# Adaptive Key Recovery Attacks on NTRU-based Somewhat Homomorphic Encryption Schemes

Ricardo Dahab[1] *, Steven Galbraith[2], and Eduardo Morais[1] **

[1] Institute of Computing, University of Campinas, Brazil
[2] Mathematics Department, University of Auckland, New Zealand

**Abstract.** In this paper we present adaptive key recovery attacks on NTRU-based somewhat homomorphic encryption schemes. Among such schemes, we study the proposal by Bos et al [BLLN13] in 2013. Given access to a decryption oracle, the attack allows us to compute the private key for all parameter choices. Such attacks show that one must be very careful about the use of homomorphic encryption in practice. The existence of a key recovery attack means that the scheme is not CCA1-secure. Indeed, almost every somewhat homomorphic construction proposed till now in the literature is vulnerable to an attack of this type. Hence our result adds to a body of literature that shows that building CCA1-secure homomorphic schemes is not trivial.

## 1 Introduction

The construction of *fully homomorphic encryption* (FHE) was conjectured in 1978 by Rivest, Adleman and Dertouzos [RAD78]. Although it was immediately recognized as a very interesting possibility in cryptography, no concrete construction was known until 2009, when Gentry used ideal lattices to settle this conjecture [Gen09a].

In short, ciphertexts produced by an FHE scheme can be operated on in such a way that we obtain a ciphertext that corresponds to the addition or multiplication of the respective plaintexts. The ability to algebraically operate over ciphertexts is of great importance because we can transform any algorithm into a sequence of additions and multiplications in $\mathbb{Z}_2$. Therefore, such a scheme can evaluate any algorithm solely with access to the encryption of its input, and such that the computation returns the encryption of the output.

Since Gentry's work, many FHE constructions have appeared in the literature. However, all the proposals have a common drawback: they are not practical. Initially, the algorithms involved in the constructions, although having polynomial complexity, had high polynomial degree. Later, the asymptotic complexity became much better. Indeed, we now have constructions with polylog overhead per operation, but with terribly high constants.

Although fully homomorphic encryption is not practical yet, many constructions have been proposed recently, achieving a somewhat homomorphic encryption (SHE) scheme. They allow a limited "depth" of operations to be performed. These constructions are indeed very useful in practice, specially in order to provide security in the scenario of cloud computing. SHE is important also in the implementation of *private information retrieval* (PIR) protocols, which can be seen as a building block to the solution for the privacy problem that emerges when we give our data to the cloud.

In the cloud computing scenario it is natural to imagine an attacker having access to a decryption oracle (e.g., the cloud can feed invalid ciphertexts to a user and monitor their behaviour). It is obvious that a homomorphic encryption scheme cannot have security of ciphertexts under adaptive attacks. Hence, adaptive attacks are already a very serious concern in this setting. But one could hope that at least the private key remains secure in the presence of a

* Partially supported by CNPq grant 311530/2011-7, and FAPESP Thematic Project 2013/25977-7
** Partially supported by FAPESP Thematic Project 2013/25977-7

decryption oracle. However, it is already known that this is not necessarily the case. Loftus et al [LMSV12] were the first to observe adaptive key recovery attacks, and further examples were given by Zhang et al [ZPS12] and Chenal and Tang [CT14]. By now, most schemes have been attacked, but the NTRU-based schemes remained unbroken.

Gentry's original construction is based on ideal lattices and is naturally implemented using cyclotomic rings. On the other hand, NTRU is a practical lattice-based cryptosystem, also based on cyclotomic rings, that remained without a security proof for a long time. Recently NTRU was put on a stronger foundation by Stehlé and Steinfeld [SS11], and NTRU-based cryptosystems returned as a fruitful research area. Scale-invariant homomorphic encryption was proposed by Brakerski [Bra12], presenting a construction that avoids the utilization of modulus switching technique, considerably simplifying the scheme.

In this work, we present *adaptive key recovery* attacks on NTRU-based SHE schemes. In particular, we attack the *scale-invariant* proposal by Bos et al [BLLN13].

### 1.1 Notation

Notation $\lfloor a \rceil$ is used to round $a$ to the nearest integer, while notation $[a]_q$ is used to denote centralized modular reduction, i.e. reduction modulo $q$, but with result given in the interval $(-q/2, q/2]$. If $a$ is a polynomial, then in order to compute $[a]_q$ we must compute a centralized modular reduction of each coefficient of $a$ (analogously for $\lfloor a \rceil$). When working over a polynomial ring $R$, if $a(x) \in R$, we use the notation $a[i]$ to denote the $i$-th coefficient of the polynomial $a(x)$.

### 1.2 Paper Organization

This paper is organized as follows. In section 2 we present basic definitions and details about the security model that will be used. In section 3 we gather information about key recovery attacks on other schemes in the literature. In section 4 we describe exactly how the SHE scheme BLLN is constructed. In section 5 we provide the main contribution of this paper, which is the key recovery attack. Finally, in section 6 we give our concluding remarks.

## 2 Fundamentals and Security Model

In this section we are going to present basic concepts and the security model that we will use throughout the paper.

**Definition 1. Homomorphic encryption.** *A homomorphic cryptosystem is defined using four algorithms,* KeyGen, Dec, Enc, Eval. *The first three are conventional encryption algorithms, with plaintext space $\mathcal{P}$ and security parameter $\lambda$. The scheme is said to be* correct *if, for a given algebraic circuit $C$, every key pair $(\mathrm{sk}, \mathrm{pk})$ generated by* KeyGen$(\lambda)$*, any message tuple $(m_1, \ldots, m_t) \in \mathcal{P}^t$ and corresponding ciphertexts $\Psi = \langle \psi_1, \ldots, \psi_t \rangle$, that is, $\psi_i =$ Enc$_{\mathrm{pk}}(m_i)$ for $1 \leq i \leq t$, then we have that the* Eval *algorithm respects the following relation*

$$\mathrm{Dec}_{\mathrm{sk}}(\mathrm{Eval}_{\mathrm{pk}}(C, \Psi)) = C(m_1, \ldots, m_t).$$

*Furthermore, the algorithms* KeyGen, Dec, Enc *and* Eval *must have polynomial complexity and we say that the scheme is homomorphic with respect to the circuit $C$.*

**Definition 2. Fully Homomorphic Encryption.** *A scheme $\mathcal{E} =$ (KeyGen, Dec, Enc, Eval) is* correct for a class $\mathbf{S_C}$ *of circuits, if it is correct for each $\mathbf{C} \in \mathbf{S_C}$. Moreover, $\mathcal{E}$ is called* fully homomorphic encryption *(FHE) scheme, if it is correct for every algebraic circuit. Alternatively, we*

*can base our construction over Boolean circuits, because both computational models are equivalent. If the scheme can deal with a restricted class of circuits, but not every one, then we call the scheme a* somewhat homomorphic encryption *(SHE) scheme.*

A cryptosystem is secure against *chosen ciphertext attack* (CCA2) if there is no polynomial time adversary $\mathcal{A}$ that can win the following game with non negligible probability.

**Setup.** The challenger obtains $(\mathrm{sk}, \mathrm{pk}) = \textsc{KeyGen}(\lambda)$ and sends $\mathrm{pk}$ to adversary $\mathcal{A}$.

**Queries.** $\mathcal{A}$ sends ciphertexts to the challenger, before or after the challenge. The challenger returns the corresponding plaintexts.

**Challenge.** The adversary randomly generates two plaintexts $m_0, m_1 \in \mathcal{P}$ and sends them to the challenger, who chooses randomly a bit $b \in \{0, 1\}$ and computes the ciphertext $c = \textsc{Enc}_{\mathrm{pk}}(m_b)$. The challenger sends $c$ to $\mathcal{A}$.

**Answer.** $\mathcal{A}$ sends a bit $b'$ to the challenger and wins the game if $b' = b$.

If we allow queries only before the challenge, we say that the cryptosystem is secure against CCA1 adversaries (lunchtime attacks). As previously described, queries can be interpreted as access to a decryption oracle. If instead we only allow access to an encryption oracle, i.e., the adversary can choose any message that is distinct from $m_0$ and $m_1$ to be encrypted under the same key pair, then we say that the cryptosystem is secure against *chosen plaintext attacks* (CPA).

In homomorphic encryption, it is impossible to achieve CCA2 security, because the adversary can add an encryption of zero to the encrypted challenge, or multiply it by the encryption of one, and send it to the decryption oracle, which allows him to trivially win the game. Many FHE schemes have as public value an encryption of the private key bits, which can be sent to the decryption oracle before the challenge, which makes such schemes insecure against CCA1 adversaries. Indeed, a *key recovery* attack is stronger than a CCA1 attack and Loftus et al [LMSV12] showed that Gentry's construction over ideal lattices is vulnerable to it and presented the only SHE proposal that is known to be CCA1 secure.

Recently [CT14], Chenal and Tang showed that many SHE schemes are not CCA1 by presenting a key recovery attack. The aim of this paper is to consider such attacks in the setting of NTRU-based schemes.

From now on we are going to work over the cyclotomic ring $R_q = \mathbb{Z}_q[x]/(x^d+1)$, where $d$ is a power of 2. Cyclotomic rings were introduced to lattice-based cryptography in [HPS98], and have been very popular since the breakthrough work of Lyubashevsky et al [LPR13]. Lattices constructed using such rings are often called *ideal lattices*. Although there is no proof that ideal lattices maintain the same security guarantees as conventional lattices, no significant improvement in the complexity of algorithms for computational problems in ideal lattices is known.

## 3 Previous Constructions

We can divide homomorphic encryption schemes as in Figure 1. In the first column, we have the schemes that are based on integers, which are simpler to understand. Lattice-based constructions are separated in four categories: the initial schemes, that still depend on the Sparse Subset Sum Problem (SSSP); Brakerski-Gentry-Vaikuntanathan (BGV)-like proposals, that bring new concepts and allow better constructions in practice; asymptotically better constructions that are based on the *approximate eigenvector* method, and NTRU-based schemes, that permit to obtain ciphertexts that correspond to just one ring element, simplifying previous schemes. NTRU-based SHE offers the possibility of encoding integers in a natural way, that can be used to solve practical problems such as statistical applications [LLAN14, BLN14].

In the literature [ZPS12, LMSV12, CT14] there are adaptive key recovery attacks on many schemes and these schemes were adapted and optimized later; thus, such constructions should be assessed in order to verify whether the attacks are still feasible. Table 1 shows which schemes

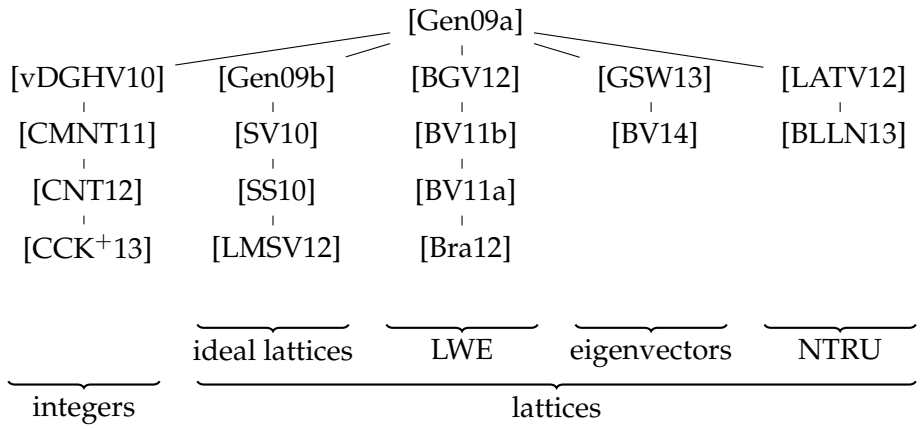


**Fig. 1.** Homomorphic Encryption Proposals

have been attacked by each of the previously cited works, showing also which schemes seem to be vulnerable to the same kind of attacks. Although some of them were not directly attacked, the key generation and decryption algorithms are so close to the attacked schemes, that the same strategy can be followed to compute the private key using decryption oracles.

| Attack | Schemes | Seems to extend to |
|---|---|---|
| [ZPS12] | [vDGHV10, CMNT11] | [CNT12] |
| [LMSV12] | [Gen09b, SV10, GS11] | [SS10] |
| [CT14] | [vDGHV10, BGV12, BV11b, BV11a, Bra12, GSW13] | [BV14] |
| this work | [LATV12, BLLN13] | - |
| no attack | [LMSV12] | - |

**Table 1.** Key recovery attacks

## 4 NTRU-based Somewhat Homomorphic Encryption

NTRU [HPS98] is an efficient lattice-based cryptographic scheme but, for many years, the lack of security proofs, reducing its security to worst-case hard lattice problems, was a serious concern. Stehlé and Steinfeld [SS11] presented such a proof, replacing the original ring $\mathbb{Z}_q[x]/(x^d - 1)$ by the previously described cyclotomic ring $R_q = \mathbb{Z}_q[x]/(x^d + 1)$, where $d$ is restricted to a power of 2.

In 2012, López-Alt, Tromer and Vaikuntanathan [LATV12] proposed the construction of *multikey fully homomorphic encryption*, which we call the LTV scheme. The difference here is that users with distinct keys can compute ciphertexts that will be processed by a server in order to obtain the homomorphic evaluation of a determined function. It means that all the users together will be able to decrypt the function evaluation and this strategy can be followed to construct a multiparty computation scheme. Doröz, Hu and Sunar [DHS14] implemented the LTV scheme. They implemented also the homomorphic evaluation of AES, showing that it offers advantages against the BGV scheme [BGV12].

However, the LTV scheme is based on non-standard assumptions. In 2013, a scale-invariant NTRU-based scheme was proposed by Bos et al [BLLN13]. We call it the BLLN scheme. The basic scheme, $\mathcal{E}_{\text{basic}}$, can be described as follows:

**Definition 3.** ***Setup.*** *Given the security parameter $\lambda$ construct the ring $R = \mathbb{Z}[x]/(x^d + 1)$, where $d$ is a power of two. Define $R_q = R/(q) \cong \mathbb{Z}_q[x]/(x^d + 1)$. Choose a small integer $t$, real numbers $\sigma_k$ and $\sigma_e$ and a prime $q$ such that $t, \sigma \ll q$. Let $\mathcal{D}_{\text{key}}$ and $\mathcal{D}_{\text{err}}$ be distributions on $R$ coming from discrete Gaussians on $\mathbb{Z}$ with standard deviations $\sigma_k$ and $\sigma_e$ respectively. The* SETUP *algorithm returns $(t, d, q, \mathcal{D}_{\text{key}}, \mathcal{D}_{\text{err}})$.*

***Key generation.*** *Given the output of the* SETUP *algorithm, sample polynomials $f', g \leftarrow \mathcal{D}_{\text{key}}$ and compute $f = [tf' + 1]_q$. Check that $f$ is invertible modulo $q$, if not choose a new $f'$. Compute the inverse $f^{-1} \in R_q$ and set $h = [tgf^{-1}]_q$. The public key is $pk = h$ and the private key is $sk = f$. Algorithm* KEYGEN *returns $(sk, pk)$.*

***Encryption.*** *The plaintext space is $R/tR$, so a message is given by a coset $m + tR$. Let $[m]_t$ be a canonical representative element of the coset. Sample $s, e \leftarrow \mathcal{D}_{\text{err}}$ and compute the ciphertext*

$$c = \text{ENC}_{pk}(m) = \left[\lfloor q/t \rfloor [m]_t + te + hs\right]_q .$$

***Decryption.*** *Compute*

$$m = \text{DEC}_{sk}(c) = \left[\lfloor (t/q).[fc]_q \rceil\right]_t .$$

*Return the message $[m]_t$.*

Given the integers $t$ and $q$ returned by the SETUP algorithm, the plaintext space is given by $R/tR$, while the ciphertext space is given by $R/qR$. Note that $t \ll q$. Indeed, the last condition is important to enable as many multiplications as possible. Thus, if $t$ grows when compared to a fixed $q$, then we would be able to execute fewer multiplications. Although the multiplicative depth of a homomorphic encryption scheme is an important issue, it is not relevant for the attacks we are going to present. Hence, we omit further details and we assume that the inequalities relating $t$ and $q$ in Lemma 1 are respected.

The security of this scheme is based on an analysis from Gentry et al [GHS12], which in turn used parameters presented in the work of Lindner and Peikert [LP11], showing that the scheme is secure as long as the LWE problem parameters $d, q, \sigma$ obey the inequality

$$d > \log\left(\frac{q}{\sigma}\right)\frac{\lambda + 110}{7.2}.$$

When applied with homomorphic schemes, this relation acquires a challenging aspect. As the standard deviation increases, fewer homomorphic operations can be evaluated, since a larger initial noise would be rapidly propagated. Thus, the ratio $q/\sigma$ determines the LWE-based cryptography security.

The distribution $\mathcal{D}_{\text{key}}$ must be chosen according to the description of Stehlé and Steinfeld [SS11], such that the public key is close enough to the uniform distribution, so that it reveals almost nothing about the private key. Rigorously, it reveals only a negligible fraction of the secret. Thus, $\mathcal{D}_{\text{key}}$ is a discrete Gaussian on $R_q$ with standard deviation at least $(d\sqrt{\log 8dq})q^k$, for $k$ in the interval $(1/2, 1)$. Furthermore, $\mathcal{D}_{\text{err}}$ is a $\omega(\sqrt{d \log(d)})$-bounded Gaussian distribution. In our attacks we may assume that $q$ is very large in comparison with $t$ and $\sigma_k$.

## 5 Adaptive Key Recovery Attacks

In a key recovery attack, we submit appropriately chosen ciphertexts to a decryption oracle in order to compute the private key. Once the private key is computed, then any ciphertext can later be decrypted. Consequently, a key recovery attack is stronger than a CCA1 attack.

### 5.1 Attacking the BLLN Scheme for $t > 2$ and Ternary $f'$

In the original paper [BLLN13], Bos et al stated that we can choose $f'$ and $g$ with coefficients in $\{-1, 0, 1\}$. We call this "ternary $f'$". We now show that in this case, and when $t > 2$, we can easily compute $f'$ using just one query to the decryption oracle. Recall that $f'[i]$ is the $i$-th coefficient of the polynomial $f'$.

**Lemma 1.** *Let $f = tf' + 1$ where $f'$ has coefficients in $\{-1, 0, 1\}$. Suppose $t \geq 3$ and $6(t^2 + t) < q$. Then,*

$$[\lfloor (t/q)[f[i]\lfloor q/t^2 \rfloor]_q \rceil]_t = f'[i].$$

*Proof.* Let $\lfloor q/t^2 \rfloor = q/t^2 - \epsilon$ for some $0 \leq \epsilon < 1$. Then,

$$f[i]\lfloor q/t^2 \rfloor = (tf'[i] + 1)(q/t^2 - \epsilon) = f'[i](q/t) + (q/t^2) - \epsilon(tf'[i] + 1)$$

and $[f[i]\lfloor q/t^2 \rfloor]_q = f[i]\lfloor q/t^2 \rfloor - vq$ for some $v \in \mathbb{Z}[x]$. Finally,

$$[\lfloor (t/q)[f[i]\lfloor q/t^2 \rfloor]_q \rceil]_t = [f'[i] + \lfloor 1/t - \epsilon(t^2 f'[i] + t)/q \rceil - vt]_t = [f'[i]]_t$$

since the entries of the polynomial $1/t - \epsilon(t^2 f' + t)/q$ all have absolute value $< 1/3 + 1/6 = 1/2$ (the bound $|t^2 f'[i] + t|/q \leq |t^2 + t|/q < 1/6$ is used here). □

We introduce the informal notation $a \ll b$ to mean that $b$ is much bigger than $a$ (say, $b > 10^6 a$ for parameters in actual cryptosystems). Hence we can observe that $t^2 \ll q$ and so $\lfloor q/t^2 \rfloor$ is a very large integer.

**Theorem 1.** *Let $t > 2$ and $6(t^2+t) < q$. Let $m_f = \text{DEC}(\lfloor q/t^2 \rfloor)$ be a polynomial in $R$ with coefficients in $[-t/2, t/2]$, where $\lfloor q/t^2 \rfloor$ is a constant integer polynomial that can easily be computed using the public parameters $q$ and $t$. Then we have that $f = tm_f + 1$.*

*Proof.* We have that $\text{DEC}(\lfloor q/t^2 \rfloor) = [\lfloor (t/q)[f(\lfloor q/t^2 \rfloor)]_q \rceil]_t$. Because we are multiplying $f$ by a constant polynomial, each coefficient of $f$ is multiplied by $\lfloor q/t^2 \rfloor$. By Lemma 1 we obtain an element in $R$ with coefficients in $\{-1, 0, 1\}$ that equals $f' \in R$. □

Note that the restriction $t > 2$ is a requirement for Lemma 1, but there is also a second reason why it is important. Because $-1 \equiv 1 \pmod 2$, we can't distinguish between $-1$ and $1$ from information modulo 2. Therefore, when $t = 2$ it will be necessary to provide an algorithm to find out the sign of each coefficient.

Algorithm 5.1 uses the ideas described above. We emphasize that the attack is very fast, since it needs to perform just one query to the decryption oracle. Also, the ciphertext that we submit to the decryption oracle is trivial to construct, and the final computation is also very easy.

**Algorithm 5.1** BLLN Attack for Ternary Polynomials when $t > 2$ and Ternary $f'$

**Require:** The public parameters $(q, d, t)$.
**Ensure:** The private key $f$.
$m_f = \text{DEC}(\lfloor q/t^2 \rfloor)$.
**return** $f = tm_f + 1$.

### 5.2 Attacking the BLLN Scheme for General $f'$ and $t > 2$

We now consider the case where $f'$ is chosen from $\mathcal{D}_{\text{key}}$ and so has a wider range of possible values. The idea is to make queries on ciphertexts $c_k = \lfloor q/(kt^2) \rfloor$ for various values $k > 1$ to learn information about $[\frac{1}{k} f'] \pmod t$.

**Lemma 2.** *Let $f = tf' + 1$ where $f'$ is a polynomial whose entries are integers bounded in absolute value by $B$ such that $B^2 < q/(36t^2)$. Let $0 \le i < d$. Let $k_{\max,i} \le 2B$ be the maximal integer such that the i-th coefficient of the decryption of ciphertext $\lfloor q/(k_{\max,i} t^2) \rfloor$ is non-zero. Then, we have that, for all $0 \le i < d$,*

$$|f'[i]| = \lfloor (k_{\max,i} + 1)/2 \rfloor.$$

*Proof.* The proof is similar to the proof of Lemma 1. Write $c_k = \lfloor q/(kt^2) \rfloor = q/(kt^2) - \epsilon$ for $0 \le \epsilon < 1$, and note that

$$[f c_k]_q = \tfrac{q}{kt^2}(tf' + 1) - \epsilon(tf' + 1) - vq$$

for some $v \in \mathbb{Z}[x]$. Then,

$$u = \tfrac{t}{q}[f c_k]_q = \tfrac{1}{k} f' + \tfrac{1}{kt} - \epsilon t(tf' + 1)/q - vt$$

is a polynomial with rational coefficients.

We now consider rounding the coefficients of the polynomial $u(x)$ to the nearest integer. For $i > 0$ we have $u[i] = \frac{1}{k} f'[i] - v[i]t$ and so

$$\lfloor u[i] \rceil = \lfloor \tfrac{1}{k} f'[i] \rceil - v[i]t.$$

It follows that the result of the decryption query is $[\lfloor u[i] \rceil]_t = [\lfloor \frac{1}{k} f'[i] \rceil]_t$. Note that if $k > 2B \ge 2|f'[i]|$, then $|\frac{1}{k} f'[i]| < 1/2$ and so the rounded value is zero.

If $k$ is maximal, then $\lfloor \frac{1}{k} f'[i] \rceil \ne 0$ but $\lfloor \frac{1}{k+1} f'[i] \rceil = 0$, and so

$$|\tfrac{1}{k} f'[i]| \ge \tfrac{1}{2} \quad \text{and} \quad |\tfrac{1}{k+1} f'[i]| \le \tfrac{1}{2}.$$

It follows that

$$\tfrac{k}{2} \le |f'[i]| \le \tfrac{k+1}{2}.$$

It remains to deal with the coefficient $f'[0]$, which has an additional error term $\frac{1}{kt} - \epsilon^\star$ where $\epsilon^\star = \epsilon t(tf' + 1)/q$ is added to it. Note that, since $q \gg t(tB + 1)$ and $t > 2$, we have $|\epsilon^\star| \ll 1$. However, we cannot ignore the error as we are adding it to the rational number $\frac{1}{k} f'[0]$. By the same argument as above, we compute

$$|\tfrac{1}{k} f'[0] + \tfrac{1}{kt} - \epsilon^\star| \ge \tfrac{1}{2} \quad \text{and} \quad |\tfrac{1}{k+1} f'[0] + \tfrac{1}{(k+1)t} - \epsilon^\star| \le \tfrac{1}{2}.$$

It follows that

$$\tfrac{k}{2} \le |f'[0] + \tfrac{1}{t} - k\epsilon^\star| \quad \text{and} \quad |f'[0] + \tfrac{1}{t} - (k+1)\epsilon^\star| \le \tfrac{k+1}{2}.$$

Since $(k+1)\epsilon^\star < 3Bt^2 2B/q \le 1/6$ and $1/t \le 1/3$ we see there is no rounding error. This completes the proof. □

Note that if $t = 2$ and $k = 1$, then we must be careful about what happens with the independent coefficient, as will be the case in the next section. However, when $t > 2$ we have that if $\lfloor \frac{1}{k} f'[i] \rceil \equiv 1 \pmod{t}$, then $f'[i]$ is positive, while if $\lfloor \frac{1}{k} f'[i] \rceil \equiv -1 \pmod{t}$, then $f'[i]$ is negative, which allows us to completely determine the private key since we know the absolute value and the sign of each coefficient.

The attack is then straightforward. Using binary search and queries to the decryption oracle one can determine $k_{\max,i}$ for $0 \leq i < d$ and hence learn all coefficients. To see that binary search is applicable, note that $|f'[i]| \leq B$ and so $|\frac{1}{2B} f'[i]| \leq 1/2$ and so decryption will generally return 0 for that coefficient. One can then query using $k = B$, and noting that $|\frac{1}{B} f'[i]| \leq 1$ and so the output of decryption is either 0 or $\pm 1$. If the output is $\pm 1$ then $\frac{B}{2} \leq |f'[i]| \leq B$ and one can try $k = (B + 2B)/2 = 3B/2$, while if the output is 0 then $|\frac{1}{B} f'[i]| \leq 1/2$ and one can try $k = B/2$, giving $|\frac{1}{k} f'[i]| \leq 1$, and so on. We give the details as Algorithm 5.2.

**Algorithm 5.2** BLLN Attack for General Polynomials when $t > 2$

**Require:** The public parameters $(q, d, t)$.
**Ensure:** The private key $f$.
  Let $B$ be the largest possible coefficient of $f$.
  **for** $i = 1$ till $d$ **do**
    Use binary search to find $1 \leq k_{\max,i} \leq 2B$ satisfying the condition of Lemma 2.
    $f'[i] = [\text{DEC}(q/(k_{\max,i} t^2))[i] . \lfloor (k_{\max,i} + 1)/2 \rfloor]_q$.
  **return** $f = tf' + 1$.

The total number of decryption oracle queries, if the algorithm is implemented naively, is $d\lceil \log_2(B) \rceil$. However, this can be improved somewhat by recycling previous oracle values and sub-dividing intervals into $t$ sub-intervals (resulting in $\log_t(B)$ steps in the search) instead of binary splitting and $\log_2(B)$ steps.

### 5.3 Attacking the BLLN Scheme for $t = 2$

If $t = 2$ we can proceed as in Section 5.2, but our main problem is to find out the sign of each coefficient. Of course, if $f$ is a valid private key then so is $-f$, so we only need to compute $f$ up to a global choice of sign.

Going back to the case of ternary polynomials, we can detect with a single decryption query when the coefficients of $f'$ are zero. But we cannot distinguish when they are 1 or $-1$, because we are operating modulo 2.

The idea is to make decryption queries to ciphertexts of the form $c = \lfloor q/(t^2 k) \rfloor (1 + x^j)$ for suitably chosen $k$ and $j$. We then get information about $\frac{1}{k} f'(1 + x^j)$. The point is that the $i$-th coefficient of $f'(1 + x^j)$ is the sum of $f'[i]$ and $f'[i - j \pmod{d}]$. If the coefficients $f'[i]$ and $f'[i - j]$ are both non-zero then they either cancel to zero or add to $\pm 2$. Hence, taking $k = 2$ we can determine the signs of coefficients relative to each other. By fixing one non-zero coefficient as a "base", we can deduce the sign of all other non-zero coefficients relative to this (as before, we leave the constant coefficient to the end of the algorithm).

When $f'$ is ternary then the details are simple. When $f'$ has general coefficients then the trick is to balance the sizes of coefficients so that cancellation to zero still takes place. So suppose we have run Algorithm 5.2 and determined each coefficient (except perhaps the constant coefficient) $f'[i]$ up to sign. Suppose without loss of generality that $f'[1]$ is non-zero. We will use this as our "base". For each $i$ such that $f'[i]$ is non-zero, we consider the ciphertext

$$c = \lfloor q/(2t^2 |f'[1]| \cdot |f'[i]|) \rfloor (|f'[1]| + x^{i-1} |f'[i]|).$$

The $i$-th coefficient of the decryption of this ciphertext will be

$$\frac{1}{|f'[1]|\cdot|f'[i]|}\left(|f'[1]|\cdot f'[i]+|f'[i]|\cdot f'[1]\right).$$

Hence, if the signs are opposite, then we get a 0 and if the signs are equal, the coefficient is $\pm 1$, which modulo $t=2$ becomes 1. It follows that multiplying the absolute value by the term $(2\text{DEC}(c)-1)$ gives us the desired result.

**Algorithm 5.3** BLLN Attack for $t=2$

**Require:** The absolute value $|f'|$, and the public parameters $(q,d)$.
**Ensure:** The private key $f$.
  Run the main part of Algorithm 5.2 to determine $|f'[i]|$ for all $0\le i<d$.
  Let $i_0$ be the smallest integer $i>0$ such that $f'[i]\neq 0$.
  $f'[i_0]=|f'[i_0]|$.
  **for** $i=i_0+1$ till $d$ **do**
    **if** $|f'[i]|>0$ **then**
      Let $c_{i,i_0}=\lfloor q/(2t^2|f'[i_0]|\cdot|f'[i]|)\rfloor(|f'[i_0]|+x^{i-i_0}|f'[i]|)$.
      $f'[i]=(2.\text{DEC}(c_{i,i_0})[i]-1).|f'[i]|$.
  Find three candidate values for $f'[0]$ and test the three possible values for $f$ using $h$
  **return** $f=tf'+1$.

Therefore, after calling algorithm 5.2, we must use algorithm 5.3 to determine the sign of each coefficient of the private key. But we still have to solve the problem of the independent coefficient, mentioned in last section. As we have seen, the term $1/t-\epsilon^\star$ can change the result of rounding to the nearest integer. For instance, considering the case of ternary $f'$ and $t=2$, then we have that $k=1$ and in the case that $f'[0]=-1$, we have that

$$[\lfloor -1+1/2+\epsilon^\star\rceil]_t=0$$

and the decryption oracle returns 0 instead of 1 as expected. Then we have to distinguish between two cases: $f'[0]=-1$ and $f'[0]=0$. But since we have arbitrarily chosen the sign of $f[i_0]$ as positive, then we must check also the case $f[0]=1$. Hence we have three candidates for $f'$. We can check which of them satisfies the requirement that $(tf'+1)h$ in $R_q$ is a polynomial with small coefficients. This completes the attack.

There are at most $d-1$ additional decryption oracle queries to determine the sign.

### 5.4 Attacking the LTV Scheme

In this section we assume that $q$ is odd. The LTV scheme is extremely similar to the BLLN scheme. The two schemes are based on the same algebraic structure, and the key generation algorithms are essentially the same, with the only difference that LTV is restricted to the case $t=2$. The LTV scheme is not scale-invariant, leading to simpler algorithms. Our focus is the decryption algorithm, so we explain this now.

**Decryption.** Compute $m=[fc]_q$. Output $m \pmod 2$.

The paper [LATV12] is vague about the exact computation of the decryption algorithm. The value $m$ is a polynomial in $R_q$ with small coefficients, so it is natural to interpret it as an element of $R=\mathbb{Z}[x]/(x^d+1)$. The ambiguity comes in the next step. Does $m \pmod 2$ mean only the constant term of the polynomial modulo 2, or the whole polynomial reduced modulo

2? In our attack we assume the latter case. The former case can be reduced to the latter case by replacing a decryption query on $c$ by $d$ decryption queries on $cx^i$ for $0 \leq i < d$.

The attack is therefore seen to be more-or-less identical to the attack in the previous section. Let $k \geq 1$ be an integer and consider the ciphertext $c_k = 2\lfloor q/(4k) \rfloor$. Lemma 3 shows why we can compute $f'$ using the same strategy as before.

**Lemma 3.** *Let $c_k = 2\lfloor q/(4k) \rfloor$. Let $k^\star_{\max,i}$ be the maximal integer such that $\text{DEC}(c_{k^\star_{\max,i}})[i]$ is non-zero. Then we have that $f[i]$ is given by $k^\star_{\max,i} + 1$.*

*Proof.* First note that $c_k$ is an even integer and so $(2f'+1)c_k$ is an integer polynomial with even coefficients.

For $k \geq 1$ we have that $c_k = q/(2k) - \epsilon$ for some $0 \leq \epsilon < 2$, and decryption of $c_k$ first computes

$$(2f' + 1)c_k = f'(q/k - 2\epsilon) + 2\lfloor q/(4k) \rfloor.$$

Note that $q/k - 2\epsilon$ is an even integer. Thus, if $k$ is big when compared to $f'[i]$, reduction by $q$ does not change the value, then after reducing by 2 we get zero. If $f'[i] \geq k$ then $f'[i](q/k) \geq q$ and so, as long as the error term is small enough, $f'[i](q/k - 2\epsilon) - q$ is odd. It follows that $[fc_k]_q \pmod 2$ is odd and so the condition $f'[i] > k$ can be tested using a decryption oracle query. Hence, we proceed using the same method as before. One chooses maximal $k^\star_{\max,i}$ such that $f'[i] > k^\star_{\max,i}$ and hence determines the value of $|f'[i]|$. For instance, we have that $|f'[i]| = k^\star_{\max,i} + 1$. The signs and the independent coefficient are handled in the same way as above. □

**Algorithm 5.4** LTV Attack

**Require:** The public parameters $(q, d, t)$.
**Ensure:** The absolute value of the private key $f$.
Let $B$ be the largest possible coefficient of $f$.
**for** $i = 1$ till $d$ **do**
Use binary search to find $1 \leq k^\star_{\max,i} \leq 2B$ satisfying the condition of Lemma 3.
$|f[i]| = [(k^\star_{\max,i} + 1)]_q$.
**return** $f$.

## 6 Concluding Remarks

We have described adaptive key recovery attacks on NTRU-based SHE schemes. Other families of SHE schemes, as represented in Figure 1, are also vulnerable to this kind of attack, showing that CCA1 security is hard to achieve in homomorphic encryption. Adaptive key recovery attacks on homomorphic encryption seem to be realistic in certain scenarios, so they are potentially a serious problem in practice. The only homomorphic encryption scheme known to resist such attacks is the scheme by Loftus et al [LMSV12].

## Acknowledgements

We thank Qiang Tang and the anonymous referees for helpful comments.

## References


BGV12. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) Fully homomorphic encryption without bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, pages 309–325, New York, NY, USA, 2012. ACM.

BLLN13. J. W. Bos, K. Lauter, J. Loftus, and M. Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In Martijn Stam, editor, *IMA Int. Conf.*, volume 8308 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2013.

BLN14. J. W. Bos, K. Lauter, and M. Naehrig. Private predictive analysis on encrypted medical data. *Journal of Biomedical Informatics*, 50:234–243, 2014.

Bra12. Z. Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In *Advances in Cryptology - Crypto 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886. Springer, 2012.

BV11a. Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the 2011 IEEE 52Nd Annual Symposium on Foundations of Computer Science*, FOCS '11, pages 97–106, Washington, DC, USA, 2011. IEEE Computer Society.

BV11b. Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Proceedings of the 31st Annual Conference on Advances in Cryptology*, CRYPTO'11, pages 505–524, Berlin, Heidelberg, 2011. Springer-Verlag.

BV14. Z. Brakerski and V. Vaikuntanathan. Lattice-based FHE as secure as PKE. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 1–12, New York, NY, USA, 2014. ACM.

CCK+13. J. Cheon, J. Coron, J. Kim, M. Lee, T. Lepoint, M. Tibouchi, and A. Yun. Batch fully homomorphic encryption over the integers. In T. Johansson and P. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 315–335. Springer Berlin Heidelberg, 2013.

CMNT11. J. Coron, A. Mandal, D. Naccache, and M. Tibouchi. Fully homomorphic encryption over the integers with shorter public keys. In *Proceedings of the 31st annual conference on Advances in cryptology*, CRYPTO'11, pages 487–504, Berlin, Heidelberg, 2011. Springer-Verlag.

CNT12. J. Coron, D. Naccache, and M. Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 446–464. Springer Berlin Heidelberg, 2012.

CT14. M. Chenal and Q. Tang. On key recovery attacks against existing somewhat homomorphic encryption schemes. In *Latincrypt (to appear)*, Florianópolis-SC, Brazil, 2014.

DHS14. Y. Doröz, Y. Hu, and B. Sunar. Homomorphic AES evaluation using NTRU. Cryptology ePrint Archive, Report 2014/039, 2014. `http://eprint.iacr.org/`.

Gen09a. C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `crypto.stanford.edu/craig`.

Gen09b. C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 169–178, New York, NY, USA, 2009. ACM.

GHS12. C. Gentry, S. Halevi, and N. P. Smart. Homomorphic evaluation of the AES circuit. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 850–867. Springer Berlin Heidelberg, 2012.

GS11. C. Gentry and Halevi S. Implementing gentry's fully-homomorphic encryption scheme. In Kenneth Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 129–148. Springer Berlin / Heidelberg, 2011.

GSW13. C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer Berlin Heidelberg, 2013.

HPS98. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer Berlin Heidelberg, 1998.

LATV12. A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 1219–1234, New York, NY, USA, 2012. ACM.

LLAN14. K. Lauter, A. Lopez-Alt, and M. Naehrig. Private computation on encrypted genomic data. Technical Report MSR-TR-2014-93, June 2014.

LMSV12. J. Loftus, A. May, N. P. Smart, and F. Vercauteren. On CCA-secure somewhat homomorphic encryption. In A. Miri and S. Vaudenay, editors, *Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 55–72. Springer Berlin Heidelberg, 2012.

LP11. R. Lindner and C. Peikert. Better key sizes (and attacks) for LWE-based encryption. In *Proceedings of the 11th International Conference on Topics in Cryptology*, CT-RSA'11, pages 319–339, Berlin, Heidelberg, 2011. Springer-Verlag.

LPR13. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43, 2013.

RAD78. R. L. Rivest, L. Adleman, and M. L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation, Academia Press*, pages 169–179, 1978.

SS10. D. Stehlé and R. Steinfeld. Faster fully homomorphic encryption. In M. Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 377–394. Springer Berlin Heidelberg, 2010.

SS11. D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 27–47, 2011.

SV10. N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 420–443. Springer Berlin Heidelberg, 2010.

vDGHV10. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In *Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'10, pages 24–43, Berlin, Heidelberg, 2010. Springer-Verlag.

ZPS12. Z. Zhang, T. Plantard, and W. Susilo. On the CCA-1 security of somewhat homomorphic encryption over the integers. In *Proceedings of the 8th International Conference on Information Security Practice and Experience*, ISPEC'12, pages 353–368, Berlin, Heidelberg, 2012. Springer-Verlag.