Fractional LWE: a nonlinear variant of LWE

Gerald Gavin[1] and Stephane Bonnevay[2]

[1] Laboratory ERIC - University of Lyon
gerald.gavin@univ-lyon1.fr

[2] Laboratory ERIC - University of Lyon
stephane.bonnevay@univ-lyon1.fr

Abstract. Many cryptographic constructions are based on the famous problem LWE [Reg05]. In particular, this cryptographic problem is currently the most relevant to build FHE [GSW13], [BV11]. In [BV11], encrypting x consists of randomly choosing a vector $\boldsymbol{c}$ satisfying $\langle \boldsymbol{s}, \boldsymbol{c} \rangle = x + \mathsf{noise} \pmod{q}$ where $\boldsymbol{s}$ is a secret size-n vector. While the vector sum is a homomorphic operator, such a scheme is intrinsically vulnerable to lattice-based attacks. To overcome this, we propose to define $\boldsymbol{c}$ as a pair of vectors $(\boldsymbol{u}, \boldsymbol{v})$ satisfying $\langle \boldsymbol{s}, \boldsymbol{u} \rangle / \langle \boldsymbol{s}, \boldsymbol{v} \rangle = x + \mathsf{noise} \pmod{q}$. This simple scheme is based on a new cryptographic problem intuitively not easier than LWE, called Fractional LWE (FLWE). While some homomorphic properties are lost, the secret vector $\boldsymbol{s}$ could be hopefully chosen shorter leading to more efficient constructions. We extensively study the hardness of FLWE. We first prove that the decision and search versions are equivalent provided q is a *small* prime. We then propose a lattice-based cryptanalysis showing that n could be chosen logarithmic in $\log q$ instead of polynomial for LWE.

1 Introduction

Many cryptographic constructions are based on the famous problem *Learning with Errors* (LWE) [Reg05]. Cryptographic work over the past decade has built many primitives based on the hardness of LWE. Today, LWE is known to imply essentially everything you could want from crypto (apart from a few notable exceptions as obfuscation). In particular, this cryptographic problem is currently the most relevant to build FHE [GSW13], [BV11]. LWE is known to be hard based on certain assumptions regarding the worst-case hardness of standard lattice problems such as GapSVP and SVP and no quantum attacks against this problem are known.

Typically, LWE deals with a secret vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ and an example $\boldsymbol{w}$ of LWE is a randomly chosen size-n vector satisfying[1] $\langle \boldsymbol{s}, \boldsymbol{w} \rangle = e \pmod{q}$ with $e \ll q$ being a randomly chosen noise value. The problem LWE consists of recovering $\boldsymbol{s}$ from a polynomial number of examples. This problem is equivalent to solve a SVP (Shortest Vector Problem) on a lattice of dimension n. The hardness of LWE holds ensuring that n is chosen sufficiently large, i.e. $\Omega(\log q)$.

[1] $\langle \boldsymbol{s}, \boldsymbol{c} \rangle$ denoting the scalar product between $\boldsymbol{s}$ and $\boldsymbol{c}$.

We propose here a nonlinear variant of LWE, called Fractional LWE (FLWE), hopefully less vulnerable to lattice-based attacks. For concreteness, an example of this new problem is a pair of randomly chosen vectors $\boldsymbol{w} = (\boldsymbol{u}, \boldsymbol{v})$ satisfying

$$\langle \boldsymbol{s}, \boldsymbol{u} \rangle / \langle \boldsymbol{s}, \boldsymbol{v} \rangle = e \pmod q$$

This problem does not intuitively seem easier than LWE and the same security level could be hopefully guaranteed in smaller dimension n. But can we quantify this? The main purpose of this paper is to extensively study this problem. Similarly to LWE, we reduce the search version to the decisional one (consisting distinguishing between m examples of FLWE and m randomly chosen vectors) provided q is a small prime (see Section 2). Then, we mainly propose two classes of lattice-based attacks. A typical lattice-based attack of the first class exploits the following equation

$$\langle \boldsymbol{s}, \boldsymbol{u} \rangle \cdot \langle \boldsymbol{s}, \boldsymbol{v} \rangle^{q-2} = e \pmod q$$

Indeed, by expanding the right term and by sampling sufficiently many examples $\boldsymbol{w}_i$, the noise values e_i and thus $\boldsymbol{s}$ can be recovered by solving a SVP. However, this attack fails by choosing q sufficiently large. The first class of lattice-based attacks is a generalization of this attack (see Section 3.4). We formally prove that this class does not contain any efficient attack for any choice of n provided q is sufficiently large.

We then consider a second class of lattice-based attacks exploiting polynomial equations between noise values (see Section 3.5). As the expanded representation size of the involved polynomials exponentially grows with n, it suffices to choose (provided the noise level is large enough to ensure that the noise values cannot be guessed with non-negligible probability)

$$n = \Omega(\log \log q)$$

(instead of $n = \Omega(\log q)$ for LWE) to ensure the inefficiency of these attacks.

In Section 4, we develop a very simple large plaintext encryption scheme whose security relies on FLWE. Typically, an encryption of $x \in \{0, \ldots, \xi - 1\}$ with $\xi \approx 2^\lambda$ is a pair of vectors $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$ satisfying

$$\langle \boldsymbol{s}, \boldsymbol{u} \rangle / \langle \boldsymbol{s}, \boldsymbol{v} \rangle = x + e\xi \pmod q$$

where e is uniform over $\{0, \ldots, \xi - 1\}$. We show that this encryption scheme is significantly more efficient that (large domain) LWE-based schemes to evaluate very short arithmetic circuits assuming the hardness of FLWE with $n = \Omega(\log \log q)$.

However, the homomorphic capabilities of our scheme are very limited due to the ciphertext expansion. Indeed, the ciphertext size polynomially (but not exponentially as we may intuitively think) grows with the number of arithmetic operations restricting evaluation to very short-size arithmetic circuits. However, very small arithmetic circuits can be evaluated very efficiently making this scheme relevant for some (cloud) applications. Can we concretely compare homomorphic performance of our scheme with the ones of LWE? In appearance, LWE seems better because one homomorphic addition only requires $O(n)$ while one homomorphic addition/multiplication requires $O(n^2)$ for our scheme. Nevertheless, one homomorphic multiplication also requires $O(n^2)$ for LWE meaning that these two schemes are equivalent in the worst case. Furthermore, n might be chosen significantly smaller in our scheme. This gives hope to improve existing LWE-based homomorphic encryption schemes. For instance, relinearization technics used in [BGV14] could be perhaps adapted to our scheme leading to more efficient homomorphic schemes. In Section 5, we propose a relinearization operator with some security guarantees under the factoring assumption. Further developments based on such operators could hopefully lead to noise-free FHE as very succinctly explained in Section 5.

Notation. *We use standard Landau notations. Throughout this paper, we let λ denote the security parameter: all known attacks against the cryptographic scheme under scope should require $2^{\Omega(\lambda)}$ bit operations to mount.*

- *The logarithm to base 2 is denoted by* log*.*
- *The cardinal of a set S will be denoted by $\#S$.*
- ’Choose at random $x \in X$*’ will systematically mean that x is chosen according to uniform probability distribution over X.*
- *Given two vectors $\boldsymbol{a} = (a_0, \dots, a_n)$ and $\boldsymbol{b} = (b_0, \dots, b_n)$, $\boldsymbol{a} \odot \boldsymbol{b} \overset{def}{=} (c_{ij})_{n \geq i \geq j \geq 0}$ with $c_{ii} = a_i b_i$ and $c_{ij} = a_i b_j + a_j b_i$ if $i > j$.*
- *Given a polynomial ϕ, the number of monomials of ϕ is denoted by $m(\phi)$. A polynomial is said to be null if it is identically zero, i.e. each coefficient of its expanded representation is equal to 0.*
- *A function ϕ is said to be rational if there exists a $\{+, -, \times, /\}$-circuit computing this function or equivalently if ϕ can be written as the ratio of two polynomials ϕ', ϕ''.*

Definition 1. *A rational function ϕ is said to be polynomial-degree if there exist two polynomial-degree polynomials ϕ', ϕ'' such that $\phi = \phi'/\phi''$.*

Remark 1. The number $M(n, m)$ of n-variate monomials of degree m is equal to $\begin{pmatrix} m+n-1 \\ n-1 \end{pmatrix}$. Fixing n, $M(n,m) = O(m^{n-1})$. This will be used in Section 4 to show that the ciphertext size polynomially grows with the number of homomorphic operations.

2 Fractional LWE

For positive integer n and $q \geq 2$, a vector $\boldsymbol{s} \in \{1\} \times \mathbb{Z}_q^n$ and a probability distribution χ on $\mathbb{Z}_q$, let $A_{\boldsymbol{s},\chi}$ be the distribution obtained by choosing at random a noise term $e \leftarrow \chi$ and two vectors $\boldsymbol{u}, \boldsymbol{v} \leftarrow \mathbb{Z}_q^{n+1}$ satisfying $\langle \boldsymbol{s}, \boldsymbol{u}\rangle / \langle \boldsymbol{s}, \boldsymbol{v}\rangle = e$ and outputting $(\boldsymbol{u}, \boldsymbol{v})$. For concreteness, $(\boldsymbol{u}, \boldsymbol{v})$ can be chosen as follows: $e \leftarrow \chi$, $(u_1, \ldots, u_n, v_0, \ldots, v_n)$ uniform over $\mathbb{Z}_q^{2n+1}$ and $u_0 := e \cdot \langle \boldsymbol{s}, \boldsymbol{v}\rangle - \sum_{i=1}^n s_i u_i$. Moreover, if $\langle \boldsymbol{s}, \boldsymbol{v}\rangle = 0$ (this happens with probability $1/q$) then this process is started again.

Definition 2. *For an integer $q = q(n)$, a distribution ψ over $\{1\} \times \mathbb{Z}_q^n$ and an error distribution $\chi = \chi(n)$ over $\mathbb{Z}_q$, the learning with errors problem $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ is defined as follows: given m independent samples from $A_{\boldsymbol{s},\chi}$ where $\boldsymbol{s} \leftarrow \psi$, output $\boldsymbol{s}$ with non-negligible probability.*

The (average-case) decision variant of the FLWE problem, denoted by $\mathsf{DFLWE}_{n,m,q,\chi,\psi}$ is to distinguish (with non-negligible advantage) m samples chosen according to $A_{\boldsymbol{s},\chi}$ from m samples chosen according to the uniform distribution over $\mathbb{Z}_q^{n+1} \times \mathbb{Z}_q^{n+1}$.

As done for LWE, we propose a reduction from FLWE to DFLWE ensuring that q is a prime polynomial in λ. The proof of the following proposition is largely inspired by the reduction from LWE to DLWE found in [Reg05]. However, we also need that the number m of samples is not too large, i.e. $m = O(q)$.

Lemma 1. *(Search to Decision). Assuming $m = O(q)$, there is a probabilistic polynomial-time reduction from solving $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ with overwhelming probability to solving $\mathsf{DFLWE}_{n,m,q,\chi,\psi}$ with overwhelming probability provided q is a small prime (polynomial in λ).*

Proof. We here assume that each example $(\boldsymbol{u}, \boldsymbol{v})$ is chosen as follows: $e \leftarrow \chi$, $(u_1, \ldots, u_n, \boldsymbol{v})$ uniform over $\mathbb{Z}_q^{2n+1}$ and $u_0 := e \cdot \langle \boldsymbol{s}, \boldsymbol{v}\rangle - \sum_{i=1}^n s_i u_i$. Our m examples $(\boldsymbol{u}_i, \boldsymbol{v}_i)_{i=1,\ldots,m}$ are thus generated according to the probability distribution considered in FLWE provided $\langle \boldsymbol{s}, \boldsymbol{v}_i\rangle \neq 0$ for any $i = 1, \ldots m$. This happens with non-negligible probability assuming $m = O(q)$.

Let $\mathcal{A}$ be a p.p.t. algorithm solving $\mathsf{DFLWE}_{n,m,q,\chi,\psi}$ with overwhelming probability. It is enough to give a polynomial-time method for checking whether the i^{th} coordinate $s_i \in \mathbb{Z}_q$ of $\boldsymbol{s} = (1, s_1, \ldots, s_n)$ is equal to a given value $\alpha \in \mathbb{Z}_q$ or not. By doing it for any $i \in \{1, \ldots, n\}$ and any $\alpha \in \mathbb{Z}_q$, one can recover $\boldsymbol{s}$ in polynomial-time (because q is assumed to be a polynomial prime). To decide whether $s_i = \alpha$ or not, it suffices to randomize each instance $(\boldsymbol{u}, \boldsymbol{v})$ as follows. We choose at random $r \in \mathbb{Z}_q$ and we output $(\boldsymbol{u}', \boldsymbol{v}')$ defined by

$$\begin{aligned} u'_0 &= u_0 + \alpha r \\ u'_i &= u_i - r \\ u'_j &= u_j \text{ for any } j \in \{1, \ldots, n\} \setminus \{i\} \\ \boldsymbol{v}' &= \boldsymbol{v} \end{aligned}$$

By construction, if $s_i = \alpha$, then $\langle \boldsymbol{s}, \boldsymbol{u}'\rangle / \langle \boldsymbol{s}, \boldsymbol{v}'\rangle = \langle \boldsymbol{s}, \boldsymbol{u}\rangle / \langle \boldsymbol{s}, \boldsymbol{v}\rangle = e$. It suffices then to prove that $(\boldsymbol{u}', \boldsymbol{v}')$ is uniformly drawn according to $\mathbb{Z}_q^{n+1} \times \mathbb{Z}_q^{n+1}$ when $s_i \neq \alpha$. Indeed, $(u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n, \boldsymbol{v})$ and thus $(u'_1, \ldots, u'_{i-1}, u'_{i+1}, \ldots, u'_n, \boldsymbol{v}')$ is uniform over $\mathbb{Z}_q^{2n}$. Fixing $(u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n, \boldsymbol{v})$, u_i can be chosen at random and $u_0 := b - s_i u_i$ with $b = e \cdot \langle \boldsymbol{s}, \boldsymbol{v} \rangle - \sum_{j \in \{1,\dots,n\} \setminus \{i\}} s_j u_j$. To prove that (u'_0, u'_i) is uniform over $\mathbb{Z}_q^2$, it suffices to notice that for any $(z_0, z_1) \in \mathbb{Z}_q^2$ there exists a unique pair (u_i, r) such that $u'_0 = z_0$ and $u'_i = z_1$. Indeed, provided $s_i \neq \alpha$, the system of the two following equations $-s_i u_i + \alpha r = z_0 - b$ and $u_i - r = z_1$ has a unique solution (u_i^*, r^*) (because the two equations are linearly independent provided $s_i - \alpha \neq 0$).

By transforming all the instances as described above, $\mathcal{A}$ can be used to decide (with overwhelming probability) whether $s_i = \alpha$ or not.

□

Challenging issues remain unresolved. For instance, can Lemma 1 be extended to large primes q or can worst-case be reduced to average?

3 Analysis of FLWE

3.1 Probability distributions χ, ψ

An example of $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ is a pair of vectors $\boldsymbol{w} = (\boldsymbol{u}, \boldsymbol{v})$ satisfying $\langle \boldsymbol{s}, \boldsymbol{u} \rangle / \langle \boldsymbol{s}, \boldsymbol{v} \rangle = e \pmod q$ where $\boldsymbol{s} \leftarrow \psi$ and $e \leftarrow \chi$. To simplify the analysis, we will only consider probability distributions χ which ensure that noise values e cannot be guessed.

Typically, χ refers to the uniform probability distribution over $\{0, \dots, \xi - 1\}$ and ψ refers to the uniform probability distribution over $\{1\} \times \mathbb{Z}_q^n$,

$$\xi \approx 2^{\lambda} < q$$
$$q \approx 2^{\delta\lambda}$$

3.2 Problem statement

Let $\boldsymbol{s}^* \leftarrow \psi$ and let $\boldsymbol{w}_1 = (\boldsymbol{u}_1, \boldsymbol{v}_1), \dots, \boldsymbol{w}_m = (\boldsymbol{u}_m, \boldsymbol{v}_m)$ be m examples of $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ drawn according to $A_{\boldsymbol{s}^*,\chi}$.

By rewriting the equations $\langle \boldsymbol{s}, \boldsymbol{u}_i \rangle / \langle \boldsymbol{s}, \boldsymbol{v}_i \rangle = e_i \pmod q$, we get the following polynomial system $\mathcal{F} = 0$ whose $(s_1 = s_1^*, \dots, s_n = s_n^*, x_1 = e_1, \dots, x_m = e_m)$ is a solution

$$\begin{cases} (u_{10} - x_1 v_{10}) + (u_{11} - x_1 v_{11}) s_1 + \cdots + (u_{1n} - x_1 v_{1n}) s_n = 0 \\ \cdots \\ (u_{m0} - x_m v_{m0}) + (u_{m1} - x_m v_{m1}) s_1 + \cdots + (u_{mn} - x_m v_{mn}) s_n = 0 \end{cases} \tag{1}$$

Let $X \subset \mathbb{Z}_q^{m+n}$ be the solution set of $\mathcal{F} = 0$. Throughout this section, $I_{\mathcal{F}}$ refers to the ideal generated by the family of polynomials $\mathcal{F}$ and I_X refers to the ideal of polynomials which are zero over X. By construction, $I_{\mathcal{F}} \subseteq I_X$ but it is well-known that the converse is not true in general.

This system is clearly underdefined (n variables can be freely chosen) and hence $\boldsymbol{s}^*$ cannot be recovered without taking into account the shortness of the variables e_i. Szepieniec et al. [SP17] have conjectured that this problem called *Short Solutions to Nonlinear Systems of Equations (SSNE)* is difficult. They identified two types of attacks (algebraic and lattice-based attacks).

3.3 Algebraic attacks

It is well-known that solving polynomial systems is $\mathcal{NP}$-hard. (ensuring that the degree of the polynomials is at least 2). To solve such systems, we classically compute a (lexicographic order) Groebner basis [BKW93] of $I_{\mathcal{F}}$ which consists of a set of univariate polynomials: this new set of (univariate) polynomial equations can be solved with Berkelamp's algorithm [BRS67]. Although the complexity of the best known algorithm to compute Groebner basis is (at least double) exponential, it is difficult to evaluate their running-time in practice. It mainly depends on the number of variables and the degree of the polynomials.

Nevertheless, this purely algebraic method cannot be applied here because the system $\mathcal{F} = 0$ (1) is underdefined[2]. Some polynomials, exploiting the fact that $\mathbb{Z}_q$ is a finite field or that $e_i \in \{0, \ldots, \xi - 1\}$, can be added to $\mathcal{F}$ in order to overdefine the system, i.e. $x_i^q - x_i$, $s_i^q - s_i$ or $\prod_{k \in \{0,\ldots,\xi\}} (x_i - k)$. However, the degree of these polynomials is large[3] making Groebner basis computations surely impracticable.

Finally, hybrid attacks consisting of guessing some variables in order to overdefine the system is not relevant here because q, ξ are assumed to be large.

3.4 The first class of lattice-based attacks

Typically, an example $\boldsymbol{w}$ of LWE satisfies $\langle \boldsymbol{s}, \boldsymbol{w} \rangle = e$ meaning that LWE is natively a lattice problem. Indeed, by considering sufficiently many examples $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t$, the vector noise $(e_1, \ldots, e_t)$ and thus $\boldsymbol{s}$ can be recovered by solving a SVP over the lattice spanned by the n vectors $\boldsymbol{\alpha}_i = (w_{1i}, \ldots, w_{ti})$.

An example of FLWE is pair of vectors $\boldsymbol{w} = (\boldsymbol{u}, \boldsymbol{v})$ s.t. $\langle \boldsymbol{s}, \boldsymbol{u} \rangle / \langle \boldsymbol{s}, \boldsymbol{v} \rangle = e$. By using $x^{-1} = x^{q-2} \pmod{q}$, we get the polynomial equation $\langle \boldsymbol{s}, \boldsymbol{u} \rangle \cdot \langle \boldsymbol{s}, \boldsymbol{v} \rangle^{q-2} = e \pmod{q}$ leading to a lattice-based attack. To highlight this, consider the case $q = 5$ and $n = 1$, i.e. $\boldsymbol{s} = (1, s)$. In this case, $(u_1 + su_2)(v_1 + sv_2)^3 = e$. By developing the right term, we get[4]

$$\sum_{i=0}^{4} s^i p_i(\boldsymbol{u}, \boldsymbol{v}) = e$$

where p_i is a degree-4 polynomial. It follows that $\boldsymbol{s}$ can be recovered by solving a SVP over a small dimension lattice. However, choosing a large prime q (exponential in λ) ensures that the dimension of the lattice is exponential. Nevertheless, one can imagine more efficient attacks based on the same idea. This section aims at formally proving the non-existence of such attacks.

Let us imagine that the attacker is able to recover functions $\varphi_1, \ldots, \varphi_\gamma$ such that there are constants (indexed by $\boldsymbol{s}$) $a_1, \ldots, a_\gamma \in \mathbb{Z}_q$ and a function ε satisfying

$$a_1 \cdot \varphi_1(\boldsymbol{w}) + \cdots + a_\gamma \cdot \varphi_\gamma(\boldsymbol{w}) = \varepsilon(\boldsymbol{w})$$

[2] For instance $s_1, \ldots, s_n$ can be chosen arbitrarily.

[3] not polynomial in the security parameter λ

[4] $u_1v_1^3 + s(u_2v_1^3 + 3u_1v_1^2v_2) + s^2(3u_2v_1^2v_2 + 3u_1v_1v_2^2) + s^3(u_1v_2^2 + 3u_2v_1v_2^2) + s^4(u_2v_2^3) = e.$

where $\varepsilon(\boldsymbol{w}) \ll q$. Note that this equality holds with $a_i = s_i$, $\varphi_i(\boldsymbol{w}) = w_i$ and $\varepsilon(\boldsymbol{w}) = e_i$ if $\boldsymbol{w}$ is a LWE example. By sampling sufficiently many instances $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t$, the coefficients $a_1, \ldots, a_\gamma$ can be recovered by solving an approximate-SVP. This is a relevant attack if $\boldsymbol{s}$ can be derived from the knowledge of $\varepsilon(\boldsymbol{w}_1), \ldots, \varepsilon(\boldsymbol{w}_t)$. This attack can be identified to the tuple $(\varphi_1, \ldots, \varphi_\gamma, \varepsilon)$. This is formally encapsulated in the following definition where the functions $\varphi_1(\boldsymbol{w}), \ldots, \varphi_\gamma(\boldsymbol{w})$ are rational and where $\varepsilon(\boldsymbol{w}) = p(e)$, p being a polynomial.

Definition 3. *Let $(\varphi_1, \ldots, \varphi_\gamma)$ be a (polynomial-size) tuple of polynomial-degree rational functions (see Definition 1) and let p be a non-constant polynomial-degree polynomial. We say that $(\varphi_1, \ldots, \varphi_\gamma, p)$ belongs to the class $\mathcal{C}$ if there exist functions $a_1, \ldots, a_t$ satisfying*

$$a_1(\boldsymbol{s}) \cdot \varphi_1(\boldsymbol{w}) + \ldots + a_\gamma(\boldsymbol{s}) \cdot \varphi_\gamma(\boldsymbol{w}) = p(e) \tag{2}$$

with non-negligible probability over the choices of $\boldsymbol{s}, \boldsymbol{w}$.

By considering sufficiently many examples $\boldsymbol{w}_i$ and by assuming that p is a small-degree polynomial with small coefficients, i.e. $p(e) \ll q$, the rational functions $\varphi_1, \ldots, \varphi_\gamma$ satisfying (2) can be used to recover $p(e_1), \ldots, p(e_t)$ and thus (hopefully) $e_1, \ldots, e_t$ and then $\boldsymbol{s}$.

Theorem 1. *$\mathcal{C}$ is empty*[5] *for any $n \geq 1$.*

Proof. See Appendix C.
□

Note that only polynomial-degree polynomials (or rational functions, see Definition 1) are considered in Definition 3. In order to remove such conditions, Zippel-Schwartz's Theorem can be replaced by Theorem 3 (see Appendix B) in the proof of Theorem 1. The price to pay would be the introduction of the factoring assumption.

3.5 Equations between noise values

The second way to investigate $\mathcal{F} = 0$ (1) consists of exploiting the fact that the noise values are relatively small *w.r.t.* q. However, $s_1^*, \ldots, s_n^*$ are not short and they should be eliminated in order to obtain a system of equations only dealing with $x_1, \ldots, x_n$. In other words, we are looking for polynomials $\phi \in I_X \cap \mathbb{Z}_q[X_1, \ldots, X_m]$. The computational methods to achieve this generally consists of searching polynomials in $\phi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$.

[5] There does not exist any lattice-based attack satisfying Definition 3

Case $\boldsymbol{n = 1}$. Let $\boldsymbol{s} = (1, s)$ and let $\boldsymbol{w} = (\boldsymbol{u}, \boldsymbol{v})$ and $\boldsymbol{w}' = (\boldsymbol{u}', \boldsymbol{v}')$ be two instances of FLWE. We can eliminate s by extracting s from the equations $\langle \boldsymbol{s}, \boldsymbol{u} \rangle = e \langle \boldsymbol{s}, \boldsymbol{v} \rangle$ and $\langle \boldsymbol{s}, \boldsymbol{u}' \rangle = e' \langle \boldsymbol{s}, \boldsymbol{v}' \rangle$, i.e. $s = (ev_1 - u_1)(u_2 - ev_2)^{-1} = (e'v'_1 - u'_1)(u'_2 - e'v'_2)^{-1} \pmod q$ leading to the equation

$$u_1 u'_2 - u'_1 u_2 + e(v_1 u'_2 - v_2 u'_1) + e'(u_1 v'_2 - v'_1 u_2) + ee'(v_1 v'_2 - v'_1 v_2) = 0 \quad (3)$$

This equation can be seen as a three-variate linear equation having a short solution (e, e', ee'). It is well-known that such a solution can be recovered by considering a dimension-4 lattice[6]. We will investigate the case $n > 1$ in next sections. In particular, we will see that the size of the linear combinations that we obtain by eliminating $s_1, \dots, s_n$ exponentially grows with n. It follows that n could be chosen logarithmic in λ instead of polynomial for LWE.

Recovering a short integer solution in linear systems. Let q be a large prime, let $\boldsymbol{x}^* = (x_1^*, \cdots, x_\ell^*)$ be a randomly chosen *short* vector and let $\mathcal{A} \in \mathbb{Z}_q^{t \times \ell}$ with $t \leq n$ be a randomly chosen matrix such that $\mathcal{A}\boldsymbol{x}^* = 0$. Our problem simply consists of recovering $\boldsymbol{x}^*$ only given $\mathcal{A}$. This problem looks like a generalization of the Subset Sum Problem but it does not fit to the famous problem SIS (Short Integer Solution) (which is equivalent to SVP on $\mathcal{L}^\perp(\mathcal{A})$) because we want to specifically recover $\boldsymbol{x}^*$ instead of an arbitrary short solution in SIS[7]. Unlike SIS, the smaller is the number of rows t, the harder is our problem. Indeed, if t is too small [8] then many short solutions - even shorter than $\boldsymbol{x}^*$ - could exist. Conversely, by increasing t, *smaller* equations can be found with gaussian eliminations, i.e. equations dealing with $\ell - t + 1$ variables which could be obtained and solved considering dimension-$(\ell - t + 1)$ lattices. More generally, the solution set of $\mathcal{A}\boldsymbol{x} = 0$ is a q-ary[9] dimension-ℓ euclidean lattice $\mathcal{L}$ spanned by at least $\ell - t$ dimension-ℓ (linearly independent) vectors[10] $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{\ell - t}$ (being solutions of the system). In order to reduce the lattice dimension, these vectors could be truncated ensuring that the truncated vector $\boldsymbol{x}^*$ can be still considered as small in the lattice spanned by the truncated vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{\ell - t}$. However, more than $\ell - t + 1$ components should be kept ($\ell - t$ is surely not enough because $\mathcal{L} = \mathbb{Z}^{\ell - t}$ in this case). It follows that dimension-$(d \geq \ell - t + 1)$ lattices should be considered. Hence, ensuring that $\ell - t$ is not *too large*, short solutions can be recovered by applying a lattice basis reduction algorithm over $\mathcal{L}$, e.g. LLL or BKZ. Let us try to quantify it.

It is well-known that SVP is a $\mathcal{NP}$-hard (under some conditions) problem and lattice basis reduction algorithms only recover approximations of the shortest

[6] However, by choosing $\delta = 1$, this attack fails because $ee' \gg q$.

[7] Unlike our problem, some columns of $\mathcal{A}$ can be removed in SIS (meaning that some components of the searched solution are set to 0) reducing the dimension of the considered lattice. Obviously, if too many columns are removed then short solutions do not exist meaning that a compromise should be done (see [MR09])

[8] typically $t < \ell / r$ according to gaussian estimations.

[9] meaning that $q\mathbb{Z}^\ell \subset \mathcal{L}$, see [MR09].

[10] and vectors belonging to $q\mathbb{Z}^\ell$.

vector within a factor[11] γ^d (with $\gamma \approx 1.01$ for the best known polynomial-time algorithms [MR09]). While this approximation may be sufficient to solve SVP on some lattices, it is ensured that $\boldsymbol{x}^*$ cannot be recovered provided[12] $\gamma^d \geq q\sqrt{d}$ and hence (provided $(\log q - \log\log q)\log\gamma \geq 1$)

$$d \geq \ell - t + 1 \geq (\log q + \log\log q)/\log\gamma \tag{4}$$

Indeed, the euclidean norm of any vector of $\mathbb{Z}_q^d$ is smaller than $q\sqrt{d}$. Consequently, satisfying (4) ensures that any solution of $\mathcal{A}\boldsymbol{x} = 0$ can be potentially output. As the number of solutions of $\mathcal{A}\boldsymbol{x} = 0$ is large, it can be assumed that $\boldsymbol{x}^*$ is output with negligible probability.

Applying it to our scheme. Contrarily to LWE-based encryption (see Appendix D), eliminating $s_1, \ldots, s_n$ from $\mathcal{F} = 0$ gives nonlinear equations (as observed in the case $n = 1$ (3)) between the variables $x_1, \ldots, x_{n+1}$. This is the major difference with LWE.

We first easily check that there do not exist equations between less than n variables. The most natural way to get equations between $n+1$ variables is to consider the n first equations of $\mathcal{F} = 0$ as a linear system where the variables are $s_1, s_2, \ldots, s_n$. By doing this, each variable s_i can be expressed as a ratio p_i/p_0 of two degree-n polynomials defined[13] over $x_1, \ldots, x_n$. By injecting these equations in the $(n+1)^{th}$ equation of $\mathcal{F} = 0$, we get an equation between the variables $x_1, \ldots, x_{n+1}$ of degree $n+1$, i.e. we obtain a polynomial $\phi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$ defined by

$$\phi(x_1, \ldots, x_{n+1}) \overset{\mathsf{def}}{=} \sum_{i=0}^{n} (u_{n+1,i} - x_{n+1}v_{n+1,i})p_i(x_1, \ldots, x_n) = 0 \tag{5}$$

We obviously obtain the same polynomial ϕ by permuting the $(n+1)$ first rows of $\mathcal{F}$. In addition,

$$\phi(x_1, \ldots, x_{n+1}) = \sum_{e \in \{0,1\}^{n+1}} a_e x_1^{e_1} \cdots x_{n+1}^{e_{n+1}}$$

where a_e are degree-$(n+1)$ polynomials defined over $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$. By considering each monomial of ϕ as a variable, we get an linear equation that could lead to lattice-based attacks. However, one could reasonably think that $a_e = 0$ with negligible probability (over the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$) implying that the number of monomials of ϕ is exponential. Nevertheless, we cannot *a priori* exclude the possibility to recover smaller equations. The following lemma establishes the non-existence of such equations.

[11] γ^d for a full rank dimension-d lattice.

[12] The norm of any vector belonging to $\mathbb{Z}_q^d$ is smaller than $q\sqrt{d}$.

[13] Consider the $n \times n$ matrix $M = [(u_{ij} - x_i v_{ij})_{1 \leq i,j \leq n}]$, the vector $\boldsymbol{t} = (u_{i0} - x_i v_{i0})_{1 \leq i \leq n}$ and the matrix M_j equal to M where the j^{th} column is replaced by $-\boldsymbol{t}$. Solving $\mathcal{F} = 0$ as a linear system gives $s^i = \det M_i / \det M$. It follows that the polynomials $p_i = \det M_i$ and $p_0 = \det M$ have 2^n monomials $x_1^{e_1} \cdots x_n^{e_n}$ where $0 \leq e_1, \ldots, e_n \leq 1$.

Lemma 2. *Let ϕ be the polynomial defined in Eq. 5. We have,*

1. *ϕ has more than $(1 - 1/\xi - n/q) \cdot 2^{n+1}$ monomials in mean*[14]*.*
2. *Any non-null multiple φ of ϕ satisfies*[15] *$m(\varphi) \geq m(\phi)$*
3. *With overwhelming probability*[14]*, any polynomial $\varphi \in I_X \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$ s.t. $\deg \varphi < \frac{q}{2(n+1)}$ is a multiple of ϕ.*

Proof. See Appendix E. Note that the proof of 3. is based on Bezout's theorem (see Lemma 6).
□

By corollary, $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$ is generated[14] by ϕ and any non-null polynomial $\varphi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$ has more than[16] 2^{n+1} monomials. What about polynomials $\varphi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$?

One can reasonably think that the number of monomials grows with the number of involved variables implying that any $\varphi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$ has at least 2^{n+1} monomials. To get such a general result, Lemma 2 should be extended.

We did not succeed in proving such a result while we obtained some partial and/or informal results. We are reasonably confident that $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$ is the sum of the ideals $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_{i_1}, \ldots, X_{i_{n+1}}]$ for any $\{i_1, \ldots, i_{n+1}\} \subseteq \{1 \ldots, m\}$, i.e. $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$ is generated by the family of polynomials ϕ obtained as done above (Eq. 5) by permuting equations of $\mathcal{F} = 0$. Some experiments going in this sense are presented in Appendix F. It would then suffice to adapt Lemma 7 to get a general result (See Appendix F.2).

Conjecture 1. With overwhelming probability[14], any non-null polynomial $\varphi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$ has more than 2^{n+1} monomials.

Proof. (Informal). See appendix F.
□

Let us now consider a set of t polynomials $\phi_1, \ldots, \phi_t \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$. Let ℓ denote the number of monomials involved in this set of polynomials. Hence, by considering each monomial as a variable, we get a system $\mathcal{A}\boldsymbol{x}^* = 0$ with t equations and ℓ variables. Without loss of generality, it can be assumed that these equations are linearly independent (otherwise it suffices to remove linearly dependent equations). According to the previous section, short solutions could be found by applying lattice basis reduction algorithms. However, assuming that Conjecture 1 is true, it is ensured that $\ell - t + 1$ is larger than 2^{n+1}. Indeed, if it is not the case, polynomials $\varphi \in I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_m]$ containing less than $\ell - t + 1 < 2^{n+1}$ monomials can be obtained by gaussian eliminations. Consequently, according to (4), it suffices that $\ell - t + 1 \geq 2^{n+1} \geq (\log q + \log\log q)/\log \gamma$ to

[14] randomness coming from the choice of $\mathcal{F}$, i.e. $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$

[15] Recall that $m(\phi)$ refers to the number of monomials of ϕ.

[16] a quantity exponentially close to 2^{n+1}.

ensure that $\mathcal{A}\boldsymbol{x}^* = 0$ cannot be solved by using lattice basis reduction algorithms. Thus, n can be chosen as follows:

$$\begin{aligned} n &\geq \log(\log q + \log\log q) - \log\log\gamma - 1 \\ &\geq \log\log q - \log\log\gamma \\ &\approx \log\lambda + \log\delta - \log\log\gamma \end{aligned}$$

For instance, one can choose $n = \log\delta + 13$ for $\gamma = 1.01$, $\lambda = 100$.

The monomials were assumed to be small relatively to q. However, it is not the case provided

$$n \geq \delta$$

This ensures the inefficiency of such lattice-based attacks. This suggests that n can be fixed independently of the security parameter λ.

3.6 Discussion

In this section, we investigated the hardness of $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ (and $\mathsf{FDLWE}_{n,m,q,\chi,\psi}$). Our security analysis deals with probability distributions χ ensuring that noise values cannot be guessed with non-negligible probability. Typically, χ is the uniform probability distribution over a set $\{0,\ldots,\xi-1\}$ with $2^\lambda \approx \xi < q$. Our analysis suggests that $\mathsf{FLWE}_{n,m,q,\chi,\psi}$ is hard ensuring that $n \geq \log\log q - \log\log\gamma$ or $n \geq \log q / \log\xi$.

Let us consider now smaller noise levels. Our analysis remains relevant except that some noise values can be guessed. Assume for instance that $\xi \approx 2^{10}$ and $q \approx \xi^\delta$. At most 10 $(= (\lambda = 100)/\log\xi)$ noise values can be guessed, one can reasonably think that it suffices to choose n larger than $10 + \log\log q - \log\log\gamma \approx 27 + \log\delta$ (assuming $\gamma = 1.01$).

4 A somewhat homomorphic private-key encryption

Let λ be a security parameter, let ξ be a λ-bit prime and let q be a $(2\delta+1)\lambda$-bit prime with $\delta \geq 1$. Throughout this section, χ will refers to the uniform distribution over $\{0,\ldots,\xi-1\}$. Note that this set will be also the plaintext domain.

Definition 4. *The functions KeyGen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$ are defined as follows:*

- *$\mathsf{KeyGen}(\lambda,\xi,q)$. Let n be indexed by λ, q. The uniform probability over $\{1\} \times \mathbb{Z}_q^n$ is denoted by ψ and let $\boldsymbol{s} \leftarrow \psi$.*

$$K = \{\boldsymbol{s}\} \ ; \ pp = \{q, \xi\}$$

- *$\mathsf{Encrypt}(K, pp, x \in \{0,\ldots,\xi-1\})$. Let $e \leftarrow \chi$ and let $\overline{x} = x + e\xi$. Output a pair $\boldsymbol{c} = (\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_q^{n+1} \times \mathbb{Z}_q^{n+1}$ of two randomly chosen vectors[17] satisfying*

$$\langle \boldsymbol{s},\boldsymbol{u}\rangle \cdot \langle \boldsymbol{s},\boldsymbol{v}\rangle^{-1} = \overline{x} \pmod{q}$$

[17] For instance, one can randomly choose $\boldsymbol{u}, v_1, \ldots, v_{n-1}, e$ and adjust v_n in order to satisfy the equality.

– $\mathsf{Decrypt}(K, pp, \boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}))$. *Output* $x = \langle \boldsymbol{s}, \boldsymbol{u} \rangle \cdot \langle \boldsymbol{s}, \boldsymbol{v} \rangle^{-1} \bmod q \bmod \xi$

In the rest of the paper, it will be assumed that $pp = \{q, \xi\}$ is public. We remark that $\boldsymbol{c}$ and $a\boldsymbol{c}$ are encryptions of the same value for any $a \in \mathbb{Z}_q^*$.

4.1 Homomorphic properties

Let $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$ and $\boldsymbol{c}' = (\boldsymbol{u}', \boldsymbol{v}')$ be *fresh* encryptions (output by $\mathsf{Encrypt}$) of respectively x and x'. Similarly to LWE-based encryption schemes, this scheme has natural homomorphic properties coming from the following equalities

$$\frac{\langle \boldsymbol{s}, \boldsymbol{u} + a\boldsymbol{v} \rangle}{\langle \boldsymbol{s}, \boldsymbol{v} \rangle} = \overline{x} + a$$

$$\frac{\langle \boldsymbol{s}, a\boldsymbol{u} \rangle}{\langle \boldsymbol{s}, \boldsymbol{v} \rangle} = a\overline{x}$$

$$\frac{\langle \boldsymbol{s}, \boldsymbol{u} \rangle \langle \boldsymbol{s}, \boldsymbol{u}' \rangle}{\langle \boldsymbol{s}, \boldsymbol{v} \rangle \langle \boldsymbol{s}, \boldsymbol{v}' \rangle} = \overline{xx}'$$

$$\frac{\langle \boldsymbol{s}, \boldsymbol{u} \rangle \langle \boldsymbol{s}, \boldsymbol{v}' \rangle + \langle \boldsymbol{s}, \boldsymbol{u}' \rangle \langle \boldsymbol{s}, \boldsymbol{v} \rangle}{\langle \boldsymbol{s}, \boldsymbol{v} \rangle \langle \boldsymbol{s}, \boldsymbol{v}' \rangle} = \overline{x} + \overline{x}'$$

It follows that vectors[18] $(\boldsymbol{u} \odot \boldsymbol{v}' + \boldsymbol{u}' \odot \boldsymbol{v}, \boldsymbol{v} \odot \boldsymbol{v}')$ and $(\boldsymbol{u} \odot \boldsymbol{u}', \boldsymbol{v} \odot \boldsymbol{v}')$ are encryptions of respectively $x + x'$ and xx' under the key $K_2 = (s_i s_j)_{n \geq i \geq j \geq 0}$ with $s_0 = 1$. This process can be naturally iterated. However, the noise exponentially grows with the homomorphic multiplications limiting evaluation to degree-δ polynomials. Moreover, the ciphertext size grows with the number of homomorphic operations m. Nevertheless, it is important to notice that this growth is *only* polynomial and not exponential. Indeed, the size of K_m is equal to the number of degree-m monomials defined over $n + 1$ variables. According to Remark 1, this number is in $O(m^n)$. While this growth strongly limits the homomorphic capabilities, short arithmetic circuits representing degree-δ polynomials could be efficiently evaluated provided n is small enough.

4.2 Security analysis

As expected, FLWE can be almost straightforwardly reduced to the security of our scheme.

Proposition 1. *Let m be the number of requests to the encryption oracle done by the CPA attacker. We have,*

[18] Recall that given two vectors $\boldsymbol{a} = (a_0, \ldots, a_n)$ and $\boldsymbol{b} = (b_0, \ldots, b_n)$, $\boldsymbol{a} \odot \boldsymbol{b} \overset{\mathsf{def}}{=} (c_{ij})_{n \geq i \geq j \geq 0}$ with $c_{ii} = a_i b_i$ and $c_{ij} = a_i b_j + a_j b_i$ if $i > j$.

1. *The CPA attacker cannot recover the secret key $\boldsymbol{s}$ assuming the hardness of* $\mathsf{FLWE}_{n,m,q,\chi,\psi}$.
2. *Our scheme is IND-CPA secure assuming the hardness of* $\mathsf{DFLWE}_{n,m,q,\chi,\psi}$.

Proof. Let m samples $(\boldsymbol{u}_i, \boldsymbol{v}_i)_{i=1,\ldots,m}$ drawn according to $A_{\boldsymbol{s},\chi}$ and let $x_1, \ldots, x_m \in \{0, \ldots, \xi-1\}$ chosen by the CPA attacker. We then consider the polynomial-time algorithm f which inputs $(\boldsymbol{u}_i, \boldsymbol{v}_i)$ and outputs $(\boldsymbol{u}'_i, \boldsymbol{v}'_i)$ defined by

$$\begin{aligned} \boldsymbol{u}'_i &= \xi \boldsymbol{u}_i + x_i \boldsymbol{v}_i \\ \boldsymbol{v}'_i &= \boldsymbol{v}_i \end{aligned}$$

Clearly,

$$\langle \boldsymbol{s}, \boldsymbol{u}'_i \rangle / \langle \boldsymbol{s}, \boldsymbol{v}'_i \rangle = \xi \langle \boldsymbol{s}, \boldsymbol{u}_i \rangle / \langle \boldsymbol{s}, \boldsymbol{v}_i \rangle + x_i \langle \boldsymbol{s}, \boldsymbol{v}_i \rangle / \langle \boldsymbol{s}, \boldsymbol{v}_i \rangle = x_i + e_i \xi$$

It follows that $\boldsymbol{c}_i = (\boldsymbol{u}'_i, \boldsymbol{v}'_i)$ is an encryption of x_i statistically indistinguishable from $\mathsf{Encrypt}(\boldsymbol{s}, x_i)$. This is sufficient to prove the result.

□

4.3 Efficiency

Proposition 1 and the analysis of FLWE suggests that our scheme is IND-CPA secure assuming either $n \geq \log(2\delta + 1) + \log \lambda - \log \log \gamma$ or $n \geq 2\delta + 1$. For instance, one can choose $n = 9$ for $\delta = 4$ with $\xi \approx 2^{100}$ and $q \approx 2^{900}$. Such parameters lead to a scheme able to evaluate degree-4 polynomials and the ratio (fresh) ciphertext size/plaintext size is close to $\frac{900}{100} \times (9 + 1) \times 2 = 180$. More generally, this ratio is

$$O\left(\delta(\log \delta + \log \lambda - \log \log \gamma)\right)$$

by choosing $n = \log(2\delta + 1) + \log \lambda - \log \log \gamma$.

Let us propose a comparison with a simple (large plaintext) LWE-based encryption where a ciphertext is a vector $\boldsymbol{c} \in \mathbb{Z}_q^n$ satisfying $\langle \boldsymbol{s}, \boldsymbol{c} \rangle = x + e\xi$. Even if we consider the smallest noise level (for instance $e \leftarrow \{0, 1\}$), q should be at least a $\delta\lambda$-bit prime to ensure correctness of degree-δ polynomial evaluation. Moreover, in such schemes, it is required that $n = \Omega(q)$ leading to a ratio ciphertext size/plaintext size in $\Omega(\delta^2 \lambda)$. This shows that our scheme significantly outperforms LWE-based schemes in the evaluation of short arithmetic circuits.

5 Perspectives

We proposed a new cryptographic primitive derived from LWE, called Fractional LWE. Our analysis suggests that n could be chosen logarithmic in $\log q$ instead of polynomial for LWE (FLWE). We then propose a very simple private-key homomorphic encryption based on this problem. This large plaintext encryption scheme achieves good efficiency to evaluate very short arithmetic circuits.

Nevertheless, a part of our security analysis is subject to Conjecture 1. While formal and experimental results are proposed in favor of Conjecture 1, we did not manage to formally prove it. In our opinion, this conjecture represents a nice algebraic challenge and its proof would be a great step in the security analysis of our scheme. More fundamentally, the existence of reductions from classical cryptographic problems (LWE, SVP,...) should be investigated. In parallel, it is interesting to wonder whether some LWE-based cryptographic primitives can be improved with our scheme. The most natural one would be an efficient (somewhat) homomorphic encryption by introducing relinearization technics to reduce the ciphertext expansion.

5.1 Relinearization

The homomorphic capabilities of our scheme are low due to the ciphertext expansion. We propose here a very simple way to relinearize ciphertexts. As seen previously, a ciphertext $\boldsymbol{c'} = (\boldsymbol{u'}, \boldsymbol{v'})$ obtained after a homomorphic operation over *fresh* ciphertexts can be decrypted with the key $K_2 = \boldsymbol{s}^2 = (s_i s_j)_{n \geq i \geq j \geq 0}$ where $s_0 = 1$, $\boldsymbol{s}^2$ having $n' = (n+1)(n+2)/2$ components. We propose to develop a way to transform $\boldsymbol{c'}$ in a ciphertext $\boldsymbol{c}$ encrypting the same message under K, i.e. $\mathsf{Decrypt}(K, \boldsymbol{c}) = \mathsf{Decrypt}(K_2, \boldsymbol{c'})$. The simplest way is certainly to build a public function $R_K : \mathbb{Z}_q^{n'} \to \mathbb{Z}_q^{n+1}$ satisfying for any $\boldsymbol{u} \in \mathbb{Z}_q^{n'}$

$$\langle \boldsymbol{s}, R_K(\boldsymbol{u}) \rangle = \rho \cdot \langle \boldsymbol{s}^2, \boldsymbol{u} \rangle \tag{6}$$

for a given $\rho \in \mathbb{Z}_q^*$. By construction, $\boldsymbol{c'}$ and $(R_K(\boldsymbol{u'}), R_K(\boldsymbol{v'}))$ encrypt the same message. The simplest way to achieve this consists of defining R_K as a linear combination, i.e. $R_K(\boldsymbol{u}) = A\boldsymbol{u}$ where $A \in \mathbb{Z}_q^{(n+1) \times n'}$ is a randomly chosen public matrix ensuring that $\langle \boldsymbol{s}, A\boldsymbol{u} \rangle = \rho \cdot \langle \boldsymbol{s}^2, \boldsymbol{u} \rangle$. However, publicizing A makes Conjecture 1 false and univariate degre-$(n+1)$ equations dealing with $\overline{x}_1$ (for instance) can be obtained. A first consequence is that the factorization of q should not be known. But, even under the factoring assumption, these equations can be polynomially solved with Coppersmith's algorithm [Cop96] provided $n < 2\delta + 1$. Nevertheless, it is not the case anymore by choosing $n \geq 2\delta + 1$. Moreover, one can show that recovering $\boldsymbol{s}$ only given A is hard assuming that the factorization of q is unknown (see Appendix G). It follows that publicizing A does not break the security of our scheme in the generic ring model and the potential attacks *should use* the shortness of the $\overline{x}_i$'s.

By assuming that our scheme remains secure by publicizing A, we would get a very efficient homomorphic encryption able to evaluate low degree polynomials. For instance, if q is a bit-1024 RSA modulus, χ a bit-128 prime and $n = 9$, we have a degree-4 homomorphic encryption. The ratio ciphertext size with plaintext size is around 200. A homomorphic addition (+relinearization) requires $100 \times 3 + 2 \times 10 \times 55 = 1400$ modular multiplications over $\mathbb{Z}_q$ and a homomorphic multiplication (+relinearization) requires $100 \times 2 + 2 \times 10 \times 55 = 1300$ modular multiplications.

5.2 Removing noise

Instead of adding noise to the encrypted value x, we propose to additively share $x = x_1 + \cdots + x_t$ and to encrypt each share x_i with the key $\boldsymbol{s}_i$. For concreteness, to encrypt x, one randomly choose $\boldsymbol{c} = (\boldsymbol{u}_i, \boldsymbol{v}_i)_{i=1,\ldots,t}$ such that $\sum_{i=1}^{t} \langle \boldsymbol{s}_i, \boldsymbol{u}_i \rangle / \langle \boldsymbol{s}_i, \boldsymbol{v}_i \rangle = x$. In other words, an encryption $\boldsymbol{c}$ is a randomly chosen vector satisfying $\phi(\boldsymbol{c}) = 0$ with

$$\phi(\boldsymbol{c}) = \sum_{\ell=1}^{t} \langle \boldsymbol{s}_\ell, \boldsymbol{u}_\ell \rangle \prod_{i \in \{1,\ldots,t\} \setminus \{\ell\}} \langle \boldsymbol{s}_i, \boldsymbol{v}_i \rangle - x \cdot \prod_{i \in \{1,\ldots,t\}} \langle \boldsymbol{s}_i, \boldsymbol{v}_i \rangle$$

ϕ is a degree-t polynomial defined over $2(n+1)t$ variables. The knowledge's attacker can be seen as evaluations of ϕ over points $\boldsymbol{c}_i$ randomly chosen in $\{\boldsymbol{y} | \phi(\boldsymbol{y}) = x_i\}$. While the monomial coefficients of ϕ could be recovered by solving a linear system, the expanded representation of ϕ exponentially grows with t. Hence, it suffices to choose $t = \Theta(\lambda)$ to make this attack fail. At this step, we get a noise-free encryption scheme with some homomorphic properties. However, the ciphertext expansion is exponential with the number of homomorphic operations. By assuming that relinearization technics (as presented in the previous section) could fix this problem, we would get a noise-free FHE. This is surely the most exciting distant prospect of our work.

References

[AM09] Divesh Aggarwal and Ueli M. Maurer. Breaking RSA generically is equivalent to factoring. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, pages 36–53, 2009.

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *TOCT*, 6(3):13:1–13:36, 2014.

[BKW93] T. Becker, H. Kredel, and V. Weispfenning. *Gröbner bases: a computational approach to commutative algebra*. Springer-Verlag, London, UK, 0 edition, 4 1993.

[BRS67] Elwyn R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10(6):553–564, 1967.

[BV11] Zvika Brakerski and Vinod 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.

[Cop96] Don Coppersmith. Finding a small root of a univariate modular equation. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 155–165, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology*

Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, pages 75–92, 2013.

[MR09] Daniele Micciancio and Odded Regev. Lattice based cryptography. In *Post-Quantum Cryptography*, pages 147–191, 2009.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342, 2009.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980.

[SP17] Alan Szepieniec and Bart Preneel. Short solutions to nonlinear systems of equations. In *Number-Theoretic Methods in Cryptology - First International Conference, NuTMiC 2017, Warsaw, Poland, September 11-13, 2017, Revised Selected Papers*, pages 71–90, 2017.

A Zippel-Schwartz's theorem

Given a function $\phi : \mathbb{Z}_q^t \to \mathbb{Z}_q$ and a nonempty subset $K \subseteq \mathbb{Z}_q^t$, $z_{\phi,K}$ denotes the probability over K that $\phi(x) = 0$,

$$z_{\phi,K} \overset{\mathsf{def}}{=} \frac{\#\{x \in K | \phi(x) = 0\}}{\#K}$$

Theorem 2. ***(Zippel-Schwartz's theorem [Sch80].)*** *Let q be a prime, let $\phi \in \mathbb{Z}_q[X_1, \ldots, X_t]$ be a non-null polynomial and let $I \subseteq \mathbb{Z}_q$ with $\#I = \xi$. We have $z_{\phi,I^t} \leq \deg\phi/\xi$.*

We propose to slightly adapt this theorem to our needs.

Proposition 2. *Let $\phi \in \mathbb{Z}_q[X_1, \ldots, X_{r+t}]$ be a non-null polynomial, let $I \subseteq \mathbb{Z}_q$ with $\#I = \xi$ and let $K = I^r \times \mathbb{Z}_q^t$. We have $z_{K,\phi} \leq (1/q + 1/\xi)\deg\phi$.*

Proof. Clearly, $\mathbb{Z}_q[X_1, \ldots, X_{r+t}]$ can be identified to $R[X_1, \ldots, X_t]$ with $R = \mathbb{Z}_q[X_{r+1}, \ldots, X_{r+t}]$. Thus, a non-null polynomial $\phi \in \mathbb{Z}_q[X_1, \ldots, X_{r+t}]$ can be identified to a non-null polynomial $\phi' \in R[X_{r+1}, \ldots, X_{r+t}]$. Thus, by fixing $X_1, \ldots, X_r$ to randomly chosen values $x_1, \ldots, x_r \in \mathbb{Z}_q$, the polynomial $\phi_{x_1,\ldots,x_r}$ defined by $\phi_{x_1,\ldots,x_r}(x_{r+1}, \ldots, x_{r+t}) = \phi(x_1, \ldots, x_{r+t})$ is (identically) null with probability (over the choice of $x_1, \ldots, x_r$) $p \leq \deg\phi/q$ according to Theorem 2. Moreover, provided $\phi_{x_1,\ldots,x_r}$ is not null, $\phi_{x_1,\ldots,x_r}(x_{r+1}, \ldots, x_{t+r}) = 0$ with probability lower than $\deg\phi/\xi$ according to Theorem 2. It follows that $z_{K,\phi} \leq p + (1-p)\deg\phi/\xi \leq \deg\phi/q + \deg\phi/\xi$.
□

Corollary 1. *If $\deg\phi/\xi$ is negligible and $z_{K,\phi}$ is not negligible then ϕ is null.*

B Roots of polynomials under the factoring assumption

The following result proved in [AM09] establishes that it is difficult to output a polynomial ϕ such that z_ϕ is non-negligible without knowing the factorization of q. The security of RSA in the generic ring model can be quite straightforwardly derived from this result (see [AM09]).

Theorem 3. ***(Lemma 4 of [AM09]).*** *Assuming factoring is hard, there is no p.p.t-algorithm $\mathcal{A}$ which inputs a RSA-modulus q and which outputs*[19] *a $\{+, -, \times\}$-circuit computing a non-null polynomial $\phi \in \mathbb{Z}_q[X]$ such that $z_{\phi,\mathbb{Z}_q}$ is non-negligible.*

Thanks to this lemma, showing that two polynomials[20] are equal with non-negligible probability becomes an algebraic problem: it suffices to prove that they are identically equal. This result can be easily extended to the multivariate case.

[19] with non-negligible probability (the coin toss being the choice of q and the internal randomness of $\mathcal{A}$)

[20] built without knowing the factorization of q

C Proof of Theorem 1

We will prove the result for $n = 1$. The result remains *a fortiori* true for $n > 1$. Let ε be the polynomial tuple defined by

$$\varepsilon(S, (Z_1, Z_2, Z_3, Z_4) = (SZ_3, Z_1 - Z_3, SZ_4, Z_2 - Z_4)$$

Lemma 3. *There does not exist any polynomial-degree polynomial $\phi \in \mathbb{Z}_q[X_1, \ldots, X_4]$ ensuring that $\phi \circ \varepsilon$ is a multiple of Z_2.*

Proof. Let ϕ be a non-null polynomial such that $\phi(SZ_3, Z_1 - Z_3, SZ_4, Z_2 - Z_4)$ is a multiple of Z_2. It follows that $\phi(sz_3, z_1 - z_3, sz_4, -z_4) = 0$ for any $(s, z_1, z_3, z_4) \in \mathbb{Z}_q^4$. Clearly, the probability distribution of $(sz_3, z_1 - z_3, sz_4, -z_4)$ is statistically close to the uniform distribution over $\mathbb{Z}_q^4$ provided (s, z_1, z_3, z_4) uniform over $\mathbb{Z}_q^4$. It follows that $\phi(x_0, \ldots, x_3) = 0$ with non negligible probability provided $(x_0, \ldots, x_3)$ uniform over $\mathbb{Z}_q^4$. Proposition 2 ensures that such a polynomial ϕ is null.
□

Let $(\phi'_1/\phi_1, \ldots, \phi'_\gamma/\phi_\gamma, p) \in \mathcal{C}$ (satisfying (2)) and let $\phi = \phi_1 \cdots \phi_\gamma$. By construction, ϕ is a polynomial-degree polynomial.

Let $\boldsymbol{s}^* = (1, s^*)$ be a choice of $\boldsymbol{s} = (1, s)$ such that (2) is satisfied with non-negligible probability over the choice of $\boldsymbol{w} = (s^*u, re - u, s^*v, r - v) \leftarrow A_{\boldsymbol{s}^*,\chi}$. By definition of χ, $\boldsymbol{y} = (u, v, r, e)$ is uniform over $\mathbb{Z}_q^3 \times \{0, \ldots, \xi - 1\}$.

Let ε^* and ν be the polynomial-degree polynomials defined by $\nu(\boldsymbol{y}) = (re, r, u, v)$ and $\varepsilon^*(\boldsymbol{z}) = (s^*z_3, z_1 - z_3, s^*z_4, z_2 - z_4)$, i.e. $\varepsilon^* \circ \nu(\boldsymbol{y}) = \boldsymbol{w}$ and let ψ^* be the polynomial defined by

$$\psi^* = a_1(\boldsymbol{s}^*) \cdot \phi'_1 \prod_{i=1,\ldots,\gamma; i \neq 1} \phi_i + \ldots + a_\gamma(\boldsymbol{s}^*) \cdot \phi'_\gamma \prod_{i=1,\ldots,\gamma; i \neq \gamma} \phi_i$$

The choice of $\boldsymbol{s}^*$ ensures that

$$p(e) \cdot \phi(\boldsymbol{w}) - \psi^*(\boldsymbol{w}) = 0$$

with non-negligible probability over the choice of $\boldsymbol{w}$. It follows that

$$p(e) \cdot \phi \circ \varepsilon^* \circ \nu(\boldsymbol{y}) = \psi^* \circ \varepsilon^* \circ \nu(\boldsymbol{y})$$

with non-negligible probability over the choice of $\boldsymbol{y}$. Consequently, according to Proposition 2, these two polynomials coincide,

$$p(z_4) \cdot \phi \circ \varepsilon^* \circ \nu(\boldsymbol{z}) = \psi^* \circ \varepsilon^* \circ \nu(\boldsymbol{z})$$

for any $\boldsymbol{z} \in \mathbb{Z}_q^4$. It follows that

$$p(z_1/z_2) \cdot \phi \circ \varepsilon^*(\boldsymbol{z}) = \psi^* \circ \varepsilon^*(\boldsymbol{z}) \qquad (7)$$

with overwhelming probability. Let p' be the polynomial defined by $p'(\boldsymbol{z}) = z_2^{\deg p} p(z_1/z_2)$. According to (7),

$$p' \cdot \phi^* \circ \varepsilon^*(\boldsymbol{z}) = z_2^{\deg p} \psi^* \circ \varepsilon^*(\boldsymbol{z})$$

with overwhelming probability. Hence, according to Proposition 2,

$$p' \cdot \phi^* \circ \varepsilon^* = z_2^{\deg p} \psi^* \circ \varepsilon^*$$

By construction, p' is not a multiple of z_2 and its degree is polynomial. Hence, according to Proposition 2, $p'(z_1, 0, z_3, z_4) = 0$ is satisfied with negligible probability and thus

$$\phi \circ \varepsilon^*(z_1, 0, z_3, z_4) = 0 \tag{8}$$

for any z_1, z_3, z_4. Let ε be the polynomial tuple defined in Lemma 3. By construction, $\phi \circ \varepsilon(s^*, z_1, z_2, z_3, z_4) = \phi \circ \varepsilon^*(z_1, z_2, z_3, z_4)$. Consequently, according to (8), $\phi \circ \varepsilon(s, z_1, 0, z_3, z_4) = 0$ with non-negligible probability over the choice of s, z_1, z_3, z_4. Hence, according to Proposition 2, the polynomial

$$\phi \circ \varepsilon(S, Z_1, 0, Z_3, Z_4)$$

is null. It follows that $\phi \circ \varepsilon(S, Z_1, Z_2, Z_3, Z_4)$ can be factored by Z_2. This contradicts Lemma 3.

□

D LWE-based encryption schemes.

Typically, in LWE-based Encryption schemes, the secret key is a randomly chosen size-n vector $\boldsymbol{s} \in \mathbb{Z}_q^n$. An instance $\boldsymbol{w}$ of LWE satisfies $\langle \boldsymbol{s}, \boldsymbol{c} \rangle = e$. By considering n instances $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$, we get a linear system of equations, $\langle \boldsymbol{s}, \boldsymbol{w}_i \rangle = e_i$. By solving this system (assuming $e_1, \ldots, e_n$ known but not $s_1, \ldots, s_n$), each component s_i can be written as a linear combination $\mathcal{L}_i$ of $e_1, \ldots, e_n$, i.e.

$$s_i = \mathcal{L}_i(e_1, \ldots, e_n)$$

By injecting these equations in the $(n+1)^{th}$ equation derived from $\boldsymbol{w}_{n+1}$, we get a linear combinations between $n+1$ noise values.

Asymptotic parameters for LWE. Peikert et al. [Pei09] have shown that LWE with $q = 2^{O(n)}$ is as hard as GapSVP. As expected, the asymptotic parameters recommended for LWE ensure that (4) $\Leftrightarrow n \geq \log q / \log \gamma$ is satisfied making this attack inefficient. By corollary, this confirms our analysis.

E Proof of Lemma 2

Lemma 4. *ϕ has at least $(1 - 1/\xi - n/q)2^{n+1}$ monomials in mean*[21].

[21] the toss coin being the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$

Proof. Each monomial coefficient of ϕ can be written as a linear combination $a_1 v_{1n} + \ldots + a_{n+1} v_{n+1,n}$ where the a_i's are degree-n polynomials defined over $(u_{ij}, v_{ij})_{(i,j)\in\{1,\ldots,n+1\}\times\{0,\ldots,n-1\}}$. According to the construction of our scheme, for any choice of $(u_{ij}, v_{ij})_{(i,j)\in\{1,\ldots,n+1\}\times\{0,\ldots,n-1\}}$, there are ξ choices for each v_{in}. Assume there exists $i \in \{1, \ldots, n+1\}$ such $a_i \neq 0$. In this case, $a_1 v_{1n} + \ldots + a_{n+1} v_{n+1,n} = 0$ with probability smaller than $1/\xi$. The probability that $a_i = 0$ is smaller that n/q according to Zippel-Schwartz's theorem (see Appendix A). Hence, $a_1 v_{1n} + \ldots + a_{n+1} v_{n+1,n} = 0$ with probability smaller than $1/\xi + n/q$.
□

Lemma 5. *Given $(x_3, \ldots, x_{n+1}) \in \mathbb{Z}_q^{n-1}$, we consider the polynomial $\phi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = \phi(X_1, X_2, x_3, \ldots, x_{n+1})$. The polynomial $\phi_{x_3,\ldots,x_{n+1}}$ is irreducible with overwhelming probability over the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$, $x_3, \ldots, x_{n+1}$.*

Proof. (Sketch.) $\phi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = a_0 + a_1 X_1 + a_2 X_2 + a_3 X_1 X_2$ where each coefficient a_i can be written as a linear combination $b_1 v_{1n} + \ldots + b_{n+1} v_{n+1,n}$ whose each coefficient b_i is a degree-$(2n-1)$ polynomial defined over $(u_{ij}, v_{ij})_{(i,j)\in\{1,\ldots,n+1\}\times\{0,\ldots,n-1\}}$ and $x_3, \ldots, x_{n+1}$. A necessary condition ensuring that ϕ can be factored is $a_0 a_3 - a_1 a_2 = 0$. As done in the proof of the previous lemma, one can prove that this condition is satisfied with negligible probability. □

Corollary 2. *ϕ is irreducible with overwhelming probability.*

Lemma 6. *Any non-null polynomial $\varphi \in I_X \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$ s.t. $\deg \varphi < q/2(n+1)$ is a multiple [22] of ϕ.*

Proof. Without loss of generality, we can assume than $m = n+1$. Let $S_{x_3,\ldots,x_{n+1}} = \{(x_1, x_2) \in \mathbb{Z}_q^2 | \exists \boldsymbol{s} \in \mathbb{Z}_q^n, (\boldsymbol{s}, \boldsymbol{x}) \in X\}$.

Clearly, $\#S_{x_3,\ldots,x_{n+1}} = q - 1$ is satisfied[23] with overwhelming probability over the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}, x_3, \ldots, x_{n+1}$. Thus, as φ and ϕ belong to $I_X \cap \mathbb{Z}_q[X_1, \ldots, X_{n+1}]$, $\phi_{x_3,\ldots,x_{n+1}}$ and $\varphi_{x_3,\ldots,x_{n+1}}$ have[24] more than $q - 1$ common roots.

It follows that they have more than $\deg \varphi_{x_3,\ldots,x_{n+1}} \deg \phi_{x_3,\ldots,x_{n+1}} \leq \deg \varphi \cdot \deg \phi < q/2$ common roots with overwhelming probability. Let $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$, $x_3, \ldots, x_{n+1}$ be such a choice. According to Bezout's theorem, $\varphi_{x_3,\ldots,x_{n+1}}$ and $\phi_{x_3,\ldots,x_{n+1}}$ have a common factor. Moreover, according to the previous lemma, $\phi_{x_3,\ldots,x_{n+1}}$ can be factored with negligible probability. Consequently $\varphi_{x_3,\ldots,x_{n+1}}$ is a multiple of $\phi_{x_3,\ldots,x_{n+1}}$, i.e. $\varphi_{x_3,\ldots,x_{n+1}} = \phi_{x_3,\ldots,x_{n+1}} \cdot \psi_{x_3,\ldots,x_{n+1}}$. Let us introduce some notation:

- $\phi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = a_0 + a_1 X_1 + a_2 X_2 + a_3 X_1 X_2$
- $\psi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = \sum_{e \in B \subset \mathbb{N}^2} b_e X_1^{e_1} X_2^{e_2}$

[22] with overwhelming probability over the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n+1}$

[23] Roughly speaking, if $\mathcal{F} = 0$ is not *degenerated*, $x_2, \ldots, x_{n+1}$ can be chosen almost freely implying that $\#S_{x_3,\ldots,x_{n+1}}$ is approximatively equal to q.

[24] According to the notation of the previous lemma, $\phi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = \phi(X_1, X_2, x_3, \ldots, x_{n+1})$ and $\varphi_{x_3,\ldots,x_{n+1}}(X_1, X_2) = \varphi(X_1, X_2, x_3, \ldots, x_{n+1})$

– $\varphi_{x_3,\ldots,x_{n+1}}(X_1,X_2) = \sum_{e\in C\subset\mathbb{N}^2} c_e X_1^{e_1} X_2^{e_2}$

As done in the proof of Lemma 4, one can show that $a_0a_1a_2a_3 \neq 0$ with overwhelming probability. Moreover, B, C are finite sets which can be chosen independently of $x_3,\ldots,x_{n+1}$, i.e. $C = \{(e_1,e_2) \in \mathbb{N}^2 | e_1+e_2 \leq \deg\varphi\}$ and $B = \{(e_1,e_2) \in \mathbb{N}^2 | e_1+e_2 \leq \deg\varphi - 2\}$. Each coefficient b_e can be written as a linear coefficient of the coefficients c_e and each coefficient of this linear combination as a rational function defined over the coefficients $a_0,\ldots,a_3$, i.e.

$$b_e = \sum_{e'\in C} \frac{p_{ee'}(a_0,\ldots,a_3)}{a_0^{\deg\varphi-1}} c_{e'}$$

where $p_{ee'}$ is a homogeneous degree-($\deg\varphi - 2$) polynomials. It is important to notice that these polynomials do not depend on $x_3,\ldots,x_{n+1}$. Moreover, by construction, $a_0,\ldots,a_3$ are evaluations over $x_3,\ldots,x_{n+1}$ of non-null degree-$(n-1)$ polynomials $A_0,\ldots,A_3$ of $\mathbb{Z}_q[X_3,\ldots,X_{n+1}]$ and c_e are evaluations of degree-φ polynomials C_e. Let us consider the polynomial ψ defined by

$$\psi(X_1,\ldots,X_{n+1}) = \sum_{e\in B}\sum_{e'\in C} p_{ee'}(A_0,\ldots,A_3) C_{e'} X_1^{e_1} X_2^{e_2}$$

By construction, $\psi(x_1,\ldots,x_{n+1}) = \psi_{x_3,\ldots,x_{n+1}}(x_1,x_2)\cdot A_0^{\deg\varphi-1}(x_3,\ldots,x_{n+1})$. for any choice of $x_3,\ldots,x_n$ which satisfies the initial conditions[25]. It follows that

$$A_0^{\deg\varphi-1}(x_3,\ldots,x_{n+1})\cdot\varphi(x_1,\ldots,x_{n+1}) = \phi(x_1,\ldots,x_{n+1})\cdot\psi(x_1,\ldots,x_{n+1})$$

with overwhelming probability. By construction, $\deg A_0^{\deg\varphi-1}\varphi$ and $\deg\phi\psi$ are smaller than $(n+1)\deg\varphi$. Thus, provided $\deg\varphi < q/2(n+1)$, the degree of these polynomials is smaller than $q/2$. Thus, according to Zippel-Schwartz's theorem,

$$\deg A_0^{\deg\varphi-1}\cdot\varphi = \psi\cdot\phi$$

As[26] $\gcd(A_0,\phi) = 1$ (with overwhelming probability), φ is a multiple of ϕ.
□

Lemma 7. *Any multiple of* $\phi_n(X_1,\ldots,X_n) = \sum_{e\in\{0,1\}^n} a_e X_1^{e_1}\cdots X_n^{e_n}$ *has at least* $m(\phi_n) = \#\{e\in\{0,1\}^n | a_e \neq 0\}$ *monomials.*

Proof. Let $\mathbb{P}_n = \{\phi_n(X_1,\ldots,X_n) = \sum_{e\in\{0,1\}^n} a_e X_1^{e_1}\cdots X_n^{e_n} | a_e \in \mathbb{Z}_q\}$ be the set of polynomials ϕ_n satisfying constraints of Lemma 7. We prove the result by induction. It is obviously true for $n = 1$. Let us assume that the result is true for $n \geq 1$ and let consider $\phi_{n+1} \in \mathbb{P}_{n+1}$. There exist $\phi_n, \phi'_n \in \mathbb{P}_n$ s.t. $\phi_{n+1} = X_{n+1}\phi_n + \phi'_n$. Clearly $m(\phi_{n+1}) = m(\phi_n) + m(\phi'_n)$. Let $\psi \in \mathbb{Z}_q[X_1,\ldots,X_n]$ be an arbitrary polynomial. $\psi = \psi_0 + X_{n+1}\psi_1 + \ldots + X_{n+1}^t\psi_t$ where $\psi_0,\ldots,\psi_t \in$

[25] $\phi_{x_3,\ldots,x_{n+1}}$ and $\varphi_{x_3,\ldots,x_n}$ have more than $q/2$ common roots.

[26] $\deg A_0 < \deg\phi$ and ϕ is irreducible with overwhelming probability

$\mathbb{Z}_q[X_1, \ldots, X_n]$. It follows that $\phi_{n+1}\psi = (X_{n+1}\phi_n + \phi'_n)(\psi_0 + X_{n+1}\psi_1 + \ldots + X_{n+1}^t\psi_t) = \phi'_n\psi_0 + X_{n+1}^{t+1}\phi_n\psi_t + \rho$ where $\rho = X_{n+1}\psi_0 + X_{n+1}^t\psi_t\phi' + (X_{n+1}\phi_n + \phi'_n)(X_{n+1}\psi_1 + \ldots + X_{n+1}^{t-1}\psi_{t-1})$. By induction hypothesis, $m(\phi'_n\psi_0) \geq m(\phi'_n)$ and $m(\phi_n\psi_t) \geq m(\phi_n)$. As the 3 polynomials $\phi'_n\psi_0$, $X_{n+1}^{t+1}\phi_n\psi_t$ and ρ do not have common monomials. $m(\phi_{n+1}\psi) \geq m(\phi'_n\psi_0) + m(X_{n+1}^{t+1}\phi_n\psi_t) + m(\rho) \geq m(\phi_n) + m(\phi'_n) = m(\phi_{n+1})$. This concludes the proof.

□

Lemma 2 is a direct consequence of Lemmas 4, 5, 6, 7.

F About Conjecture 1

We first propose to experiment our intuition that

$$I_{\mathcal{F}} = \bigoplus_{(i_1,\ldots,i_{n+1})\subseteq\{1\ldots,m\}} I_{\mathcal{F}} \cap \mathbb{Z}_q[X_{i_1}, \ldots, X_{i_{n+1}}] \tag{9}$$

We then conjecture[27] that any polynomial of $\bigoplus_{(i_1,\ldots,i_{n+1})\subseteq\{1\ldots,m\}} I_{\mathcal{F}} \cap \mathbb{Z}_q[X_{i_1}, \ldots, X_{i_{n+1}}]$ has at least 2^{n+1} monomials.

F.1 Experiments

We present an experiment done with *SageMath* suggesting (9) with the parameters $n = 2; m = 4$. In this experiment, we randomly select polynomials $\varphi \in J = I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, \ldots, X_{m=4}]$ and we check that $\varphi \in L = \langle Phi123, Phi124, Phi234, Phi134\rangle$, these polynomials being respectively generators of the ideals $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, X_2, X_3]$, $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, X_2, X_4]$, $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_2, X_3, X_4]$, $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_1, X_3, X_4]$.

SageMath experiment.

```
var('X1,X2,X3,X4,S1,S2');
X1,X2,X3,X4,S1,S2=ZZ[X1,X2,X3,X4,S1,S2].gens()

p10=randint(-5, 5)-randint(-5, 5)*X1;
p11=randint(-5, 5)-randint(-5, 5)*X1;
p12=randint(-5, 5)-randint(-5, 5)*X1;
p20=randint(-5, 5)-randint(-5, 5)*X2;
p21=randint(-5, 5)-randint(-5, 5)*X2;
p22=randint(-5, 5)-randint(-5, 5)*X2;
p30=randint(-5, 5)-randint(-5, 5)*X3;
p31=randint(-5, 5)-randint(-5, 5)*X3;
p32=randint(-5, 5)-randint(-5, 5)*X3;
p40=randint(-5, 5)-randint(-5, 5)*X4;
```

[27] partially proved

```
p41=randint(-5, 5)-randint(-5, 5)*X4;
p42=randint(-5, 5)-randint(-5, 5)*X4;

f1=p10+p11*S1+p12*S2;
f2=p20+p21*S1+p22*S2;
f3=p30+p31*S1+p32*S2;
f4=p40+p41*S1+p42*S2;

D12=p11*p22-p21*p12
s12=p10*p22-p20*p12;
t12=p11*p20-p21*p10;

D23=p21*p32-p31*p22;
s23=p20*p32-p30*p22;
t23=p21*p30-p31*p20;
D34=p31*p42-p41*p32;

s34=p30*p42-p40*p32;
t34=p31*p40-p41*p30;

Phi123=-p30*D12+p31*s12+p32*t12
Phi124=-p40*D12+p41*s12+p42*t12
Phi234=-p40*D23+p41*s23+p42*t23
Phi134=-p10*D34+p11*s34+p12*t34

IF=ideal(f1,f2,f3,f4)
J=IF.elimination_ideal([S1,S2])
L=ideal(Phi123,Phi124,Phi234,Phi134)

for d in range(1,7):
    for i in range(50):
        varphi=J.random_element(degree=d)
        varphi in L
```

F.2 Extension of Lemma 7

Notation. *Given $\phi \in \mathbb{Z}_q[X_1, \dots, X_m]$, $M(\phi)$ refers to the set of monomials of the polynomial ϕ, i.e. $\phi = \sum_{m \in M(\phi)} a_m m$ where a_m is the coefficient of the monomial m. Two polynomials ϕ and ϕ' are said to be disjoint if $M(\phi) \cap M(\phi') = \emptyset$. Finally, $\deg_i \phi$ is the highest degree of the indeterminate X_i, e.g. $\deg_2 X_1 X_2^7 + X_1^5 X_2^5 = 7$.*

The section aims at showing that any polynomial of $\bigoplus_{(i_1,\dots,i_{n+1}) \subseteq \{1\dots,m\}} I_{\mathcal{F}} \cap \mathbb{Z}_q[X_{i_1}, \dots, X_{i_{n+1}}]$ has at least 2^{n+1} monomials. To achieve this, an extension of Lemma 7 is required. We propose a weaker result going in this sense.

Lemma 8. *For any $S = \{i_1, \ldots, i_n\} \subseteq \{1, \ldots, m\}$, ϕ_S refers to the polynomial defined by $\phi_S(X_1, \ldots, X_m) = \sum_{e \in \{0,1\}^n} X_{i_1}^{e_1} \cdots X_{i_n}^{e_n}$. Let I_n be the ideal generated by the family of polynomials $(\phi_S)_{S \subseteq \{1,\ldots,m\};\#S=n}$. Any non-null polynomial of $\varphi \in I_n$ has at least 2^n monomials.*

Proof. To prove our result, we prove by induction the following stronger result. We consider the ideal I_{nt}, $1 \leq t \leq n$ generated by the degree-t polynomial $(\phi_S)_{S \subset \{1,\ldots,n\};\#S=t}$ and we want to prove that any non-null polynomial $\varphi \in J_{nt} = I_{nt} + \cdots + I_{nn}$ has at least 2^t monomials for any $n \geq 1, t \geq 1$. This property will be denoted $\mathcal{P}_{nt}$. Proving $\mathcal{P}_{mn}$ would prove our result by noticing that $I_n \subseteq J_{mn}$.

First, one can easily prove (also by induction) that $\varphi \in J_{n,n \geq t \geq 1}$ has at least 2 monomials (using the fact that $\mathcal{P}_{11}$ is trivially true, i.e. $(1+X_1)\psi(X_1, \ldots, X_m)$ has at least 2 monomials provided ψ is not null). Let us consider the property $\mathcal{P}_n \equiv (\forall t \in \{1, \ldots, n\}, P_{nt}$ is true). As $\mathcal{P}_1$ is equivalent to $\mathcal{P}_{11}$, $\mathcal{P}_1$ is true. Assume $\mathcal{P}_{n-1}$ is true and let us prove that $\mathcal{P}_n$ is true. Let $K_{nt} = \{S \subseteq \{1, \ldots, n\} : \#S \geq t\}$. We previously saw that $\mathcal{P}_{n1}$ is true. To show $\mathcal{P}_{n,t>1}$, let us consider a non-null polynomial $\varphi = \sum_{S \in K_{nt}} \phi_S \psi_S \in J_{nt}$ with $t \in \{2, \ldots, n\}$. As φ has at least two monomials, there exist $i \in \{1, \ldots, n\}$, $m_1, m_2 \in M(\varphi)$ such that $\deg_i m_1 \neq \deg_i m_2$. Without loss of generality, we assume that $i = n$ and $\deg_n m_1 = 0$. It follows that one can write $\varphi = \varphi_1 + \varphi_2$ as the sum of two non-null disjoint (having non common monomials) polynomials φ_1, φ_2 s.t. $\deg_n \varphi_1 = 0$ and for any $m \in M(\varphi_2)$, $\deg_n m > 0$. Moreover, ψ_S can be written as the sum of two disjoint (perhaps null) polynomials ψ'_S, ψ''_S s.t. $\deg_n \psi'_S = 0$ and for any $m \in M(\psi''_S)$, $\deg_n m > 0$. Let $E_{nt} = \{S \in K_{nt} | n \notin S\}$ and $F_{nt} = \{S \in K_{nt} | n \in S\}$. By noticing that for any $S \in F_{nt}$, $\phi_S = (1 + X_n)\phi_{S \setminus \{n\}}$, we have

– $\varphi_1 = \sum_{S \in E_{nt}} \phi_S \psi'_S + \sum_{S \in F_{nt}} \phi_{S \setminus \{n\}} \psi'_S$
– $\varphi_2 = \sum_{S \in E_{nt}} \phi_S \psi''_S + \sum_{S \in F_{nt}} \phi_{S \setminus \{n\}} (X_n \psi_S + \psi''_S)$

These two non-null polynomials clearly belong to $J_{n-1,t-1}$. Thus, by induction hypothesis, they have at least 2^{t-1} monomials. As they do not have common monomials, φ has at least 2^t monomials.

□

This result is unfortunately not sufficient because the generator of the ideal $I_{\mathcal{F}} \cap \mathbb{Z}_q[X_{i_1}, \ldots, X_{i_{n+1}}]$ does not exactly fit to the requirements of Lemma 8. Indeed, this generator $\phi_{i_1,\ldots,i_{n+1}}$ is defined by

$$\phi_{i_1,\ldots,i_{n+1}}(X_1, \ldots, X_m) = \sum_{e \in \{0,1\}^n} a_e X_{i_1}^{e_1} \cdots X_{i_n}^{e_n}$$

where the coefficients a_e are randomly chosen[28] (instead of being equal to 1 as required in Lemma 8). Further investigations are required to get an exploitable result.

[28] randomness coming from the choice of $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$

G Relinearization

In this section, q is a RSA modulus. The following p.p.t algorithm RELIN inputs $\boldsymbol{s} = (1, s_1, \ldots, s_n)$ and outputs A satisfying for any $\boldsymbol{u} \in \mathbb{Z}_q^{(n+1)(n+2)/2}$

$$\langle \boldsymbol{s}, A\boldsymbol{u} \rangle = \rho \cdot \langle \boldsymbol{s}^2, \boldsymbol{u} \rangle$$

where $\boldsymbol{s}^2 = (s_i s_j)_{0 \le i \le j \le n}$.

RELIN*($\boldsymbol{s}$).*

For sake of simplicity, let us detail the construction for $n = 1$. The extension to the case $n > 1$ is straightforward and will be explained later. Let us first randomly generate a matrix M such that $\boldsymbol{s} = (1, s_1)$ is an eigenvector. The associated eigenvalue is denoted by ρ. The challenge consists of building $A = [a_{ij}]$ only knowing M (in particular, without knowing $\boldsymbol{s}$) satisfying $\langle \boldsymbol{s}, A\boldsymbol{u} \rangle = \rho \cdot \langle \boldsymbol{s}^2, \boldsymbol{u} \rangle$ for any in $\mathbb{Z}_q^3$ or equivalently

$$\begin{cases} a_{11} + a_{21}s_1 = \rho \\ a_{12} + a_{22}s_1 = \rho s_1 \\ a_{13} + a_{23}s_1 = \rho s_1^2 \end{cases}$$

First, we can remark that the vector $\boldsymbol{s} = (1, s_1)$ is an eigenvector of the matrix

$$\begin{bmatrix} a_{11}, a_{21} \\ a_{12}, a_{22} \end{bmatrix}$$

with the associated eigenvalue ρ. Thus, one can set this matrix to M. Let us see how to recover a_{31} and a_{32} in order to finish the construction of A. It is achieved by noting that the vectors s is also an eigenvector of the matrix

$$\begin{bmatrix} a_{12}, a_{22} \\ a_{13}, a_{23} \end{bmatrix}$$

For any $x, y \in \mathbb{Z}_n$ $\boldsymbol{s}$ is eigenvector of $T_{xy} = xI + yM$. To get the values (a_{13}, a_{23}), it suffices to adjust $x, y \in \mathbb{Z}_n$ in order that the first row of $T_{xy} = xI + yM$ is equal to (a_{12}, a_{22}). Let $T = [t_{ij}]$ be this matrix. Thus, one can choose $a_{13} = t_{21}$ and $a_{23} = t_{22}$ finishing the construction of A.

More generally, for $n > 1$, we proceed in the same way by considering the matrices $I, M, M^2, \ldots, M^n$ in the adjustment phase (to find T_{xy} in the case $n =$ 1).

□

Proposition 3. *Let $\boldsymbol{s} \leftarrow \mathsf{KeyGen}(\lambda)$ and $A \leftarrow$ RELIN($\boldsymbol{s}$).*

1. *A satisfies $\langle \boldsymbol{s}, A\boldsymbol{u} \rangle = \rho \cdot \langle \boldsymbol{s}^2, \boldsymbol{u} \rangle$ for any $\boldsymbol{u} \in \mathbb{Z}_q^{(n+1)(n+2)/2}$*
2. *There does not exist any p.p.t algorithm $\mathcal{B}$ such that $\mathcal{B}(A) = \boldsymbol{s}$ holds with non-negligible probability[29] assuming the hardness of factoring.*

[29] randomness coming from the choice of $\boldsymbol{s}$ and the internal randomness of RELIN.

Proof. Assertion 1 is true by construction. The matrix M is a randomly chosen matrix having at least one eigenvector. It follows that the characteristic polynomial p of M is a randomly chosen degree-n polynomial having at least one root. Assuming the hardness of factoring, p cannot be factored, implying that recovering at least one eigenvalue and thus one eigenvector of M is hard. Thus recovering $\boldsymbol{s}$ from M is hard assuming the hardness of factoring. We conclude by using the fact that A is polynomially derived from M.

□