Attack on Fully Homomorphic Encryption over Principal Ideal Lattice

Gu Chun-sheng[1,2] Gu Ji-xing[3]

[1] School of Computer Engineering, Jiangsu Teachers University of Technology, China Changzhou 213001
[2] School of Computer Science and Technology, University of Science and Technology of China, China Hefei 230027
[3] Institute of Image Communication & Information Processing, Shanghai Jiaotong University, China Shanghai 200240
guchunsheng@gmail.com

Abstract. For the fully homomorphic encryption schemes in [3, 6], this paper presents attacks to solve an equivalent secret key and directly recover plaintext from ciphertext for lattice dimensions n=2048 by using lattice reduction algorithm. Suppose the average-case behavior of LLL in [8] is true, then their schemes are also not secure for n=8192.

Keywords: Fully Homomorphic Encryption, Cryptanalysis, Principal Ideal Lattice, Lattice Reduction

1 Introduction

Rivest, Adleman and Dertouzos [1] first presented the concept of homomorphic encryption, which has many applications in cryptography. But until 2009, Gentry [2] constructed the first fully homomorphic encryptions based on ideal lattice, all previous schemes are insecure. After the scheme of [2], Smart and Vercauteren [3] presented an optimizating FHE with smaller ciphertext and key by using principal ideal lattice. Dijk, Gentry, Halevi, and Vaikuntanathan [4] proposed a simple fully homomorphic encryption scheme over the integers, whose security depends on the hardness of solving approximate GCD over the integers. Stehle and Steinfeld [5] improved Gentry's fully homomorphic scheme and obtained to a faster fully homomorphic scheme. Similar to [3], Gentry and Halevi [6] implemented Gentry's scheme by applying principal ideal lattice. The security of FHE's in [3, 6] depends on the hardness assumption of finding small principal ideal lattice, given its HNF form or two elements form. This paper will present two lattice attacks for FHE's in [3, 6].

By using block lattice reduction algorithm [7], we solve an equivalent secret key for n=2048 of FHE's in [3, 6]. Suppose the average case behavior of LLL [8], then the ratio $\|b_1\| / \lambda(L)$ is about $(1.02)^n$, i.e. $\|b_1\| \le (1.02)^n \lambda_1(L) << 2^{380} \lambda_1(L)$ for n=8192, where 380 is the bit-size of the coefficients in the generator polynomial of [6]. So, our first result shows the FHE's in [3, 6] are not secure for n=8192.

2 Preliminaries

Let n be security parameter, $[n]=\{0,1,...,n\}$. Let R be a ring of integer polynomials modulo $f_n(x)$, i.e., $R=\mathbb{Z}[x]/f(x)$, where $f_n(x)$ is an irreducible polynomial of degree n over the integers. Let R_p denote the polynomial ring $\mathbb{Z}_p[x]/f(x)$ over modulo p. For $\forall u\in R$, we denote by $\|u\|_\infty$ the infinity norm of u, $\vec{u}=[u_0,...,u_{n-1}]$ the coefficient vector of u, $[u]_2$ the polynomial of u's coefficients modulo 2.

Theorem 2.1 (Theorem 2.6 [10]) Every block $2k$-reduced basis $b_1,...,b_{mk}$ of lattice L satisfies $\|b_1\|\le\sqrt{\gamma_k}\beta_k^{\frac{m-1}{2}}\lambda_1(L)$, where β_k is another lattice constant using in Schnorr's algorithm analysis.

Theorem 2.2 (Theorem 2, 3 [7]) For all $k\ge 2$, Schnorr's constant β_k satisfies: $k/12\le\beta_k\le(1+k/2)^{2\ln 2+1/k}$. Asymptotically it satisfies $\beta_k\le 0.1\times k^{2\ln 2+1/k}$. In particular, $\beta_k\le k^{1.1}$ for all $k\le 100$.

Theorem 2.3 ([8]). Suppose the average case behavior of LLL is true, then the first vector b_1 of LLL is satisfied to $\|b_1\|/\lambda(L)\approx(1.02)^n$ on the average for lattice L.

3 Attack on Smart-Vercauteren's FHE

Theorem 3.1. Given a principal ideal π in either two element (p,α) or HNF representation, there is a polynomial time algorithm which finds $w(x)=\delta(x)\times v(x)$ over $\mathbb{Z}$ such that $\|\delta(x)\|_\infty\le\sqrt{\gamma_k}(4/3)^{(3k-1)/4}\beta_k^{n/2k-1}$.

Proof. Since α is a root of $f_n(x)=x^n+1$ over modulo p, so $x^n+1=(x-\alpha)\cdot g(x)\bmod p$. It is easy to verify $g(x)=t(x)\cdot v(x)\bmod p$. Assume $g(x)=x^{n-1}+g_{n-2}x^{n-2}+\cdots+g_0$. One constructs the following lattice M.

$$M=\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-2} & 1\\ -1 & g_0 & \cdots & g_{n-3} & g_{n-2}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ -g_1 & -g_2 & \cdots & -1 & g_0\\ p & 0 & \cdots & 0 & 0\\ 0 & p & \cdots & 0 & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & p \end{pmatrix}.$$

To reduce lattice M, one calls the lattice reduction algorithm in [7,10]. By Theorem 2.1, 2.2, one gets $w(x)=\delta(x)\times v(x)$ such that $\|\delta(x)\|_\infty\le\|\delta(x)\|_2\le\sqrt{\gamma_k}(4/3)^{(3k-1)/4}\beta_k^{n/(2k)-1}$. Recall that $w(x)\in R$ since $u(x)\times v(x)=p\bmod f_n(x)$. ■

When $n=2048$, $k=16$ and $\eta>298$, $\sqrt{\gamma_k}(4/3)^{(3k-1)/4}\beta_k^{n/(2k)-1}<2^{\eta-12}$. Hence, if $\|w(x)\times C(x)\|_\infty<p/2$, then one can correctly recover the bit in a ciphertext.

4 Attack on Gentry-Halevi's FHE

By the decryption algorithm in [6], a ciphertext vector is $\vec{c} = (c, 0, ..., 0)$. Hence, $[\vec{c} \times Rot(v)]_p = [c \cdot (v_0, v_1, ..., v_{n-1})]_p = ([cv_0]_p, [cv_1]_p, ..., [cv_{n-1}]_p)$. On the other hand, we have $[\vec{c} \times Rot(v) / p] = [\vec{a} \times Rot(v) / p] = \vec{a} \times Rot(v) / p$, where $[\cdot]$ is fractional part, and $\vec{a} = 2\vec{r} + b \cdot \vec{e}_1$ with small vectors $\vec{r}$ and $\vec{e}_1 = (1, 0, ..., 0)$. So, $[\vec{c} \times Rot(v)]_p = \vec{a} \times Rot(v) = 2\vec{r} \times Rot(v) + b \cdot \vec{v}$. That is, $([cv_0]_p, [cv_1]_p, ..., [cv_{n-1}]_p) = b \cdot \vec{v} \bmod 2$ for any decryptable ciphertext c.

We apply the same method in Section 3, which finds a small multiple $w(x) = \delta(x) \times v(x)$ of the secret key $v(x)$. When all the entries of $\vec{a} \times Rot(w(x))$ are less than $p/2$, we may recover the message bit in a ciphertext c as follows: $b = 1$ if $([cw_0]_p, [cw_1]_p, ..., [cw_{n-1}]_p) = \vec{w} \bmod 2$, otherwise $b = 0$. Thus, we finds $w(x) = \delta(x) \times v(x)$ over $\mathbb{Z}[x]$ with $\|\delta(x)\|_\infty \le \sqrt{\gamma_k} (4/3)^{(3k-1)/4} \beta_k^{n/2k-1}$ by Theorem 3.1.

When $n = 2048$, $k = 16$ and $\eta = 380$, we can recover the message bit in a ciphertext by the above method. Furthermore, we can also recover the message bit in a ciphertext for $n = 8196$, $\eta = 380$ by Theorem 2.3.

Reference

1. R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pages 169-180, 1978.
2. C. Gentry. Fully homomorphic encryption using ideal lattices. STOC 2009, pages 169-178.
3. N. P. Smart and Frederik Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. PKC 2010, LNCS 6056, pages 420-443.
4. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. Eurocrypt 2010, LNCS 6110, pages 24-43.
5. D. Stehle and R. Steinfeld. Faster Fully Homomorphic Encryption. Asiacrypt 2010, LNCS 6477, pages 377-394.
6. C. Gentry and Shai Halevi. Implementing Gentry's fully-homomorphic encryption scheme. EUROCRYPT 2011, LNCS 6632, pages 129-148.
7. N. Gama, N. Howgrave-Graham, H. Koy, and P. Q. Nguyen. Rankin's constant and blockwise lattice reduction. CRYPTO 2006, pages 112–130.
8. P. Q. Nguyen and D. Stehle, LLL on the average. ANTS VII, 2006, LNCS 4076, pages 238-256.
9. H. W. Lenstra Jr., A.K. Lenstra and L. Lov´asz, Factoring polynomials with rational coefficients, Mathematische Annalen 261, pages 515-534, 1982.
10. C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science, 53, pages 201-224, 1987.
11. Miklos Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. STOC 2001, pages 601-610.