can be found which are increases after each operation:

$$\forall n \in \mathbb{Z}, u_n > 0 : k_n = \sum_{i\,=\,n+1}^{N} h_i(u, p) \cdot q_i$$

And for total noise vector $k = k_1, k_2, ...$ it needed for correct decryption to be each part is less than corresponding value of q_n:

$$\forall n \in \mathbb{Z}, u_n > 0 : q_n > k_n$$

As it can be seen homomorphic encryption is aimed to have each $k_n \ll q_n$ to maximize number of h-operations. So the mentioned ciphertext is never covers full range of set Ψ otlining the set of reduced ciphertext T with:

$$|\mathrm{T}| < |\Psi|$$

It is reflected in the natural increase of k-components after each group operation which is also called "noise grow". As a weak assumption, it can be state that the purpose of FHE is to count each of the nested noise components to perform their reduction under certain conditions.

Technically, it consists in the loss of distribution property, e. g. for some $\circ$-operation composed on group operation with refreshing that is:

$$\psi_1 \circ (\psi_2 \circ \psi_3) \neq (\psi_1 \circ \psi_2) \circ \psi_3$$

3. Applications

To demonstrate presented assumptions it was analyzed different lattice-based systems. There is notations below that express such systems within decryption process that obtain an open text message from the encrypted ciphertext.

3.1. Use for base reducing element method in congruential encryption system

To show existence for the base reducing element method congruential cryptosystem is used. This system described by Hoffstein [4] and works under the next conditions:

$$\pi^* = f\,(\pi, r, q, \mathrm{f}, g)\,, \begin{cases} \pi, r, q, \mathrm{f}, g \in \mathbb{Z} \\ g < q,\ \mathrm{f} < \sqrt{q/2} \\ \exists\, \mathrm{f}^{-1}\ mod\ q = \mathrm{f}_q^{-1} \\ gcd(\mathrm{f}, g) = 1 \end{cases}$$

where ψ – ciphertext, π – open message, r – random integer, q, g, f - parameters of a system (secrets).

Its notation can be expressed as a function that obtains an open text message from the encrypted ciphertext which works as follows:

$$\pi^* = \left(\mathrm{f}_g^{-1} \cdot (\mathrm{f} \cdot \psi\ mod\ q)\right)\ mod\ g = \left(\mathrm{f}_g^{-1} \cdot (\mathrm{f} \cdot (r \cdot h + \pi)\ mod\ q)\right)\ mod\ g =$$
$$= \left(\mathrm{f}_g^{-1} \cdot \left(\mathrm{f} \cdot \left(r \cdot \left(g \cdot \mathrm{f}_q^{-1}\right) + \pi\right)\ mod\ q\right)\right)\ mod\ g$$

As it can be seen, notation above reveals the structure of ciphertext. Nature of lattices supports some homomorphic algebra without additional constructions by default. For addition and multiplication it preserves the structure with generous number of operations:

$$\psi_1 + \psi_2 = ((\pi_1 + \pi_2) + h \cdot (r_1 + r_2)) \ mod\ q;$$

$$\psi_1 \cdot \psi_2 = \pi_1 \cdot \pi_2 + h \cdot (\pi_1 r_2 + \pi_2 r_1 + h r_1 r_2)\ mod\ q;$$

Also it represents the decryption process from which two base reducing elements structures b_1, b_2 can be extracted for each mod operation respectively. It is implied further that for some q-th residue space, expression $A \cdot A^{-1}$ produces local one $(q \cdot k + 1)$ for arbitrary $k \in \mathbb{Z}$. Performing analysis of ψ for each element b_1, b_2 and arbitrary k, k_1, k_2 gives:

$$b_1 = qk_1 + r \cdot (qk_2 + 1) \cdot g + \pi \mathrm{f} = qk + rg + \pi \mathrm{f}$$

$$b_2 = r \mathrm{f}_g^{-1} g + (gk + 1) \cdot \pi = (k + r \mathrm{f}_g^{-1}) g + \pi$$

From that point, we continue to determine meaningful (p_1, p_2) and random parts (u_1, u_2) of base reducing elements:

$$u_1 = qk,\ p_1 = rg + \pi \mathrm{f}$$

$$u_2 = (k + r \mathrm{f}_g^{-1}) g,\ p_2 = \pi$$

Thus the security determines by three elements by (q, g, f) however the homomorphic property comes down only for two elements (q, g). These elements produce two noisy homomorphic buffers which ones must be taken into account in order to construct a homomorphic encryption system.

3.2. Reduced ciphertext property in NTRU

The NTRU system is the same as a congruential system except for the use of polynomial rings $\mathcal{R}_q[X]/(X^N - 1)$ instead of integers. The same applies to the implementation of homomorphic operations. The main difference is that in a polynomial ring with specific $(X^N - 1)$ polynomial the ciphertext multiplication becomes equivalence to convolution product that involves faster calculation.

For two different base reducing elements defined by p and q we can show sets of reduced ciphertext separately for addition and multiplication:

$$\overset{+}{\max}(p_1) = q/2;\ \overset{+}{\max}(p_2) = g/2;$$

$$\overset{*}{\max}(p_1) = \sqrt{\frac{q}{N}};\ \overset{*}{\max}(p_2) = \sqrt{\frac{g}{N}};$$

where *max* - max value of any element from related vector-represented polynomial.

3.3. Homomorphic property from FHE over integers

To demonstrate homomorphic property parameters of homomorphic encryption system it can be analyzed in relation to the security parameter. From FHE over integers [10] homomorphic ciphertext can be produced as:

$$Encrypt(pk, p \in \{0, 1\}); S \subseteq \{1, 2, 3, ..., \tau\}, r \in (-2^{\rho'}, 2^{\rho'}) : \psi \leftarrow \left[p + 2u + 2 \sum_{i \in S} x_i \right]_{x_0},$$

where τ - public key length, $pk = (x_0, x_1, ..., x_\tau)$, S - set of subkeys used for encryption, ρ - bit-length of the noise, $\rho = 2\rho'$, p - opentext, which match same message space, u - random part, [.] - means mod operation.

The keys are obtained from the next calculations:

$$x_i \overset{\$}{\leftarrow} \mathcal{D}_{\gamma,\rho}(p) \text{ - } public\ key; p \overset{\$}{\leftarrow} (2\mathbb{Z} + 1) \cap [2^{\eta-1}, 2^\eta) \text{ - } secret\ key,$$

where $\mathcal{D}_{\gamma,\rho}$ is sampling function in form:

$$\mathcal{D}_{\gamma,\rho} = \left\{ choose\ q \xleftarrow{\$} \mathbb{Z} \cap [0, 2^{\gamma}/p), r \xleftarrow{\$} \mathbb{Z} \cap (-2\rho, 2\rho) : output\ x = pq + r \right\}$$

To simplify the view all parameters with not described yet are listed again below:

- τ - public key length, $pk = (x_0, x_1, ..., x_\tau)$, $\tau >= \gamma + \omega(log\lambda) = \gamma + \rho$ - match gcd reduction lemma.
- γ - bit-length of integers in the pk, $\gamma = \omega(\eta^2 log\lambda)$.
- ρ - bit-length of the noise, $\rho = \omega(log\lambda)$ - choosen for bruteforce protection.
- η - bit-length of secret key l, $\eta >= \rho \cdot \Theta(\lambda log^2 \lambda)$
- λ - security parameter.
- ω - noise expand, secondary dependancy.
- Θ - homomorphism vol, secondary dependancy

As can be seen, homomorphic property Θ has simple relation to security parameter λ, therefore, it can be chosen independently.

Conclusion

In this paper was described an analysis method for an ideal lattice-based encryption system. The base reducing element concepts with its nested combinations used as a foundation for the analysis method. This method was linked to homomorphic encryption explaining its property of noise growing and the procedure of noise reduction. As proof for the revelated concept different encryption systems was analyzed, including non-homomorphic systems with homomorphic operations were provided.

This analysis shows nearly independent relations in choice of security either homomorphic parameters and the existence of different reduced ciphertext spaces for each of group operations.

For future directions of work, it will be solved the question, what if both group operations can be defined under one reduced ciphertext space easy linking them with one noise-control parameter. Another question is to prove that reduced ciphertext either probabilistic part is an obstacle for constructing FHE schemes.

Acknowledgement

The research is supported by the grant of the Russian Science Foundation (Project № 19-19-00566).

References

[1] Acar, A., Aksu, H., Uluagac, A.S., Conti, M., 2018. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR) 51, 1–35.
[2] Boneh, D., Lipton, R., et al., 1996. Searching for elements in black-box fields and applications, in: Crypto, pp. 283–297.
[3] Gentry, C., Boneh, D., 2009. A fully homomorphic encryption scheme. volume 20. Stanford university Stanford.
[4] Hoffstein, J., Pipher, J., Silverman, J.H., Silverman, J.H., 2008. An introduction to mathematical cryptography. volume 1. Springer.
[5] Maurer, U., Raub, D., 2007. Black-box extension fields and the inexistence of field-homomorphic one-way permutations, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer. pp. 427–443.
[6] Rivest, R.L., Adleman, L., Dertouzos, M.L., et al., 1978. On data banks and privacy homomorphisms. Foundations of secure computation 4, 169–180.
[7] Rohloff, K., Cousins, D.B., 2014. A scalable implementation of fully homomorphic encryption built on ntru, in: International Conference on Financial Cryptography and Data Security, Springer. pp. 221–234.
[8] Vaikuntanathan, V., 2011. Computing blindfolded: New developments in fully homomorphic encryption, in: 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, IEEE. pp. 5–16.
[9] Van Dam, W., Hallgren, S., Ip, L., 2006. Quantum algorithms for some hidden shift problems. SIAM Journal on Computing 36, 763–778.
[10] Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V., 2010. Fully homomorphic encryption over the integers, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer. pp. 24–43.