TFHE Public-Key Encryption Revisited

Marc Joye

Zama, Paris, France

Abstract

This note introduces a public-key variant of TFHE. The output ciphertexts are of LWE type. Interestingly, the public key is shorter and the resulting ciphertexts are less noisy. The security of the scheme holds under the standard RLWE assumption. Several variations and extensions are also described.

Keywords: Fully homomorphic encryption (FHE) · Public-key encryption · Ring LWE (RLWE) · TFHE cryptosystem.

1 Public-Key TFHE Encryption

TFHE and its variants (e.g., [4, 3]) are natively private-key encryption schemes. The same key is used to encrypt or to decrypt messages. As already demonstrated in [6, § 6.1], certain private-key homomorphic encryption schemes can be turned into a public-key encryption scheme by providing encryptions of zero. See [12] for a more general result.

If $[\![\cdot]\!]_{\mathsf{sk}}$ denotes the probabilistic [private-key] encryption algorithm, the public encryption key consists of z encryptions of 0; i.e., $\mathsf{pk} = \big(a_1 \leftarrow [\![0]\!]_{\mathsf{sk}}, \dots, a_z \leftarrow [\![0]\!]_{\mathsf{sk}}\big)$. Let $\boxplus$ denote the ciphertext addition. The public-key encryption of a plaintext m then proceeds as follows:

- Draw a random bit-string $(r_1, \dots, r_z) \xleftarrow{\$} \{0, 1\}^z$;
- Compute a randomized encryption of zero as $S \leftarrow \boxplus_{i=1}^{z} r_i\, a_i$;

- Compute a trivial[1] encryption of m and get $M \leftarrow [\![m]\!]_{\mathsf{sk}}$;
- Output the ciphertext $C \leftarrow S \boxplus M$.

Noting that $C = [\![m]\!]_{\mathsf{sk}}$, the ciphertext C can be decrypted using the private key sk.

In the case of TFHE, the private decryption key is an n-bit string $\mathbf{s} = (s_1, \dots, s_n)$. The matching public encryption key is

$$\left\{(\mathbf{a_i}, b_i) \in (\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{Z}/q\mathbb{Z}\right\}_{1 \leqslant i \leqslant z}$$

where

$$\begin{cases} \mathbf{a_i} \xleftarrow{\$} (\mathbb{Z}/q\mathbb{Z})^n \\ b_i \leftarrow e_i + \sum_{j=1}^{n} (\mathbf{a_i})_j \, s_j \pmod q \end{cases}$$

and $(\mathbf{a_i})_j$ denotes the j-th component of vector $\mathbf{a_i}$. The encryption of a plaintext $m \in \mathbb{Z}/t\mathbb{Z}$ is given by $\mathbf{c} = (\mathbf{a}, b) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$ with $\mathbf{a} = \sum_{i=1}^{z} r_i \, \mathbf{a_i}$ and $b = \sum_{i=1}^{z} r_i \, b_i + \Delta m$ where $\Delta = q/t$. This assumes that t divides q. If not, an option is for example to define $\Delta = \lfloor q/t \rfloor$ (flooring), $\Delta = \lceil q/t \rceil$ (ceiling), or $\Delta = \lceil q/t \rfloor$ (rounding).

Another option is for example to define $\tilde{m} = \lfloor m\, q/t \rfloor$ (flooring), $\tilde{m} = \lceil m\, q/t \rceil$ (ceiling), or $\tilde{m} = \lceil m\, q/t \rfloor$ (rounding). The body b of the ciphertext is then defined as $b = \sum_{i=1}^{z} r_i \, b_i + \tilde{m}$. An example of plaintexts encoded using the flooring function is given in [11, Sect. 5] for $t = 2$.

Remark 1. Using matrix notation with vectors as column matrices, if we view the public key as the pair $\mathsf{pk} = (A, \mathbf{b})$ with

$$A = \begin{pmatrix} (\mathbf{a}_1)_1 & \dots & (\mathbf{a}_z)_1 \\ \vdots & & \vdots \\ (\mathbf{a}_1)_n & \dots & (\mathbf{a}_z)_n \end{pmatrix} \in (\mathbb{Z}/q\mathbb{Z})^{n \times z} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_z \end{pmatrix} \in (\mathbb{Z}/q\mathbb{Z})^z$$

where $\mathbf{b} = A^{\intercal} \mathbf{s} + \mathbf{e}$, then ciphertext $\mathbf{c}$ can be expressed as $\mathbf{c} = (\mathbf{a}, b)$ with $\mathbf{a} = A\, \mathbf{r}$ and $b = \mathbf{b}^{\intercal} \mathbf{r} + \Delta m$ where $\mathbf{r} = \begin{pmatrix} r_1 & \dots & r_z \end{pmatrix}^{\intercal} \in (\mathbb{Z}/q\mathbb{Z})^z$.

The decryption of a ciphertext $\mathbf{c} = (a_1, \dots, a_n, b) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$ proceeds in two steps. The first step is to recover the corresponding phase defined as

$$\phi_{\mathbf{s}}(\mathbf{c}) = b - \sum_{j=1}^{n} a_j \, s_j \bmod q$$

[1] A "trivial" encryption is an (insecure) encryption that can be obtained without the knowledge of the private key. The so-obtained ciphertext decrypts to the input plaintext.

which represents a noisy value of plaintext m. Indeed, it turns out from the definition that $\phi_s(\mathbf{c}) = \Delta m + \mathrm{Err}(\mathbf{c})$ (resp. $\phi_s(\mathbf{c}) = \tilde{m} + \mathrm{Err}(\mathbf{c})$). The second step is to remove the noise $\mathrm{Err}(\mathbf{c})$ to get Δm (resp. $\tilde{m}$) and, in turn, m.

Remark 2. The above description makes use of the ring $\mathbb{Z}/q\mathbb{Z}$. TFHE and the likes can similarly be defined over the discretized torus $\mathbb{T}_q = \frac{1}{q}\mathbb{Z}/\mathbb{Z}$; see [8].

In order to have a sufficient security margin, the leftover hash lemma teaches that the value of z should verify

$$z = (n+1)|q|_2 + \kappa\;;$$

the additional term κ, where κ is the security parameter, accounts for the corresponding subset-sum problems.

For a random variable X, its expectation is denoted by $\mathbb{E}[X]$ and its variance by $\mathrm{Var}(X)$; see Appendix A. Assuming that the noise e_i is centered and that its variance is bounded by the same threshold $\sigma^2 = \mathrm{Var}(e_i)$, the noise variance in an output ciphertext—where $\mathbf{r} \xleftarrow{\$} \{0,1\}^z$—is of $\frac{1}{2} z\sigma^2$. In the worst case, $\mathbf{r} = (1, 1, \dots, 1)$ and $\mathrm{Var}(\mathrm{Err}(\mathbf{c})) = z\sigma^2$.

Proof. Let $\mathbf{c}$ denote the output ciphertext. It is easy to check that $\phi_s(\mathbf{c}) = \sum_{i=1}^{z} r_i\, e_i + \Delta m$ and thus $\mathrm{Err}(\mathbf{c}) = \sum_{i=1}^{z} r_i\, e_i$. Noting that for a uniform bit b in $\{0,1\}$, $\mathbb{E}[b] = 1/2$ and $\mathrm{Var}(b) = 1/4$, it follows that $\mathrm{Var}(\mathrm{Err}(\mathbf{c})) = \sum_{i=1}^{z} \mathrm{Var}(r_i\, e_i) = \sum_{i=1}^{z} \big(\frac{1}{4}\,\sigma^2 + \frac{1}{4}\,0 + \sigma^2\,(\frac{1}{2})^2\big) = z\,\frac{1}{2}\,\sigma^2$. If $\mathbf{r} = (1, 1, \dots, 1)$ then $\mathrm{Var}(\mathrm{Err}(\mathbf{c})) = \sum_{i=1}^{z} \mathrm{Var}(e_i) = z\sigma^2$. □

Further, assuming the masks $\mathbf{a}_i$ are derived from a random seed $\vartheta \in \{0,1\}^\kappa$ where κ is the security parameter, the size of the public encryption key is of $|\vartheta|_2 + \big((n+1)|q|_2 + \kappa\big)\,|q|_2$ bits.

Illustration For example, at the 128-bit security level, with $n = 1024$, $q = 2^{64}$ and $\sigma = 2^{-25}q = 2^{39}$, we have $z = 65728 \approx 2^{16}$. This results in an increase of the noise variance in an output ciphertext by an expected factor of 2^{15}. With $\sigma = 2^{39}$, the standard deviation of the noise in an output ciphertext is of $2^{46.5}$. We also have that the public encryption key takes 4206720 bits, that is, about 526 kB.

2 Smaller Public Keys, Less Noisy Ciphertexts

It is useful to introduce a new vector operator. The *reverse negative wrapped convolution* of two vectors $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ is the vector $\mathbf{w} = \mathbf{u} \circledast \mathbf{v} = (\mathbf{u} \circledast_1 \mathbf{v}, \ldots, \mathbf{u} \circledast_n \mathbf{v}) \in \mathbb{Z}^n$ defined by

$$w_i = \mathbf{u} \circledast_i \mathbf{v} = \textstyle\sum_{j=1}^{i} u_j\, v_{n+j-i} - \sum_{j=i+1}^{n} u_j\, v_{j-i} \ .$$

For example, $(1, 2, 3) \circledast (4, 5, 6)$ is the vector $(-17, 5, 32)$.

Remark 3. For a vector $\mathbf{v} \in \mathbb{Z}^n$, $\overleftarrow{\mathbf{v}}$ denotes vector $\mathbf{v}$ in reverse order; i.e., if $\mathbf{v} = (v_1, \ldots, v_n)$ then $\overleftarrow{\mathbf{v}} = (v_n, \ldots, v_1)$. The above convolution bears its name from the classical negative wrapped convolution (a.k.a. skew circular convolution or negacyclic convolution) defined by $\mathbf{w} = \mathbf{u} * \mathbf{v}$ where $w_i = \sum_{j=1}^{i} u_j\, v_{i+1-j} - \sum_{j=i+1}^{n} u_j\, v_{n+1+i-j}$. Indeed, it turns out that $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \overleftarrow{\mathbf{v}}$.

The main properties of the reverse negative wrapped convolution are captured by the next lemma.

Lemma 1. *Given three vectors $\mathbf{t}, \mathbf{u}, \mathbf{v} \in \mathbb{Z}^n$, it holds that*

1. $\mathbf{u} \circledast \mathbf{v} = \overleftarrow{\mathbf{v}} \circledast \overleftarrow{\mathbf{u}}$;
2. $\mathbf{u} \circledast_n \mathbf{v} = \langle \mathbf{u}, \mathbf{v} \rangle$;
3. $\langle \mathbf{t} \circledast \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{t} \circledast \mathbf{v}, \mathbf{u} \rangle$.

Proof. The first property is immediate. Since $*$ is commutative, it follows that $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \overleftarrow{\mathbf{v}} = \overleftarrow{\mathbf{v}} * \mathbf{u} = \overleftarrow{\mathbf{v}} \circledast \overleftarrow{\mathbf{u}}$.

Now, write $\mathbf{t} = (t_1, \ldots, t_n)$, $\mathbf{u} = (u_1, \ldots, u_n)$, and $\mathbf{v} = (v_1, \ldots, v_n)$. From the definition, denoting [pred] $= 1$ if some predicate pred is true and [pred] $= 0$ otherwise, we can express $\mathbf{u} \circledast_i \mathbf{v}$ compactly as

$$\sum_{j=1}^{n} (-1)^{[j>i]}\, u_j\, v_{[j \leqslant i]n+j-i} \ .$$

Plugging $i = n$, we so get $\mathbf{u} \circledast_n \mathbf{v} = \sum_{j=1}^{n} u_j\, v_j = \langle \mathbf{u}, \mathbf{v} \rangle$.

Likewise, we also get

$$\begin{aligned} \langle \mathbf{t} \circledast \mathbf{u}, \mathbf{v} \rangle &= \sum_{i=1}^{n} \left(\textstyle\sum_{j=1}^{n} (-1)^{[j>i]}\, t_j\, u_{[j \leqslant i]n+j-i} \right) v_i \\ &= \sum_{j=1}^{n} t_j \left(\textstyle\sum_{i=1}^{n} (-1)^{[i<j]}\, u_{[i \geqslant j]n+j-i}\, v_i \right) \end{aligned}$$

$$= \sum_{j=1}^{n} t_j \left(-\sum_{i=1}^{j-1} u_{j-i}\, v_i + \sum_{i=j}^{n} u_{n+j-i}\, v_i\right)$$

$$= \sum_{j=1}^{n} t_j \left(-\sum_{i=1}^{j-1} v_{j-i}\, u_i + \sum_{i=j}^{n} v_{n+j-i}\, u_i\right)$$

$$= \langle \mathbf{t} \circledast \mathbf{v}, \mathbf{u} \rangle$$

by symmetry. □

2.1 Description

Equipped with the $\circledast$ operator, we can now present a public-key cryptosystem. Interestingly, the encryption algorithm outputs regular LWE-type ciphertexts. As a consequence, the decryption algorithm is unchanged.

A public-key LWE-type scheme

KeyGen(1^κ) On input security parameter κ, define an integer $n = 2^\eta$ for some $\eta > 0$, select positive integers t and q with $t \mid q$, let $\Delta = q/t$, and define two discretized error distributions $\hat{\chi}_1$ and $\hat{\chi}_2$ over $\mathbb{Z}$.

Sample uniformly at random a vector $\mathbf{s} = (s_1, \ldots, s_n) \xleftarrow{\$} \{0,1\}^n$. Using $\mathbf{s}$, select uniformly at random a vector $\mathbf{a} \xleftarrow{\$} (\mathbb{Z}/q\mathbb{Z})^n$ and form the vector $\mathbf{b} = \mathbf{a} \circledast \mathbf{s} + \mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^n$ with $\mathbf{e} \leftarrow \hat{\chi}_1{}^n$.

The plaintext space is $\mathcal{M} = \{0, 1, \ldots, t-1\}$. The public parameters are $\mathsf{pp} = \{n, \sigma, t, q, \Delta\}$, the public key is $\mathsf{pk} = (\mathbf{a}, \mathbf{b})$, and the private key is $\mathsf{sk} = \mathbf{s}$.

Encrypt$_{\mathsf{pk}}(m)$ The public-key encryption of a plaintext $m \in \mathcal{M}$ is given by $\mathbf{c} = (\mathbf{a}, b) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$ with

$$\begin{cases} \mathbf{a} = \mathbf{a} \circledast \mathbf{r} + \mathbf{e}_1 \\ b = \langle \mathbf{b}, \mathbf{r} \rangle + \Delta m + e_2 \end{cases}$$

for a random vector $\mathbf{r} \xleftarrow{\$} \{0,1\}^n$, and where $\mathbf{e}_1 \leftarrow \hat{\chi}_1{}^n$ and $e_2 \leftarrow \hat{\chi}_2$.

Decrypt$_{\mathsf{sk}}(\mathbf{c})$ To decrypt $\mathbf{c} = (\mathbf{a}, b)$, using secret decryption key $\mathbf{s}$, return

$$\lceil (\mu^* \bmod q)/\Delta \rfloor \bmod t$$

where $\mu^* = b - \langle \mathbf{a}, \mathbf{s} \rangle$.

2.2 Correctness

Let $\mathbf{c} = (\mathbf{a}, b) \leftarrow \mathrm{Encrypt}_{\mathsf{pk}}(m)$. Then, by Lemma 1, we have $b - \langle \mathbf{a}, \mathbf{s} \rangle = \langle \mathbf{a} \circledast \mathbf{s} + \mathbf{e}, \mathbf{r} \rangle + \Delta m + e_2 - \langle \mathbf{a} \circledast \mathbf{r} + \mathbf{e}_1, \mathbf{s} \rangle = \Delta m + e_2 + \langle \mathbf{e}, \mathbf{r} \rangle - \langle \mathbf{e}_1, \mathbf{s} \rangle + \langle \mathbf{a} \circledast \mathbf{s}, \mathbf{r} \rangle - \langle \mathbf{a} \circledast \mathbf{r}, \mathbf{s} \rangle = \Delta m + E$ where $E = e_2 + \langle \mathbf{e}, \mathbf{r} \rangle - \langle \mathbf{e}_1, \mathbf{s} \rangle$. Decryption correctness thus requires that $|E| < \Delta/2$.

2.3 Security

We state the semantic security [7] of the proposed cryptosystem under the RLWE assumption [9] in $\mathbb{Z}_{n,q}[X] \coloneqq (\mathbb{Z}/q\mathbb{Z})[X]/(X^n + 1)$.

Definition 1 (RLWE Assumption). Given a security parameter κ, let $n, q \in \mathbb{N}$ with n a power of 2 and let $\mathscr{s} \xleftarrow{\$} \mathbb{B}[X]/(X^n + 1)$ where $\mathbb{B} = \{0, 1\}$. Let also $\hat{\chi}$ be an error distribution over $\mathbb{Z}[X]/(X^n + 1)$; namely, over polynomials of $\mathbb{Z}[X]/(X^n + 1)$ with coefficients drawn according to $\hat{\chi}$. The *ring learning with errors (RLWE) problem* is to distinguish samples chosen according to the following distributions:

$$\mathrm{dist}_0(1^\kappa) = \left\{ (\mathscr{a}, \mathscr{b}) \mid \mathscr{a} \xleftarrow{\$} \mathbb{Z}_{n,q}[X], \mathscr{b} \xleftarrow{\$} \mathbb{Z}_{n,q}[X] \right\}$$

and

$$\mathrm{dist}_1(1^\kappa) = \Big\{ (\mathscr{a}, \mathscr{b}) \mid \mathscr{a} \xleftarrow{\$} \mathbb{Z}_{n,q}[X], \\ \mathscr{b} = \mathscr{a}\,\mathscr{s} + \mathscr{e} \in \mathbb{Z}_{n,q}[X], \mathscr{e} \leftarrow \hat{\chi} \Big\} \;.$$

The *RLWE assumption* posits that for all probabilistic polynomial-time algorithms $\mathcal{R}$, the function

$$\Big| \Pr\big[\mathcal{R}(\mathscr{a}, \mathscr{b}) = 1 \mid (\mathscr{a}, \mathscr{b}) \xleftarrow{\$} \mathrm{dist}_0(1^\kappa)\big] - \\ \Pr\big[\mathcal{R}(\mathscr{a}, \mathscr{b}) = 1 \mid (\mathscr{a}, \mathscr{b}) \xleftarrow{\$} \mathrm{dist}_1(1^\kappa)\big] \Big|$$

is negligible in κ.

We identify polynomials in $\mathbb{Z}_{n,q}[X]$ with their coefficient vectors in $(\mathbb{Z}/q\mathbb{Z})^n$, and conversely. A vector $\mathbf{u} = (u_1, \dots, u_n) \in (\mathbb{Z}/q\mathbb{Z})^n$ corresponds to polynomial $\mathscr{u} = \sum_{i=0}^{n-1} u_{j+1} X^j \in \mathbb{Z}_{n,q}[X]$; the correspondence is written $\mathbf{u} \cong \mathscr{u}$.

The next lemma relates the corresponding operations.

Lemma 2. *Let* $\mathbf{u} = (u_1, \dots, u_n)$ *and* $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{Z}/q\mathbb{Z})^n$. *Let also* $\mathcal{u} = \sum_{j=0}^{n-1} u_{j+1} X^j$ *and* $\mathcal{v} = \sum_{j=0}^{n-1} v_{j+1} X^j \in \mathbb{Z}_{n,q}[X]$. *Then*

$$\mathbf{u} \circledast \overleftarrow{\mathbf{v}} = \mathbf{v} \circledast \overleftarrow{\mathbf{u}} \cong \mathcal{u} \cdot \mathcal{v} \quad .$$

Proof. From Remark 3, if $*$ denotes the negative wrapped convolution, it turns out that $\boldsymbol{w} = (w_1, \dots, w_n) := \mathbf{u} \circledast \overleftarrow{\mathbf{v}} = \mathbf{u} * \mathbf{v}$ with $w_i = \sum_{j=1}^{i} u_j\, v_{i+1-j} - \sum_{j=i+1}^{n} u_j\, v_{n+1+i-j}$. Now looking at the corresponding polynomials $\mathcal{u}$ and $\mathcal{v}$, it is easily seen that their multiplication in $\mathbb{Z}_{n,q}[X] = (\mathbb{Z}/q\mathbb{Z})[X](X^n+1)$ yields polynomial $\mathcal{w} = \sum_{j=0}^{n-1} w_{j+1} X^j$. Hence, we have $\boldsymbol{w} \cong \mathcal{w}$ or, equivalently, $\mathbf{u} \circledast \overleftarrow{\mathbf{v}} \cong \mathcal{u} \cdot \mathcal{v}$. The equality $\mathbf{u} \circledast \overleftarrow{\mathbf{v}} = \mathbf{v} \circledast \overleftarrow{\mathbf{u}}$ follows from Lemma 1. □

Back to the encryption scheme, it is instructive to observe that the public key $\mathsf{pk} = (\mathfrak{a}, \mathfrak{b} = \mathfrak{a} \circledast \mathbf{s} + \boldsymbol{e})$ corresponds to a (polynomial) RLWE sample under secret key $\sum_{j=0}^{n-1} s_{n-j} X^j \cong \overleftarrow{\mathbf{s}} = (s_n, \dots, s_1)$. Under the RLWE assumption, the public key as output by the key generation algorithm is therefore pseudo-random; i.e., indistinguishable from uniform. Regarding a ciphertext $\mathbf{c} = (\mathbf{a}, b)$ with $\mathbf{a} = \mathfrak{a} \circledast \mathbf{r} + \boldsymbol{e}_1$ and $b = \langle \mathfrak{b}, \mathbf{r} \rangle + \Delta m + e_2$, consider the vector $\mathbf{b} := \mathfrak{b} \circledast \mathbf{r} + \boldsymbol{e}_2$ for some $\boldsymbol{e}_2 \in \hat{\chi}_2{}^n$ such that $(\boldsymbol{e}_2)_n = e_2$. Again, it is worth noting that the pairs $(\mathfrak{a}, \mathbf{a} = \mathfrak{a} \circledast \mathbf{r} + \boldsymbol{e}_1)$ and $(\mathfrak{b}, \mathbf{b} = \mathfrak{b} \circledast \mathbf{r} + \boldsymbol{e}_2)$ correspond respectively to two (polynomial) RLWE samples under 'secret key' $\sum_{j=0}^{n-1} r_{n-j} X^j \cong \overleftarrow{\mathbf{r}}$ and thus appear to be pseudo-random. The same is true for $\langle \mathfrak{b}, \mathbf{r} \rangle + e_2$ since, from Lemma 1, this turns out to be the n^{th} component of vector $\mathfrak{b} \circledast \mathbf{r} + \boldsymbol{e}_2$: $\langle \mathfrak{b}, \mathbf{r} \rangle + e_2 = \mathfrak{b} \circledast_n \mathbf{r} + (\boldsymbol{e}_2)_n$. It is also important that the randomness can be re-used in multiple ciphertexts provided they are all encrypted under different keys. This follows from [2]. Indeed, when the randomness is given explicitly in a ciphertext, it is readily verified that the "reproducibility" criterion [1, Definition 9.3] is satisfied.

The semantic security under the RLWE assumption is established by a series of hybrid games where the different RLWE samples are successively replaced with uniform samples.

2.4 Performance

The public key expands to $2n|q|_2$ bits. If the component $\mathfrak{a}$ of the public key is generated from a random seed, the public key only requires $n|q|_2 + \kappa$ bits for its storage or transmission. With the example parameters of Section 1, this amounts to 65664 bits, or about 8.2 kB.

Suppose $\hat{\chi}_i = \mathcal{N}(0, {\sigma_i}^2)$ for $i \in \{1, 2\}$. For a ciphertext $\mathbf{c}$ output by the encryption algorithm, from Section 2.2, the noise variance satisfies

$\mathrm{Var}(\mathrm{Err}(\mathbf{c})) = \mathrm{Var}(e_2 + \langle \boldsymbol{e}, \mathbf{r}\rangle - \langle \boldsymbol{e}_1, \mathbf{s}\rangle) = \mathrm{Var}(e_2) + \sum_{j=1}^{n} \mathrm{Var}((\boldsymbol{e})_i\, r_i) + \sum_{j=1}^{n} \mathrm{Var}((\boldsymbol{e}_1)_j\, s_j) = {\sigma_2}^2 + 2n\big({\sigma_1}^2\, \frac{1}{4} + {\sigma_1}^2\, (\frac{1}{2})^2 + \frac{1}{4}\, 0\big) = {\sigma_2}^2 + n\, {\sigma_1}^2$. Again, with the example parameters of Section 1, for ${\sigma_1}^2 = {\sigma_2}^2$, this translates in an increase of $n + 1 \approx 2^{10}$ in the noise variance. With $\sigma_1 = \sigma_2 = 2^{39}$, the standard deviation of the noise in an output ciphertext is of 2^{44}. Larger values for ciphertext modulus q lead to larger gains compared to the direct approach using encryptions of 0 for the public key (Section 1).

3 Generalization

Let $\mathscr{p}$ be a monic (irreducible) polynomial of degree n. Let also $\mathfrak{R}$ and $\mathfrak{R}_q$ denote the polynomial rings $\mathbb{Z}[X]/(\mathscr{p}(X))$ and $\mathfrak{R}/(q) = (\mathbb{Z}/q\mathbb{Z})[X]/(\mathscr{p}(X))$, respectively. A polynomial $\mathscr{a} \in \mathfrak{R}$ (resp. $\mathscr{a} \in \mathfrak{R}_q$) of degree less than n and given by $\mathscr{a}(X) = \sum_{i=0}^{n-1} a_i\, X^i$ with $a_i \in \mathbb{Z}$ (resp. $a_i \in \mathbb{Z}/q\mathbb{Z}$) can be identified with its coefficient vector $\mathbf{a} := (a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}^n$ (resp. $\in (\mathbb{Z}/q\mathbb{Z})^n$). Over $\mathfrak{R}_q$, we let Υ_q denote the corresponding map

$$\begin{aligned} \Upsilon_q \colon \mathfrak{R}_q &\xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^n, \\ &\qquad \mathscr{a} = \textstyle\sum_{i=0}^{n-1} a_i\, X^i \longmapsto \Upsilon_q(\mathscr{a}) = (a_0, a_1, \dots, a_{n-1}) \ . \end{aligned}$$

This one-to-one correspondence defines the convolution $*$ between two vectors in $(\mathbb{Z}/q\mathbb{Z})^n$. Given $\mathbf{a}, \mathbf{b} \in (\mathbb{Z}/q\mathbb{Z})^n$, their convolution is defined as

$$\mathbf{a} * \mathbf{b} = \Upsilon_q\big({\Upsilon_q}^{-1}(\mathbf{a}) \cdot {\Upsilon_q}^{-1}(\mathbf{b})\big) \in (\mathbb{Z}/q\mathbb{Z})^n$$

where $\cdot$ denote the polynomial multiplication in $\mathfrak{R}_q$.

Interestingly, the convolution operator allows expressing a ring-LWE (in short, RLWE) ciphertext with vectors. One advantage of RLWE-type encryption is that it comes with an efficient public-key variant. For example, adapting [5, Sect. 3.2] following [10] (see also [9]), an RLWE public-key encryption scheme can be abstracted as follows. The key generation draws at random a small secret key $\mathscr{s} \in \mathfrak{R}$ and forms the matching public key $(\mathscr{A}, \mathscr{B}) \in (\mathfrak{R}_q)^2$ where $\mathscr{A}$ is a random polynomial in $\mathfrak{R}_q$ and $\mathscr{B} = \mathscr{A} \cdot \mathscr{s} + \mathscr{e}$ for a small random noise error $\mathscr{e} \in \mathfrak{R}$. Let $t \mid q$ and $\Delta = q/t$. The public-key encryption of a plaintext $\mathscr{m} := \mathscr{m}(X) = \sum_{i=0}^{n-1} m_i\, X^i \in \mathfrak{R}_t$ is given by the pair of polynomials $(\mathscr{a}, \mathscr{b}) \in (\mathfrak{R}_q)^2$ with

$$\begin{cases} \mathscr{a} = \mathscr{A} \cdot \mathscr{r} + \mathscr{e}_1 \\ \mathscr{b} = \mathscr{B} \cdot \mathscr{r} + \Delta\, \mathscr{m} + \mathscr{e}_2 \end{cases}$$

for some small random polynomial $\mathscr{r} \in \mathfrak{R}$ and small random noise errors $\mathscr{e}_1, \mathscr{e}_2 \in \mathfrak{R}$. The decryption of ciphertext $(\mathscr{a}, \mathscr{b})$, using secret key $\mathscr{s}$, proceeds in two steps: (i) compute in $\mathfrak{R}_q$ the phase $\mathscr{b} - \mathscr{a} \cdot \mathscr{s} = \Delta\,\mathscr{m} + \mathscr{E}$ with $\mathscr{E} := \mathscr{e} \cdot \mathscr{r} + \mathscr{e}_2 - \mathscr{e}_1 \cdot \mathscr{s} \in \mathfrak{R}$, and (ii) remove $\mathscr{E}$ to get $\Delta\,\mathscr{m}$ and, in turn, $\mathscr{m} \in \mathfrak{R}_t$.

Using the convolution operator as defined above, we get the corresponding formulation using vectors. The secret key is a small vector $\mathbf{s} \in \mathbb{Z}^n$ and the public key is a pair of vectors $(\mathbf{A}, \mathbf{B})$ where $\mathbf{A}$ is a random vector in $(\mathbb{Z}/q\mathbb{Z})^n$ and $\mathbf{B} = \mathbf{A} * \mathbf{s} + \boldsymbol{e} \pmod q$ for some small random vector $\boldsymbol{e} \in \mathbb{Z}^n$. Then encryption of a plaintext $\mathbf{m}$ seen as a vector in $(\mathbb{Z}/t\mathbb{Z})^n$ is given by the pair of vectors $(\mathbf{a}, \mathbf{b})$ in $(\mathbb{Z}/q\mathbb{Z})^n$ where

$$\begin{cases} \mathbf{a} = \mathbf{A} * \mathbf{r} + \mathbf{e}_1 \\ \mathbf{b} = \mathbf{B} * \mathbf{r} + \Delta\,\mathbf{m} + \mathbf{e}_2 \end{cases} \tag{1}$$

for some small random vector $\mathbf{r} \in \mathbb{Z}^n$ and small random noise errors $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{Z}^n$. Next, given ciphertext $(\mathbf{a}, \mathbf{b})$, plaintext $\mathbf{m}$ can be recovered using secret key $\mathbf{s}$ from the phase $\mathbf{b} - \mathbf{a} * \mathbf{s} = \Delta\,\mathbf{m} + \mathbf{E} \pmod q$ where $\mathbf{E} := \mathbf{e} * \mathbf{r} + \mathbf{e}_2 - \mathbf{e}_1 * \mathbf{s} \in \mathbb{Z}^n$.

Three important observations are in order:

1. If b_i (resp. m_i) denotes the i-th component of vector $\mathbf{b}$ (resp. $\mathbf{m}$) in (1) then the pair $(\mathbf{a}, b_i)$ is an LWE-type encryption of message $m_i \in \mathbb{Z}/t\mathbb{Z}$ provided that

   $$b_i - \langle \mathbf{a}, \mathbf{s} \rangle = \Delta\,m_i + (\text{small noise}) \ .$$

   In particular, we have

   $$\begin{aligned} b_i - \langle \mathbf{a}, \mathbf{s} \rangle &= (\mathbf{B} * \mathbf{r})_i + \Delta\,m_i + (\mathbf{e}_2)_i - \langle \mathbf{A} * \mathbf{r} + \mathbf{e}_1, \mathbf{s} \rangle \\ &= \big((\mathbf{A} * \mathbf{s} + \mathbf{e}) * \mathbf{r}\big)_i + \Delta\,m_i + (\mathbf{e}_2)_i - \langle \mathbf{A} * \mathbf{r} + \mathbf{e}_1, \mathbf{s} \rangle \\ &= \Delta\,m_i + (\mathbf{A} * \mathbf{s} * \mathbf{r})_i - \langle \mathbf{A} * \mathbf{r}, \mathbf{s} \rangle \\ &\qquad\qquad + (\mathbf{e} * \mathbf{r})_i + (\mathbf{e}_2)_i - \langle \mathbf{e}_1, \mathbf{s} \rangle \ . \end{aligned}$$

   As a consequence, if the condition

   $$(\mathbf{A} * \mathbf{s} * \mathbf{r})_i \approx \langle \mathbf{A} * \mathbf{r}, \mathbf{s} \rangle \tag{2}$$

   is satisfied, one ends up with an LWE-type ciphertext for plaintext $m_i \in \mathbb{Z}/t\mathbb{Z}$.

2. If the public key is replaced with $(\mathbf{A}, \mathbf{B} = \mathbf{A} * \varphi_1(\mathbf{s}) + \mathbf{e}) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^n$ for some (bijective) map $\varphi_1\colon (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})^n$ then Condition (2) relaxes to

$$(\mathbf{A} * \varphi_1(\mathbf{s}) * \mathbf{r})_i \approx \langle \mathbf{A} * \mathbf{r}, \mathbf{s} \rangle \ . \tag{3}$$

3. Further, the above encryption scheme is unchanged if vector $\mathbf{r}$ is replaced with vector $\varphi_2(\mathbf{r})$ for some (bijective) map $\varphi_2\colon (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})^n$. In particular, taking $\varphi_2 = \varphi_1$ and letting $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \varphi_1(\mathbf{v})$, Condition (3) can be written as

$$(\mathbf{A} \circledast \mathbf{s} \circledast \mathbf{r})_i = (\mathbf{A} \circledast \mathbf{r} \circledast \mathbf{s})_i \approx \langle \mathbf{A} \circledast \mathbf{r}, \mathbf{s} \rangle \ . \tag{4}$$

We argue that one can find a map φ_1 such that Condition (4) is strictly verified. Define $\mathbf{C} = \mathbf{A} \circledast \mathbf{r} = (C_1, \dots, C_n)$ and write $\varphi_1(\mathbf{s}) = (s'_1, \dots, s'_n)$. Then

$$\begin{aligned}&(\mathbf{C} \circledast \mathbf{s})_i := (\mathbf{C} * \varphi_1(\mathbf{s}))_i = \langle \mathbf{C}, \mathbf{s} \rangle \iff \\ &\left(\Upsilon_q\left(\left(\textstyle\sum_{j=1}^n C_j X^{j-1}\right) \cdot \left(\textstyle\sum_{j=1}^n s'_j X^{j-1}\right)\right)\right)_i = \textstyle\sum_{j=1}^n C_j s_j \pmod{q} \ . \end{aligned} \tag{5}$$

The left-hand side of the last equation can be rewritten as

$$\sum_{j=1}^{n} C_j \left(\textstyle\sum_{k=1}^n \alpha_{j,k}\, s'_k\right) \tag{6}$$

for some $\alpha_{j,k} \in \mathbb{Z}/q\mathbb{Z}$ given by the multiplication $\cdot$ in $\mathfrak{R}_q$. Equating each multiplier of C_j yields a system of n equations, $\sum_{k=1}^n \alpha_{j,k}\, s'_k = s_j$ (for $1 \leqslant j \leqslant n$), from which values for $s'_1, \dots, s'_n$ can be derived and, in turn, map φ_1.

This leads to the following public-key encryption scheme. For security reasons, we restrict quotient polynomial $\mathcal{P}(X)$ to cyclotomic polynomials $\Phi_M(X)$. We so have $\mathfrak{R}_q = (\mathbb{Z}/q\mathbb{Z})[X]/(\Phi_M(X))$ with $n = \deg(\Phi_M)$. The multiplication in $\mathfrak{R}_q$ is denoted by $\cdot$ and the corresponding convolution in $(\mathbb{Z}/q\mathbb{Z})^n$ by $*$. The 'specialized' convolution operator in $(\mathbb{Z}/q\mathbb{Z})^n$ is denoted by $\circledast$. For any two vectors $\mathbf{u}, \mathbf{v} \in (\mathbb{Z}/q\mathbb{Z})^n$, we define $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \varphi_1(\mathbf{v})$. With this corresponding definition of φ_1, it holds by construction that $\mathbf{u} \circledast_i \mathbf{v} = \langle \mathbf{u}, \mathbf{v} \rangle$; see Equation (5).

A public-key LWE-type scheme (General case)

KeyGen(1^κ) On input security parameter κ, define an integer $n = \phi(M)$ for some integer M and where ϕ denotes Euler's totient function, select positive integers t and q with $t \mid q$, let $\Delta = q/t$, and define two discretized error distributions $\hat{\chi}_1$ and $\hat{\chi}_2$ over $\mathbb{Z}$.

Sample uniformly at random a vector $\mathbf{s} = (s_1, \dots, s_n) \xleftarrow{\$} \{0,1\}^n$. Using $\mathbf{s}$, select uniformly at random a vector $\mathfrak{a} \xleftarrow{\$} (\mathbb{Z}/q\mathbb{Z})^n$ and form the vector $\mathfrak{b} = \mathfrak{a} \circledast \mathbf{s} + \mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^n$ with $\mathbf{e} \leftarrow \hat{\chi}_1{}^n$.

The plaintext space is $\mathcal{M} = \{0, 1, \dots, t-1\}$. The public parameters are $\mathsf{pp} = \{n, \sigma, t, q, \Delta\}$, the public key is $\mathsf{pk} = (\mathfrak{a}, \mathfrak{b})$, and the private key is $\mathsf{sk} = \mathbf{s}$.

Encrypt$_{\mathsf{pk}}(m)$ The public-key encryption of a plaintext $m \in \mathcal{M}$ is given by $\mathbf{c} = (\mathbf{a}, b) \in (\mathbb{Z}/q\mathbb{Z})^{n+1}$ with

$$\begin{cases} \mathbf{a} = \mathfrak{a} \circledast \mathbf{r} + \mathbf{e}_1 \\ b = \langle \mathfrak{b}, \mathbf{r} \rangle + \Delta m + e_2 \end{cases}$$

for a random vector $\mathbf{r} \xleftarrow{\$} \{0,1\}^n$, and where $\mathbf{e}_1 \leftarrow \hat{\chi}_1{}^n$ and $e_2 \leftarrow \hat{\chi}_2$.

Decrypt$_{\mathsf{sk}}(\mathbf{c})$ To decrypt $\mathbf{c} = (\mathbf{a}, b)$, using secret decryption key $\mathbf{s}$, return

$$\lceil (\mu^* \bmod q)/\Delta \rfloor \bmod t$$

where $\mu^* = b - \langle \mathbf{a}, \mathbf{s} \rangle$.

Remark 4. Applied the basic scheme given in Section 2, this corresponds to $M = 2^{\eta+1}$, $\mathcal{p}(X) = X^n + 1$ with $n = 2^\eta$ and, letting $\mathbf{s} = (s_1, \dots, s_n)$, $\varphi_1(\mathbf{s}) = (s_n, \dots, s_1)$. Indeed, for $i = n$ and $\mathcal{p}(X) = X^n + 1$, left-hand side of Equation (5) becomes

$$\left(\Upsilon_q\left(\left(\sum_{j=1}^n C_j X^{j-1}\right) \cdot \left(\sum_{j=1}^n s_j' X^{j-1}\right)\right)\right)_n = \sum_{j=1}^n C_j\, s'_{n+1-j}$$

that is, comparing with Equation (6),

$$(\alpha_{j,k})_{\substack{1\leqslant j\leqslant n\\1\leqslant k\leqslant n}} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1\\ 0 & 0 & \dots & 1 & 0\\ \vdots & \vdots & \iddots & & \vdots\\ 0 & 1 & \dots & 0 & 0\\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} .$$

Equating each multiplier of C_j with those of $\sum_{j=1}^{n} C_j\, s_j$ yields $s'_{n+1-j} = s_j$ or, equivalently, $(s'_1, \dots, s'_n) = (s_n, \dots, s_1)$; and thus $\varphi_1(\mathbf{s}) = (s_n, \dots, s_1)$.

Remark 5. The map φ_1 in the basic scheme of Section 2 is obtained by selecting $i = n$; namely, $\varphi_1(\mathbf{s}) = (s_n, \dots, s_1)$. However, another vector convolution operator that is 'compatible' with the multiplication in $\mathfrak{R}_q = \mathbb{Z}_{n,q}[X] \coloneqq (\mathbb{Z}/q\mathbb{Z})/(X^n + 1)$ can be used. An alternative therefore consists in choosing another value for i. For a general value for $i \neq n$, the vector $\mathbf{s} = (s_1, \dots, s_n)$ is mapped to

$$\begin{aligned}\varphi_1(\mathbf{s}) &= (s_i, \dots, s_1, -s_n, \dots, -s_{i+1})\\ &= \left((-1)^{[j>i]}\, s_{1+(i-j \bmod n)}\right)_{1\leqslant j\leqslant n} .\end{aligned}$$

For example, for $i = n - 1$, we get $\varphi_1(\mathbf{s}) = (s_{n-1}, \dots, s_1, -s_n)$. The matching specialized convolution operator is defined as $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \varphi_1(\mathbf{v})$ for any two vectors $\mathbf{u}$ and $\mathbf{v}$, where $*$ denotes the classical negative wrapped convolution operator.

The general construction presents the advantage that the condition n being a power of two can be relaxed. For quotient polynomial $\mathcal{p}(X) = \Phi_M(X)$, the corresponding value for n is given by the Euler's totient function of M. For example, if $M = 3^w$ then $n = 2 \cdot 3^{w-1} = 2M/3$ and $\mathcal{p}(X) = X^n + X^{n/2} + 1$. For $i = n$, $*$ corresponds to the multiplication in $(\mathbb{Z}/q\mathbb{Z})[X]/(X^n + X^{n/2} + 1)$ and

$$\begin{aligned}\varphi_1(\mathbf{s}) = (&s_n + s_{n/2}, s_{n-1} + s_{n/2-1}, \dots, s_{n-(n/2-1)} + s_{n/2-(n/2-1)},\\ &s_{n/2}, s_{n/2} - 1, \dots, s_{n/2-(n/2-1)})\\ = \big(&s_{n+1-j} + [j \leqslant n/2]\, s_{1+(n/2-j \bmod n)}\big)_{1\leqslant j\leqslant n} .\end{aligned}$$

Again, by construction, letting $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \varphi_1(\mathbf{v})$, it holds that $\mathbf{u} \circledast_n \mathbf{v} = \langle \mathbf{u}, \mathbf{v} \rangle$ for any two vectors $\mathbf{u}$ and $\mathbf{v}$.

4 Encrypting Multiple Plaintexts

When multiple plaintexts need to be encrypted, the natural way is to encrypt them individually. For Z plaintexts this requires $Z \cdot (n+1) \lceil \log_2 q \rceil$ bits for the corresponding ciphertexts. We show in this section how to only make use of $(\lceil Z/n \rceil n + Z) \lceil \log_2 q \rceil$ bits. This saves

$$(Z - \lceil Z/n \rceil) \cdot n \lceil \log_2 q \rceil$$

bits.

Given an LWE dimension n and a convolution operator $*$ operating on n-dimensional vectors, fix an integer $i \in \{1, \dots, n\}$. This integer i defines a map φ_1 and, in turn, the matching specialized convolution operator $\circledast$ as $\mathbf{u} \circledast \mathbf{v} = \mathbf{u} * \varphi_1(\mathbf{v})$ for any two n-dimensional vectors $\mathbf{u}$ and $\mathbf{v}$. As detailed in the previous sections, this operator $\circledast$ gives rise to a public-key encryption scheme. With the previous notations, a plaintext m is encrypted under public key $(\mathfrak{a}, \mathfrak{b}) \in (\mathbb{Z}/q\mathbb{Z})^{2n}$ as

$$\begin{cases} \mathbf{a} = \mathfrak{a} \circledast \mathbf{r} + \mathbf{e}_1 \\ b = \langle \mathfrak{b}, \mathbf{r} \rangle + \Delta m + e_2 \end{cases}$$

for some $\mathbf{r} \xleftarrow{\$} \{0,1\}^n$, $\mathbf{e}_1 \leftarrow \hat{\chi}_1{}^n$, and $e_2 \leftarrow \hat{\chi}_2$. Part $\mathbf{a}$ is called the mask of the ciphertext and part b is called the body of the ciphertext.

When Z plaintexts, $m_1, \dots, m_Z$, need to be encrypted, they are first put in $\lceil Z/n \rceil$ bins so that each bin contains at most n plaintexts. Next, for each bin:

1. A fresh mask $\mathbf{a}$ is generated from a fresh randomizer $\mathbf{r} \xleftarrow{\$} \{0,1\}^n$ and a fresh noise vector $\mathbf{e}_1 \leftarrow \hat{\chi}_1{}^n$ as $\mathbf{a} \leftarrow \mathfrak{a} \circledast \mathbf{r} + \mathbf{e}_1$;

2. The first plaintext, say m_1, is encrypted as above; namely, by adding the body $b := b_1 \leftarrow \langle \mathfrak{b}, \mathbf{r} \rangle + \Delta m_1 + e_{2,1}$ for a fresh random noise $e_{2,1} \leftarrow \hat{\chi}_2$;

3. The remaining plaintexts in the bin (if any), say $m_2, \dots, m_L$ for some $L \leqslant n$, are represented by pairs of the form

   $$\{(\mathbf{a}, b_\ell)\}_{2 \leqslant \ell \leqslant L}$$

   where $\mathbf{a}$ is the mask generated in 1 and

   $$b_\ell \leftarrow (\mathfrak{b} \circledast \mathbf{r})_{j_\ell} + \Delta m_\ell + e_{2,\ell} \quad (\text{for } 2 \leqslant \ell \leqslant L)$$

for a fresh random noise $e_{2,\ell} \leftarrow \hat{\chi}_2$ and distinct indexes $j_\ell \in \{1, \dots, n\} \setminus \{i\}$.

(Note that, by construction, $(\mathfrak{b} \circledast \mathbf{r})_i = \langle \mathfrak{b}, \mathbf{r} \rangle$.)

Ciphertext $(\mathfrak{a}, b_1)$ is an LWE-type ciphertext but ciphertexts in $\{(\mathfrak{a}, b_\ell)\}_{2 \leqslant \ell \leqslant L}$ are not. To turn them into LWE-type ciphertexts the common mask $\mathfrak{a}$ needs first to be converted into the corresponding mask $\Psi_{j_\ell}(\mathfrak{a})$ to get the LWE-type ciphertext $(\Psi_{j_\ell}(\mathfrak{a}), b_{j_\ell})$ for some map $\Psi_{j_\ell} \colon (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})^n$. There is always such a map. For instance, map Ψ_{j_ℓ} can be chosen as a linear map satisfying

$$(\mathbf{C} \circledast \mathbf{s})_{j_\ell} \approx \langle \Psi_{j_\ell}(\mathbf{C}), \mathbf{s} \rangle$$

for any vector $\mathbf{C} = (C_1, \dots, C_n)$. An expression for ψ_{j_ℓ} can be obtained in a way similar to what is done to derive map φ_1; see Section 3.

For example, for $i = n$ and n a power of two as in Section 2.1, for a vector $\mathbf{x} = (x_1, \dots, x_n)$, we can define

$$\Psi_{j_\ell}(\mathbf{x}) = \left((-1)^{[k \leqslant n - j_\ell]} \, x_{1 + (k + j_\ell - 1 \bmod n)}\right)_{1 \leqslant k \leqslant n} \ .$$

For such a choice for Ψ_{j_ℓ}, it can be verified that $(\Psi_{j_\ell}(\mathfrak{a}), b_{j_\ell})$ is an LWE-type ciphertext encrypting plaintext m_ℓ; that is, that

$$b_{j_\ell} - \langle \Psi_{j_\ell}(\mathfrak{a}), \mathbf{s} \rangle = \Delta\, m_\ell + (\text{small noise}) \ .$$

It is also interesting to observe that when $i = n$, replacing j_ℓ by i yields $\Psi_i(\mathbf{x}) = (x_k)_{1 \leqslant k \leqslant n} = (x_1, \dots, x_n)$; namely, Ψ_i is the identity map.

5 Variants

There are a number of possible variants. Instead of selecting $t \mid q$, plaintext modulus t can be more generally chosen as an arbitrary positive integer $< q$. In this case, a plaintext m is encrypted as $\mathbf{c} = (\mathfrak{a}, b)$ with $\mathfrak{a} = \mathfrak{a} \circledast \mathbf{r} + \mathbf{e}_1$ and $b = \langle \mathfrak{b}, \mathbf{r} \rangle + \lfloor q/t \rfloor m + e_2$ or $b = \langle \mathfrak{b}, \mathbf{r} \rangle + \lceil (q/t) m \rfloor + e_2$. See Section 1.

Another variant is to select private key $\mathbf{s}$ and/or randomizer $\mathbf{r}$ at random in e.g. $\{-1, 0, 1\}^n$, or in any small subset of $\mathbb{Z}/q\mathbb{Z}$.

References

[1] Mihir Bellare, Alexandra Boldyreva, Kaoru Kurosawa, and Jessica Staddon. Multi-recipient encryption schemes: How to save on band-

width and computation without sacrificing security. *IEEE Transactions on Information Theory*, 53(11):3927–3943, 2007. doi:10.1109/TIT.2007.907471.

[2] Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon. Randomness re-use in multi-recipient encryption schemes. In Y. Desmedt, editor, *Public Key Cryptography (PKC 2003)*, volume 2567 of *Lecture Notes in Computer Science*, pages 85–99. Springer, 2003. doi:10.1007/3-540-36288-6_7.

[3] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91, January 2020. doi:10.1007/s00145-019-09319-x.

[4] Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 617–640. Springer, Heidelberg, April 2015. doi:10.1007/978-3-662-46800-5_24.

[5] Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012. https://eprint.iacr.org/2012/144.

[6] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 197–206. ACM Press, May 2008. doi:10.1145/1374376.1374407.

[7] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[8] Marc Joye. SoK: Fully homomorphic encryption over the [discretized] torus. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(4):661–692, 2022. doi:10.46586/tches.v2022.i4.661-692.

[9] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances*

in Cryptology – EUROCRYPT 2010, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, Heidelberg, May / June 2010. doi:10.1007/978-3-642-13190-5_1.

[10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. Cryptology ePrint Archive, Report 2012/230, 2012. https://eprint.iacr.org/2012/230.

[11] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM Press, May 2005. doi:10.1145/1060590.1060603.

[12] Ron Rothblum. Homomorphic encryption: From private-key to public-key. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 219–234. Springer, Heidelberg, March 2011. doi:10.1007/978-3-642-19571-6_14.

A Variance and Covariance

The variance captures how much a randomly drawn variable is spread out from the average value. Formally, the variance of a random variable X is defined as

$$\mathrm{Var}(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right]$$

or, equivalently, as $\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.

Composition formulas For two *independent* variables X_1 and X_2, the expectation and variance of their sum and of their product satisfy

$$\begin{cases} \mathbb{E}[X_1 + X_2] = \mathbb{E}[X_1] + \mathbb{E}[X_2] \\ \mathrm{Var}(X_1 + X_2) = \mathrm{Var}(X_1) + \mathrm{Var}(X_2) \end{cases}$$

and

$$\begin{cases} \mathbb{E}[X_1 X_2] = \mathbb{E}[X_1]\,\mathbb{E}[X_2] \\ \mathrm{Var}(X_1 X_2) = \mathrm{Var}(X_1)\,\mathrm{Var}(X_2) + \mathrm{Var}(X_1)\,\mathbb{E}[X_2]^2 \\ \qquad\qquad + \mathrm{Var}(X_2)\,\mathbb{E}[X_1]^2 \end{cases} .$$

The covariance indicates the joint variability of two random variables X_1 and X_2; it is written $\mathrm{Cov}(X_1, X_2)$. In particular, the covariance is zero when X_1 and X_2 are independent.

For correlated random variables X_1 and X_2, the composition formulas generalize to

$$\begin{cases} \mathbb{E}[X_1 + X_2] = \mathbb{E}[X_1] + \mathbb{E}[X_2] \\ \mathrm{Var}(X_1 + X_2) = \mathrm{Var}(X_1) + \mathrm{Var}(X_2) + 2\,\mathrm{Cov}(X_1, X_2) \end{cases}$$

and

$$\begin{cases} \mathbb{E}[X_1\, X_2] = \mathbb{E}[X_1]\,\mathbb{E}[X_2] + \mathrm{Cov}(X_1, X_2) \\ \mathrm{Var}(X_1\, X_2) = \mathrm{Cov}({X_1}^2, {X_2}^2) \\ \qquad\qquad + (\mathrm{Var}(X_1) + \mathbb{E}[X_1]^2))\,(\mathrm{Var}(X_2) + \mathbb{E}[X_2]^2) \\ \qquad\qquad - (\mathrm{Cov}(X_1, X_2) + \mathbb{E}[X_1]\,\mathbb{E}[X_2])^2 \end{cases}.$$