Noise-Free Symmetric Fully Homomorphic Encryption Based on Non-Commutative Rings

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

ABSTRACT

A framework of noise-free symmetric fully homomorphic encryption (FHE) is proposed in this work. Different from the frameworks that are defined over non-commutative groups, our framework is constructed from matrices over non-commutative rings. The scheme is one-way secure against chosen plaintext attacks (OW-CPA) 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. On the basis of this framework, a verifiable FHE is proposed, where the receiver can check the validity of ciphertexts.

Keywords

Non-commutative rings, Noise-free, Symmetric-FHE, Verifiable FHE

1. MOTIVATION

The pioneering design of fully homomorphic encryption (FHE), proposed by Gentry [2] in 2009, relies on the bootstrapping technique to cut down the noise accumulation during the process of combination of ciphertexts. After that, a lot of improvements towards Gentry's FHE scheme were proposed and most of them focus on reducing or removing the cost of the bootstrapping process. In 2014, a noise-free, and thus bootstrapping-free, framework for constructing public key fully homomorphic encryption was invented due to Nuida [5]. However, up to now, finding a secure instantiation of Nuida's framework is still an open problem.

Besides asymmetric scenario, finding symmetric fully homomorphic encryption is also a challenge problem. In 2012, Kipnis and Hibshoosh [3] proposed a noise-free symmetric fully homomorphic encryption based on matrices over ring $\mathbb{Z}_n$. Most recently, another symmetric fully homomorphic encryption schemes were proposed by Liu [4]. Unfortunately, all these schemes were proved insecure [6]. With careful investigation of these schemes and the related attacks, we think the weakness of these schemes are partially embedding in the commutativity of the underlying operations. Thus, our main motivation is to design a new framework of noise-free fully homomorphic encryption based on non-commutativity rings.

2. A SYMMETRIC FHE FRAMEWORK

2.1 Scheme Description

Suppose R be a non-commutative ring throughout the remain sections. Then, our symmetric fully homomorphic encryption scheme consists the following 5 algorithms:

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

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

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 $H^{-1}CH$.

Addition & Multiplication: Let C_1 and C_2 be the ciphertexts of m_1 and m_2, respectively. Then, the addition and multiplication of C_1 and C_2 are defined respectively as

$$C_1 \boxplus C_2 = C_1 + C_2 \tag{1}$$

and

$$C_1 \boxdot C_2 = C_1 \cdot C_2, \tag{2}$$

where $+$ and $\cdot$ denote respectively the general addition and multiplication operations of matrices over R.

It is trivial to verify the consistency of encryption and decryption, as well as the homomorphism of the addition and multiplication over ciphertexts.

2.2 Security Analysis

According to the decryption algorithm, the plaintext m can be recovered deterministically as follows:

$$\begin{aligned} m &= y_1c_1h_1 + y_2c_4h_1 + y_3c_7h_1 + y_1c_2h_4 + y_2c_5h_4 \\ &\quad + y_3c_8h_4 + y_1c_3h_7 + y_2c_6h_7 + y_3c_9h_7, \end{aligned} \tag{3}$$

where $y_i, c_j, h_k \in R$ $(i = 1, 2, 3;\ j = 1, \cdots, 9;\ k = 1, 4, 7)$.

Now, suppose that an adversary makes q encryption queries on the messages $m_1, \cdots, m_q$ that are selected by the adversary. Then, the equation (3) is instantiated as q equations:

$$\begin{aligned} m_\ell &= y_1c_{\ell,1}h_1 + y_2c_{\ell,4}h_1 + y_3c_{\ell,7}h_1 + y_1c_{\ell,2}h_4 + y_2c_{\ell,5}h_4 \\ &\quad + y_3c_{\ell,8}h_4 + y_1c_{\ell,3}h_7 + y_2c_{\ell,6}h_7 + y_3c_{\ell,9}h_7 \end{aligned} \tag{4}$$

for $\ell = 1, \cdots, q$, where $y_1, y_2, y_3, h_1, h_4, h_7$ are fixed unknowns. When $q < 6$, the equation system given by (4) is undetermined. When $q = 6$, the number of equations is equal to the number of unknowns. Without loss of generality, we assume that $q > 6$, then the equation system given by (4) is over-defined. At present, we do not know how to solve this kind of equation system, considering that both y_i and h_k are taken from a non-commutative ring R, and both of them are non-commute with $c_{\ell,j}$.

Remark 1. If the underlying ring R is commutative (e.g. R is a number ring or even field), then the equation system (4) is equivalent to the following linear system

$$\begin{aligned} m_\ell &= c_{\ell,1} \cdot \gamma_1 + c_{\ell,4} \cdot \gamma_2 + c_{\ell,7} \cdot \gamma_3 + c_{\ell,2} \cdot \gamma_4 + c_{\ell,5} \cdot \gamma_5 \\ &\quad + c_{\ell,8} \cdot \gamma_6 + c_{\ell,3} \cdot \gamma_7 + c_{\ell,6} \cdot \gamma_8 + c_{\ell,9} \cdot \gamma_9 \end{aligned} \tag{5}$$

for $\ell = 1, \cdots, q$, where γ_i $(i = 1, \cdots, 9)$ are fixed unknowns. Thus, this linear equation system (5) cannot stop adversary's efforts for extracting γ_is. This is one of the key reasons for us to choose a *non-commutative* ring as the underlying algebraic structure. Furthermore, based on the hard problem of solving equation of high degree, the scheme can be secure against the eigenvalue attacks.

3. VERIFIABLE FHE

This section presents a verifiable FHE. The core technique is to use the framework given in Section 2 by a nested manner.

Setup: Let R be a noncommutative ring and the encryption 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, let the corresponding verification key be $K = H_1$.

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

$$M_1 = \begin{pmatrix} m & r_1 & r_2 \\ 0 & r_3 & r_4 \\ 0 & 0 & r_5 \end{pmatrix}, \quad M_2 = \begin{pmatrix} m & r_6 & r_7 \\ 0 & r_3 & r_8 \\ 0 & 0 & r_5 \end{pmatrix}.$$

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

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 $H^{-1}CH$.

Addition & Multiplication: Same as "Addition & Multiplication" given in Section 2.1.

Remark 2. Our schemes fails to achieve the IND-CPA security considering that for given $C_1 = Enc_H(m)$ and $C_2 = Enc_H(m')$, if the rank of $C_1 - C_2$ is 2, then $m = m'$ holds.

Acknowledgements

We would like to thank Dr. Qiang Tang and Dr. Massimo Chenal for informing us the rank attacks.

4. REFERENCES

[1] Markus Bläser. Noncommutativity makes determinants hard. In Fedor V. Fomin et al. editors, ICALP 2013, Riga, Latvia, July 8-12, 2013, volume 7965 of Lecture Notes in Computer Science, pages 172–183, Springer 2013.

[2] Craig Gentry. Fully homomorphic encryption using ideal lattices. In: Proceedings of STOC'09, pp. 169–178, 2009.

[3] A. Kipnis, E. Hibshoosh. Efficient Methods for Practical Fully-Homomorphic Symmetric-key Encryption, Randomization and Verification. Cryptology ePrint Archive, Report 2012/637.

[4] D. Liu. Practical Fully Homomorphic Encryption without Noise Reduction. Cryptology ePrint Archive: http://eprint.iacr.org/2015/468.pdf.

[5] 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.

[6] Y. Wang. Notes on Two Fully Homomorphic Encryption Schemes without Bootstrapping. Cryptology ePrint Archive: http://eprint.iacr.org/2015/519.pdf.