Noise-free Symmetric Fully Homomorphic Encryption based on noncommutative rings

Jing Li, Licheng Wang

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876 P.R. China.

Abstract. In this paper, we propose a noise-free symmetric fully homomorphic encryption (FHE) based on matrices over noncommutative rings. The scheme is secure against chosen plaintext attacks based on the factorization problem of matrices over noncommutative rings as well as the hardness of an overdefined system of multivariate polynomial equations over the given non-commutative algebraic structure. Meanwhile, the new proposal is efficient in terms of computational cost and the sizes of plaintext/ciphertext. On the basis of this framework, a verifiable FHE is proposed, where the receiver can check the validity of ciphertexts. Furthermore, any attacker fails to construct a valid ciphertext without making query of encryption oracle, then the verifiable FHE scheme maybe secure against non-adaptively chosen ciphertext attacks (IND-CCA1).

Keywords: Noncommutative rings, Noise-free, Symmetric-FHE, verifiable FHE.

1 Introduction

The pioneering design of fully homomorphic encryption was proposed by Gentry [8], which enables anyone to perform homomorphic operations on the ciphertexts for achieving arbitrary operations on the plaintexts, without revealing any information about the encrypted plaintexts. Due to the theoretical and practical significance, much outstanding work have been demonstrated to improve the efficiency and security [1–7, 9–12, 14]. Most of the current FHE schemes rely on the bootstrapping technique to cut down the noise on the ciphertexts. In 2014, Nuida proposed a noise-free framework for constructing public key fully homomorphic encryption without using bootstrapping [16]. After that, many researchers throw themselves into realizing this framework by a secure instantiation.

In 2012, a noise-free symmetric fully homomorphic encryption was constructed based on matrices over ring Z_n [13]. In 2015, two symmetric fully homomorphic encryption were given on 2015-05-17 and 2015-05-19 [15, 19]. However, these schemes have been proved to be insecure under chosen plaintext

attacks [18]. Thus, our motivation is to construct a secure and efficient noise-free fully homomorphic encryption.

CONTRIBUTIONS. In this paper, we propose a noise-free symmetric fully homomorphic encryption (FHE) based on matrices over noncommutative rings. In the encryption phase, the plaintext is encoded into a triangular matrix as plaintext-matrix, where the plaintext, chosen from the given ring, is hidden into the upper left corner of the triangular matrix. Meanwhile, other elements of the triangular matrix are randomly chosen from the noncommutative ring. Let the key-matrix act on the plaintext-matrix using conjugate operation and get the ciphertext-matrix. We can see that the encryption algorithm achieves both addition homomorphism and multiplication homomorphism and it is a non-deterministic encryption. Meanwhile, the scheme is secure based on the factorization problem of matrices over noncommutative rings and the hardness of an overdefined system of multivariate polynomial equations over this algebraic structure. The new proposal is efficient in terms of computational cost and the sizes of plaintext/ciphertext. Furthermore, by using the mewly proposed FHE framework, an asymmetric verifiable FHE (VFHE) is designed, where the receiver can check the validity of ciphertexts. Based on the verification property, the attackers fails to output a valid ciphertext without issuing query of encryption oracle, then the verifiable FHE scheme may be secure against non-adaptively chosen ciphertext attacks (IND-CCA1).

2 Our FHE based on matrix over noncommutative rings

Now we give the construction of the symmetric FHE based on noncommutative ring R.

2.1 Description

Setup**:** Let the symmetric key be

$$H = \begin{pmatrix} h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 \\ h_7 & h_8 & h_9 \end{pmatrix},$$

where $h_i \in R\ (i = 1, \ldots, 9)$ are randomly chosen such that H is invertible.

Encryption**:** The user will encrypt the message $m \in R$. He randomly selects $r_i \in R\ (i = 1, \ldots, 5)$ and constructs a matrix as

$$M = \begin{pmatrix} m & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix}.$$

Then the ciphertext is

$$C = Enc_H(m) = HMH^{-1}.$$

$\mathrm{Decryption}$**:** The receiver computes

$$m = Dec_H(C) = (H^{-1}CH)_{11},$$

where $(H^{-1}CH)_{11}$ denotes the top left corner element of matrix $H^{-1}CH$.

$\mathrm{Operations}$**:** Let C_1 and C_2 be the ciphertexts of m_1 and m_2, respectively. Now define "$\oplus$" gate and "$\otimes$" gate as

$$C_1 \oplus C_2 = C_1 + C_2, \;\; C_1 \otimes C_2 = C_1 \cdot C_2$$

that are matrix addition and matrix multiplication, respectively.

Homomorphic property. The addition homomorphism holds since

$$\begin{aligned} C_1 \oplus C_2 &= Enc_H(m_1) + Enc_H(m_2) \\ &= H \begin{pmatrix} m_1 & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix} H^{-1} + H \begin{pmatrix} m_2 & r_1' & r_2' \\ 0 & r_3' & r_4' \\ 0 & 0 & r_5' \end{pmatrix} H^{-1} \\ &= H \begin{pmatrix} m_1 + m_2 & r_1 + r_1' & r_2 + r_2' \\ 0 & r_3 + r_3' & r_4 + r_4' \\ 0 & 0 & r_5 + r_5' \end{pmatrix} H^{-1}. \end{aligned}$$

Then we have that $Dec_H(C_1 \oplus C_2) = m_1 + m_2$. Meanwhile, the encryption has the multiplication homomorphism since

$$\begin{aligned} C_1 \otimes C_2 &= Enc_H(m_1) \cdot Enc_H(m_2) \\ &= H \begin{pmatrix} m_1 & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix} H^{-1} \cdot H \begin{pmatrix} m_2 & r_1' & r_2' \\ 0 & r_3' & r_4' \\ 0 & 0 & r_5' \end{pmatrix} H^{-1} \\ &= H \begin{pmatrix} m_1 m_2 & r_1'' & r_2'' \\ 0 & r_3'' & r_4'' \\ 0 & 0 & r_5'' \end{pmatrix} H^{-1}. \end{aligned}$$

Then $Dec_H(C_1 \otimes C_2) = m_1 m_2$.

2.2 Security

In this section, we will analyze the security of the new proposal based on the given ring R. Denote

$$H^{-1} = \begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix}.$$

The ciphertext is determined by

$$C = HMH^{-1} = \begin{pmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{pmatrix},$$

where each component of matrix C is represented as

$$c_1 = h_1 m y_1 + h_1 r_1 y_4 + h_2 r_3 y_4 + h_1 r_2 y_7 + h_2 r_4 y_7 + h_3 r_5 y_7, \quad (1)$$
$$c_2 = h_1 m y_2 + h_1 r_1 y_5 + h_2 r_3 y_5 + h_1 r_2 y_8 + h_2 r_4 y_8 + h_3 r_5 y_8, \quad (2)$$
$$c_3 = h_1 m y_3 + h_1 r_1 y_6 + h_2 r_3 y_6 + h_1 r_2 y_9 + h_2 r_4 y_9 + h_3 r_5 y_9, \quad (3)$$
$$c_4 = h_4 m y_1 + h_4 r_1 y_4 + h_5 r_3 y_4 + h_4 r_2 y_7 + h_5 r_4 y_7 + h_6 r_5 y_7, \quad (4)$$
$$c_5 = h_4 m y_2 + h_4 r_1 y_5 + h_5 r_3 y_5 + h_4 r_2 y_8 + h_5 r_4 y_8 + h_6 r_5 y_8, \quad (5)$$
$$c_6 = h_4 m y_3 + h_4 r_1 y_6 + h_5 r_3 y_6 + h_4 r_2 y_9 + h_5 r_4 y_9 + h_6 r_5 y_9, \quad (6)$$
$$c_7 = h_7 m y_1 + h_7 r_1 y_4 + h_8 r_3 y_4 + h_7 r_2 y_7 + h_8 r_4 y_7 + h_9 r_5 y_7, \quad (7)$$
$$c_8 = h_7 m y_2 + h_7 r_1 y_5 + h_8 r_3 y_5 + h_7 r_2 y_8 + h_8 r_4 y_8 + h_9 r_5 y_8, \quad (8)$$
$$c_9 = h_7 m y_3 + h_7 r_1 y_6 + h_8 r_3 y_6 + h_7 r_2 y_9 + h_8 r_4 y_9 + h_9 r_5 y_9. \quad (9)$$

Meanwhile, the plaintext can be determined by

$$\begin{aligned} m = {} & y_1 c_1 h_1 + y_2 c_4 h_1 + y_3 c_7 h_1 + y_1 c_2 h_4 + y_2 c_5 h_4 + \\ & y_3 c_8 h_4 + y_1 c_3 h_7 + y_2 c_6 h_7 + y_3 c_9 h_7 \end{aligned} \quad (10)$$

for $y_i, c_j, h_k \in R$.

Consider the chosen plaintext attacks. There is an adversary who is allowed to make queries from the encryption oracle but not from the decryption oracle (since the adversary may obtain each secret parameter by establishing relevant query-ciphertexts).

Remark 1. In Eq. (10), $y_1, y_2, y_3, h_1, h_4, h_7$ are undetermined. Thus, assume that ring R is commutative, then the adversary can solve the following linear equations about $y_1 h_1, \ldots, y_3 h_7$ as

$$\begin{aligned} m_i = {} & c_{i1} y_1 h_1 + c_{i4} y_2 h_1 + c_{i7} y_3 h_1 + c_{i2} y_1 h_4 + c_{i5} y_2 h_4 \\ & + c_{i8} y_3 h_4 + c_{i3} y_1 h_7 + c_{i6} y_2 h_7 + c_{i9} y_3 h_7 \end{aligned}$$

derived from encryption queries. Note that, $y_1h_1, \ldots, y_3h_7$ can act as the decryption key. Therefore, the scheme is not secure against linear attacks when R is an abelian ring e.g. a number field.

Then we will discuss the **security of secret key** for a non-abelian FHE. Observe the Eqs. (1)-(10), the adversary will try to derive the secret key, where there are random elements in Eqs. (1)-(9). Thus, we mainly discuss the security of the decryption key with respect to Eq. (10). After q-query of encryption oracle, the adversary can get the corresponding equations:

$$\begin{aligned}
m_1 &= y_1c_{11}h_1 + y_2c_{14}h_1 + y_3c_{17}h_1 + y_1c_{12}h_4 + y_2c_{15}h_4 + \\
&\qquad y_3c_{18}h_4 + y_1c_{13}h_7 + y_2c_{16}h_7 + y_3c_{19}h_7. \\
m_2 &= y_1c_{21}h_1 + y_2c_{24}h_1 + y_3c_{27}h_1 + y_1c_{22}h_4 + y_2c_{25}h_4 + \\
&\qquad y_3c_{28}h_4 + y_1c_{23}h_7 + y_2c_{26}h_7 + y_3c_{29}h_7. \\
&\qquad \cdots \\
m_q &= y_1c_{q1}h_1 + y_2c_{q4}h_1 + y_3c_{q7}h_1 + y_1c_{q2}h_4 + y_2c_{q5}h_4 + \\
&\qquad y_3c_{q8}h_4 + y_1c_{q3}h_7 + y_2c_{q6}h_7 + y_3c_{q9}h_7.
\end{aligned}$$

where c_{ij} are known to the attacker, but y_l, c_{ij}, h_k are noncommutative. Note that since our FHE is non-deterministic, these ciphertexts are randomly independent even if the queried messages are the same one. In the chosen plaintext attacks, solving the decryption key is equivalent to a problem of solving an overdefined system of quadratic multivariate polynomial equations in noncommutative rings. We have found the FHE schemes based on some noncommutative rings are not secure. Therefore, the most important task is to find a noncommutative ring and obtain a secure FHE.

3 Verifiable FHE

This section presents a verifiable FHE. The core technique is based on a nesting with respect to the given framework in Section 3.

3.1 Description

Setup**:** Let R be a noncommutative ring and the symmetric key be

$$H = \begin{pmatrix} H_1 & H_2 \\ H_3 & H_4 \end{pmatrix},$$

where

$$H_i = \begin{pmatrix} h_{i1} & h_{i2} & h_{i3} \\ h_{i4} & h_{i5} & h_{i6} \\ h_{i7} & h_{i8} & h_{i9} \end{pmatrix}$$

for $h_{ij} \in R$ $(i = 1, \ldots, 4,\ j = 1, \ldots, 9)$ are randomly chosen such that H is invertible. Now we consider the above encryption as a hash function, the corresponding secret key is

$$K = \begin{pmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{pmatrix}.$$

Encryption**:** The user will encrypt the message $m \in R$. He randomly selects $r_i \in R$ $(i = 1, \ldots, 17)$ and constructs a matrix as

$$M = \begin{pmatrix} M_1 & Q \\ 0 & KM_2K^{-1} \end{pmatrix}.$$

where

$$Q = \begin{pmatrix} r_9 & r_{10} & r_{11} \\ r_{12} & r_{13} & r_{14} \\ r_{15} & r_{16} & r_{17} \end{pmatrix},$$

$$M_1 = \begin{pmatrix} m & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} m & r_6 & r_7 \\ 0 & r_3 & r_8 \\ 0 & 0 & r_5 \end{pmatrix}.$$

Then the ciphertext is

$$C = Enc_H(m) = HMH^{-1}.$$

Decryption**:** The receiver computes and checks whether

$$((H^{-1}CH)_{11})_{11} = (K^{-1}(H^{-1}CH)_{21}K)_{11},$$

then $m = ((H^{-1}CH)_{11})_{11}$ is the top left corner element of 11-block of matrix $H^{-1}CH$. That is,

$$m = (Y_1C_1H_1 + Y_1C_2H_3 + Y_2C_3H_1 + Y_2C_4H_3)_{11}.$$

Operations**:** Let C_1 and C_2 be the ciphertexts of m_1 and m_2, respectively. Now define "$\oplus$" gate and "$\otimes$" gate as

$$C_1 \oplus C_2 = C_1 + C_2,\ \ C_1 \otimes C_2 = C_1 \cdot C_2$$

they are matrix addition and matrix multiplication, respectively.

Homomorphic property. The addition homomorphism holds since

$$\begin{aligned} C_1 \oplus C_2 &= Enc_H(m_1) + Enc_H(m_2) \\ &= H \begin{pmatrix} M_1^{(1)} & Q^{(1)} \\ 0 & KM_2^{(1)}K^{-1} \end{pmatrix} H^{-1} + H \begin{pmatrix} M_1^{(2)} & Q^{(2)} \\ 0 & KM_2^{(2)}K^{-1} \end{pmatrix} H^{-1} \\ &= H \begin{pmatrix} M_1^{(1)} + M_1^{(2)} & Q^{(1)} + Q^{(2)} \\ 0 & K(M_2^{(1)} + M_2^{(2)})K^{-1} \end{pmatrix} H^{-1}. \end{aligned}$$

Then we have that $Dec_H(C_1 \oplus C_2) = m_1 + m_2$. Meanwhile, the encryption has the multiplication homomorphism since

$$\begin{aligned} C_1 \otimes C_2 &= Enc_H(m_1) \cdot Enc_H(m_2) \\ &= H \begin{pmatrix} M_1^{(1)} & Q^{(1)} \\ 0 & KM_2^{(1)}K^{-1} \end{pmatrix} H^{-1} \cdot H \begin{pmatrix} M_1^{(2)} & Q^{(2)} \\ 0 & KM_2^{(2)}K^{-1} \end{pmatrix} H^{-1} \\ &= H \begin{pmatrix} M_1^{(1)} \cdot M_1^{(2)} & Q^{(3)} \\ 0 & KM_2^{(1)} \cdot M_2^{(2)}K^{-1} \end{pmatrix} H^{-1}. \end{aligned}$$

Note that,

$$\begin{aligned} M_1^{(1)} \otimes M_1^{(2)} &= \begin{pmatrix} m_1 & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix} \cdot \begin{pmatrix} m_2 & r_1' & r_2' \\ 0 & r_3' & r_4' \\ 0 & 0 & r_5' \end{pmatrix} \\ &= \begin{pmatrix} m_1 m_2 & r_1'' & r_2'' \\ 0 & r_3'' & r_4'' \\ 0 & 0 & r_5'' \end{pmatrix}. \end{aligned}$$

Then $Dec_H(C_1 \otimes C_2) = m_1 m_2$.

3.2 Analysis

In the verifiable FHE, the receiver can check the validity of the ciphertext. Thus, the scheme maybe secure against non-adaptively chosen ciphertext attacks (IND-CCA1). Note that, any adversary fails to obtain valid ciphertext meeting verification equation

$$((H^{-1}CH)_{11})_{11} = (K^{-1}(H^{-1}CH)_{21}K)_{11},$$

without the encrption key and verification key. Therefore, the FHE can be viewed as a fully homomorphism hash function.

4 Conclusions

This paper presents a framework of a noise-free symmetric fully homomorphism encryption over a noncommutative ring. The security of our FHE scheme is based on the factorization problem of matrices over noncommutative rings as well as the hardness of an overdefined system of multivariate polynomial equations over the given noncommutative algebraic structure. On the basis of this framework, a verifiable FHE is proposed, where the receiver can check the validity of ciphertexts. Furthermore, any attacker fails to construct a valid ciphertext, then the verifiable FHE scheme may be secure against non-adaptively chosen ciphertext attacks (IND-CCA1).

References

1. A. Lopez-Alt, E. Tromer and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption, in: Proceedings of STOC 2012, pp. 1219-1234, 2012.
2. Z. Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. in: Proceedings of CRYPTO 2012, LNCS 7417, pp. 868-886, 2012.
3. Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. in: Proceedings of FOCS 2011, pp. 97-106, 2011.
4. Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. in: Proceedings of CRYPTO 2011, LNCS 6841, pp. 505-524, 2011.
5. J.H. Cheon, J.S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi and A. Yun. Batch fully homomorphic encryption over the integers. in: Proceedings of EUROCRYPT 2013, LNCS 7881, pp. 315-335, 2013.
6. J.S. Coron, A. Mandal, D. Naccache and M. Tibouchi. Fully homomorphic encryption over the integers with shorter public keys. in: Proceedings of CRYPTO 2011, LNCS 6841, pp. 487-504, 2011.
7. J.S. Coron, D. Naccache and M. Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. in: Proceedings of EUROCRYPT 2012, LNCS 7237, pp. 446-464, 2012.
8. Craig Gentry. Fully homomorphic encryption using ideal lattices. In: Proceedings of STOC'09, pp. 169 – 178, 2009.
9. C. Gentry. Toward basing fully homomorphic encryption on worst-case hardness. in: Proceedings of CRYPTO 2010, LNCS 6223, pp. 116-137, 2010.
10. C. Gentry and S. Halevi. Implementing Gentry's fully-homomorphic encryption scheme. in: Proceedings of EUROCRYPT 2011, LNCS 6632, pp. 129-148, 2011.
11. C. Gentry and S. Halevi. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits, in: Proceedings of FOCS 2011, pp. 107-109, 2011.
12. C. Gentry, S. Halevi and N. P. Smart. Fully homomorphic encryption with polylog overhead, in: Proceedings of EUROCRYPT 2012, LNCS 7237, pp. 465-482, 2012.
13. A. Kipnis, E. Hibshoosh. Efficient Methods for Practical Fully-Homomorphic Symmetric-key Encryption, Randomization and Verification. Cryptology ePrint Archive, Report 2012/637.

14. D. Kahrobaei. C. Koupparis. V. Shpilrain. Public key exchange using matrices over group rings. Groups-Complexity-Cryptology, 5, pp. 97-115, 2013.
15. D. Liu. Practical Fully Homomorphic Encryption without Noise Reduction Cryptology ePrint Archive: http://eprint.iacr.org/2015/468.pdf.
16. K. Nuida. A Simple Framework for Noise-Free Construction of Fully Homomorphic Encryption from a Special Class of Non-Commutative Groups. Cryptology ePrint Archive, Report 2014/97.
17. B. Tsaban, N. Lifshitz. Cryptanalysis of the more symmetric key Fully Homomorphic Encryption scheme. Cryptology ePrint Archive, Report 2014/250.
18. Y. Wang. Notes on Two Fully Homomorphic Encryption Schemes without Bootstrapping. Cryptology ePrint Archive: http://eprint.iacr.org/2015/519.pdf.
19. M. Yagisawa. Fully homomorphic encryption without bootstrapping. Cryptology ePrint Archive: http://eprint.iacr.org/2015/474.pdf.