Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping

Yongge Wang
UNC Charlotte
Charlotte, NC 28223, USA
yonwang@uncc.edu

Abstract

Last week, IACR ePrint archive posted two fully homomorphic encryption schemes without bootstrapping. In this note, we show that these schemes are trivially insecure.

I. Introduction

Though it is a very challenging problem to design fully homomorphic encryption schemes without bootstrapping. We still see that quite a few researchers post candidate designs frequently. This note points out that the two schemes posted to IACR ePrint archive last week are trivially insecure: the scheme by Masahiro Yagisawa [4] on 19 May 2015 and the scheme by Dongxi Liu [3] on 17 May 2015.

II. Masahiro Yagisawa [4]'s Scheme

Octonion (see, e.g., Conway and Smith [2] or Baez [1]) is the largest of the four normed division algebra and is the only normed division algebra that is neither commutative nor associative. Each octonion number is a vector $\mathbf{a} = [a_0, \cdots, a_7] \in R^8$ where R is the real number. For each octonion number $\mathbf{a} = [a_0, \cdots, a_7]$, we define an associate 8×8 matrix

$$A_{\mathbf{a}} = \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 & -a_4 & -a_5 & -a_6 & -a_7 \\ a_0 & a_1 & a_2 & a_3 & -a_4 & a_5 & -a_6 & -a_7 \\ a_0 & -a_1 & a_2 & a_3 & a_4 & -a_5 & a_6 & -a_7 \\ a_0 & -a_1 & -a_2 & a_3 & a_4 & a_5 & -a_6 & a_7 \\ a_0 & a_1 & -a_2 & a_3 & a_4 & a_5 & a_6 & -a_7 \\ a_0 & -a_1 & a_2 & -a_3 & -a_4 & a_5 & a_6 & a_7 \\ a_0 & a_1 & -a_2 & a_3 & -a_4 & -a_5 & a_6 & a_7 \\ a_0 & a_1 & a_2 & -a_3 & a_4 & -a_5 & -a_6 & a_7 \end{pmatrix} \tag{1}$$

For two octonions $\mathbf{a} = [a_0, \cdots, a_7]$ and $\mathbf{b} = [b_0, \cdots, b_7]$, we can add them as $\mathbf{a} + \mathbf{b} = [a_0 + b_0, \cdots, a_7 + b_t]$ and multiply them as $\mathbf{ab} = \mathbf{b}A_{\mathbf{a}}^T$.

Using octonions over $GF(q)$, Yagisawa [4] introduced a fully homomorphic encryption scheme. Though Yagisawa [4] defined his fully homomorphic encryption scheme in terms of a sequence of private octonion numbers, the scheme could be simplified using matrix operations. Let $GF(q)$ be the underlying finite field that we will work with and $\mathbf{1} = [1, 0, 0, 0, 0, 0, 0, 0]$. Then the protocol works as follows:

Key Setup. Choose a random invertible 8×8 matrix $K \in GF(q)^{8\times8}$. K is the private key.

Encryption. For a message $\mathbf{m} \in GF(q)^8$, compute the cipher text $C_m = \texttt{Enc}(K, \mathbf{m}) = K^{-1}A_{\mathbf{m}}K \in GF^{8\times8}$ where $A_{\mathbf{m}}$ is the associate matrix for $\mathbf{m}$ when $\mathbf{m}$ is considered as an octonion number.

Decryption. For a received ciphertext C_m, compute $A_{\mathbf{m}} = KC_mK^{-1}$. $\mathbf{m}$ can then be recovered from $A_{\mathbf{m}}$.

Ciphertext addition. The addition of two ciphertexts $C_{\mathbf{m}_0}$ and $C_{\mathbf{m}_1}$ is defined as the component wise addition $C_{\mathbf{m}_0+\mathbf{m}_1} = C_{\mathbf{m}_0} + C_{\mathbf{m}_1}$. That is, this is just the regular matrix addition.

Ciphertext multiplication. The multiplication of two ciphertexts $C_{\mathbf{m}_0}$ and $C_{\mathbf{m}_1}$ is defined as the regular matrix multiplication $C_{\mathbf{m}_0\times\mathbf{m}_1} = C_{\mathbf{m}_0}C_{\mathbf{m}_1} = KA_{\mathbf{m}_0}K^{-1}KA_{\mathbf{m}_1}K^{-1} = KA_{\mathbf{m}_0}A_{\mathbf{m}_1}K^{-1}$.

First we note that the above scheme is not fully homomorphic over $GF(q)$. Indeed, it is only fully homomorphic over the octonion numbers over $GF(q)$ since the multiplication of ciphertexts is the ciphertext of an octonion number which is a multiplication over the octonions. Since the multiplication in octonions is neither associative nor commutative, we generally cannot get a fully homomorphic scheme for $GF(q)$ using the above scheme. Though it is possible to revise the scheme to make it fully homomorphic over $GF(q)$. For example, for a plain text message $m \in GF(q)$ one may define an associate matrix $A_a = \begin{pmatrix} m & 0 \\ \mathbf{b}^T & B \end{pmatrix} \in GF(q)^{8\times 8}$ with uniformly at random chosen $\mathbf{b} \in GF(q)^7$ and $B \in GF(q)^{7\times 7}$.

Next we briefly mention that the above scheme could not be secure. The major issue for the above scheme is that the plaintext $\mathbf{0} = [0,0,0,0,0,0,0,0]$ is encrypted to the zero matrix. In other words, we can easily distinguish the ciphertext of $\mathbf{m}$ and $-\mathbf{m}$ since $C_{\mathbf{m}} + C_{-\mathbf{m}} = 0$.

III. DONGXI LIU [3]'S SCHEME

Liu [3] proposed a candidate fully homomorphic encryption scheme using linear algebra over $GF(q)$. Though the design in [3] is very complicated, we give a simple (equivalent) description of the protocol in [3]. From the simplified description, it is straightforward that the public evaluation keys leak all of the private key.

Let l, n be given numbers with $l \le n-2$. It is recommended to use $n = 5$ and $l = 3$ in [3]. The protocol works as follows.

Key Setup.

- Choose random vectors $\mathbf{k} = [k_0, \cdots, k_n] \in GF(q)^{n+1}$ and $\Theta = [\theta_0, \cdots, \theta_{l-1}] \in GF(q)^l$.
- For each $m \in GF(q)$, let $\mathbf{c}_m = \texttt{ENC}(\mathbf{k}, m) = [c_0, \cdots, c_n] \in GF(q)^{n+1}$ such that $m = \mathbf{k} \cdot \mathbf{c}_m$ where $\cdot$ is the inner product of $\mathbf{k}$ and $\mathbf{c}_m$. That is, $\mathbf{k} \cdot \mathbf{c}_m = c_0 k_0 + c_1 k_1 + \cdots + c_n k_n$.
- Let $\Phi = [\texttt{ENC}(\mathbf{k}, \theta_0), \cdots, \texttt{ENC}(\mathbf{k}, \theta_{l-1}), \texttt{ENC}(\mathbf{k}, 1)]$.
- The private key is $\mathbf{k}$ and Θ.
- The public evaluation key is $\mathbf{pek} = \{\mathbf{p}_{i,j} = \texttt{ENC}(\mathbf{k}, k_i k_j) : 0 \le i, j \le n\}$

Encryption. For a message $\mathbf{m} \in GF(q)$, choose random $r_0, \cdots, r_l \in GF(q)$ with $m = r_0 \oplus r_1 \oplus \cdots \oplus r_l$. The ciphertext of m is $\mathbf{c}_m = (r_0 \cdot \texttt{ENC}(\mathbf{k}, \theta_0)) \oplus \cdots \oplus (r_{l-1} \cdot \texttt{ENC}(\mathbf{k}, \theta_{l-1})) \oplus (r_l \cdot \texttt{ENC}(\mathbf{k}, 1))$.

Decryption. For a received ciphertext $\mathbf{c}_m$, compute $m = \mathbf{k} \cdot \mathbf{c}_m$.

Ciphertext addition. The addition of two ciphertexts $\mathbf{c}_{m_0}$ and $\mathbf{c}_{m_1}$ is defined as the component wise addition $\mathbf{c}_{m_0+m_1} = \mathbf{c}_{m_0} + \mathbf{c}_{m_1}$. That is, this is just the regular component wise vector addition.

Ciphertext multiplication. The multiplication of two ciphertexts $\mathbf{c}_{m_0} = [c_0, \cdots, c_n]$ and $\mathbf{c}_{m_1} = [c'_0, \cdots, c'_n]$ is defined as $\mathbf{c}_{m_0 m_1} = \sum_{i,j=0}^{n} c_i c_j \mathbf{p}_{i,j}$.

The correctness of the protocol could be easily verified (for details, it is referred to the original paper [3]. However, the protocol cannot be secure since the private key $\mathbf{k}$ could be trivially derived from the public evaluation key $\mathbf{pek}$. As an example, we can assume that $\mathbf{p}_{i,j} = [p_{i,j,0}, \cdots, p_{i,j,n}]$. Then we have the equations

$$\begin{array}{l} k_0 k_0 = p_{0,0,0} k_0 + \cdots + p_{0,0,n} k_n \\ \cdots \\ k_i k_j = p_{i,j,0} k_0 + \cdots + p_{i,j,n} k_n \\ \cdots \\ k_n k_n = p_{n,n,0} k_0 + \cdots + p_{nn,,n} k_n \end{array} \tag{2}$$

Using equation (2), one can easily obtain the private key $\mathbf{k}$ by constructing polynomial equations $f(k_i) = 0$ in one variable and then using the Euclidean algorithm to compute $\gcd(f(x), x^q - x)$ (or use Berlekamp's algorithm). For example, from the first equation, one can obtain an expression of k_n in terms of $k_0, \cdots, k_{n-1}$. By substituting this k_n into all remaining equations, one eliminates the occurrence of k_n from all remaining equations.

REFERENCES

[1] John Baez. The octonions. *Bulletin of the American Mathematical Society*, 39(2):145–205, 2002.

[2] John H Conway and Derek A Smith. On quaternions and octonions. *AMC*, 10:12, 2003.

[3] Dongxi Liu. Practical fully homomorphic encryption without noise reduction. Technical report, Cryptology ePrint Archive, Report 2015/468. http://eprint.iacr.org/2015/468, 2015.

[4] Masahiro Yagisawa. Fully homomorphic encryption without bootstrapping. Technical report, Cryptology ePrint Archive, Report 2015/474. http://eprint.iacr.org/2015/474, 2015.