Homomorphic sign evaluation with a RNS representation of integers

Philippe Chartier

INRIA, IRMAR, Rennes, France,
(this work was done while all four authors were at Ravel Technologies, Paris, France)

Joint work with M. Koskas (Ravel Technologies), M. Lemou (CNRS-IRMAR, Rennes) and F. Méhats (Ravel Technologies)

Kolkata, Friday 13th of December, 2024

Homomorphic encryption

The choice of TFHE at Ravel

- The concept of fully homomorphic encryption (FHE), established since 1978 and advanced by Craig Gentry in 2009, has seen limited application due to its previously prohibitive costs.
- Recently, several startups are developing FHE libraries, with Ravel Technology focusing specifically on privacy-preserving targeted advertising and confidential data analytics.
- Ravel's decision to build on the TFHE scheme is driven by two main factors:
  (i) Lattice-based cryptography offers post-quantum security.
  (ii) TFHE features one of the fastest bootstrapping processes compared to other schemes (at least in terms of latency).

FHE with ring variants (TFHE/FHEW)

The technique was introduced in several key papers:

1. L. Ducas and D. Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. Eurocrypt 2015. This paper introduced fast bootstrapping techniques for the FHEW scheme.
2. I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. Asiacrypt 2016. This work further optimized bootstrapping, reducing the time significantly.
3. I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology, 2020. This paper established the TFHE scheme and its performance benefits.

Adding homomorphic comparison to FHE

Homomorphic encryption on large integers

Ravel is developing homomorphic algorithms for large integers (32-bits or 64-bits) to enable various computations.

Addition, multiplication, comparison

$$\begin{tikzcd}
\text{Plain} & (a_1, a_2) \arrow[r, "{+,\times,\leq}"] & a_1 + a_1 \times a_2 \leq a_2 & \text{Plain output} \\
\text{Encrypt} & \downarrow & \uparrow & \text{Decrypt} \\
\text{Ciphers} & (c_1, c_2) \arrow[r, "{\oplus,\otimes,\leq}"] & c_1 \oplus c_1 \otimes c_2 \leq c_2 & \text{Cipher output}
\end{tikzcd}$$

Of course, practical FHE implementations should offer more homomorphic functions.

The torus and its discretized version

Definition (Discretized torus for messages)

Let $P \geq 3$ be an odd integer. The structure of the discrete torus $\mathbb{T}_P$ is inherited from $(\mathbb{Z}_P, +, \times)$, with privileged representative

$$i \text{ mods } P \in \{-(P-1)/2, ..., (P-1)/2\}$$

The discrete torus $\mathbb{T}_P \subset \mathbb{T} = [-\frac{1}{2}, \frac{1}{2}) + \mathbb{Z}$ is defined by $\mathbb{T}_P = \frac{1}{P}\mathbb{Z}_P$:

$$\mathbb{T}_P = \{-(P-1)/(2P), ..., (P-1)/(2P)\} + \mathbb{Z}$$

Note that $\mathbb{T}_P$ is a ring [isomomorphic to $(\mathbb{Z}_P, +, \times)$] :

1. the addition in $\mathbb{T}_P$ is inherited from $\mathbb{T}$, that is to say

$$\forall (x, y) \in \mathbb{T}_P \times \mathbb{T}_P, x + y \equiv x + y \mod 1$$

2. the multiplication is inherited from $\mathbb{Z}_P$:

$$\forall (x, y) \in \mathbb{T}_P \times \mathbb{T}_P, x \times y = (Px) \times y \mod 1$$

Residue Number System (I)

Consider an integer $p > 2$ of the form

$$p = \prod_{i=1}^{\kappa} p_i$$

where the $p_i \geq 3$ are pairwise coprime $\forall i \neq j, p_i \wedge p_j = 1$. Elements

$$\mu \in \mathbb{T}_p := \frac{1}{p}\mathbb{Z}_p = \Big\{ -(p-1)/(2p), \cdots, (p-1)/2p \Big\} + \mathbb{Z}$$

may be represented unambiguously (Chinese Remainder Theorem) by their coordinates

$$(\mu_1, \dots, \mu_\kappa) \in \mathbb{T}_{p_1} \times \cdots \times \mathbb{T}_{p_\kappa}$$

where, for all $i = 1, \dots, \kappa$,

$$\mathbb{T}_{p_i} := \frac{1}{p_i}\mathbb{Z}_{p_i} = \Big\{ -(p_i-1)/(2p_i), \dots, (p_i-1)/(2p_i) \Big\} + \mathbb{Z}$$

and $\mu_i = (p\mu \mod p_i)/p_i$ or equivalently $\mu_i = p\mu/p_i \mod 1$.

Residue Number System (II)

The Chinese Remainder Theorem states that the map

$$\begin{aligned}\Phi : \mathbb{T}_p &\to \mathbb{T}_{p_1} \times \cdots \times \mathbb{T}_{p_\kappa} \\ \mu &\mapsto (\mu_1, \cdots, \mu_\kappa) = \left(\frac{p\mu}{p_1} \mod 1, \cdots, \frac{p\mu}{p_\kappa} \mod 1\right)\end{aligned}$$

is an isomorphism with inverse

$$\begin{aligned}\Phi^{-1} : \mathbb{T}_{p_1} \times \cdots \times \mathbb{T}_{p_\kappa} &\to \mathbb{T}_p \\ (\mu_1, \cdots, \mu_\kappa) &\mapsto \mu = \sum_{i=1}^{\kappa} v_i \mu_i \mod 1\end{aligned}$$

where the (u_i, v_i) satisfy $u_i p_i + v_i \frac{p}{p_i} = 1$ for $i = 1, \cdots, \kappa$ (Bezout).

Encoding

A message $\mu \in \mathbb{T}_p$ is encoded by its “residues” $\mu_i = \frac{p\mu}{p_i} \mod 1$ for $i = 1, \cdots, \kappa$. Note that all $+$ and $\times$ operations can be done on residues in parallel.

Encryption/decryption schemes in $\mathbb{T}$

Assume LWE problem on $\mathbb{Z}_q$ is secure and assimilate $\mathbb{T} \equiv \frac{1}{q}\mathbb{Z}_q$.

EncryptLWE$_s(\mu)$

TLWE-encryption of $\mu \in \mathbb{T}$ with secret key $s \in \mathbb{S}^n$ is defined as

$$c = TLWE_s(\mu) = (a, b) \in \mathbb{T}^{n+1} \quad with \quad \begin{cases} (a_1, \ldots, a_n) \xleftarrow{\$} \mathbb{T}^n \\ e \leftarrow \mathcal{N}(0, \sigma^2) \\ b = a \cdot s + \mu + e \end{cases}$$

DecryptLWE$_s$ (c, P)

TLWE-decryption of $(a, b) \in \mathbb{T}^{n+1}$ with key $s \in \mathbb{S}^n$ is defined as

$$\pi_P(b - a \cdot s) \in \mathbb{T}_P$$

where π_P is a projection on the discrete torus $\mathbb{T}_P$.

Complete encoding/encryption of messages of $\mathbb{T}_p$

$$\mu \in \mathbb{T}_p$$

$$\downarrow\uparrow$$

Encoding (Residues) Decoding (Bezout)

$$\downarrow\uparrow$$

$$((p\mu) \bmod p_1, \cdots, (p\mu) \bmod p_\kappa) \in \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_\kappa}$$

$$\downarrow\uparrow$$

Encoding Decoding

$$\downarrow\uparrow$$

$$\left(\frac{p\mu}{p_1} \bmod 1, \cdots, \frac{p\mu}{p_\kappa} \bmod 1\right) \in \mathbb{T}_{p_1} \times \cdots \times \mathbb{T}_{p_\kappa}$$

$$\downarrow\uparrow$$

Encryption Decryption

$$\downarrow\uparrow$$

$$(TLWE_s(\mu_1), \ldots, TLWE_s(\mu_\kappa))$$

Computing the sign in $\mathbb{T}_p$ homomorphically

Objective: Find an encryption of the sign of $\mathbb{T}_{p_1} \times \cdots \times \mathbb{T}_{p_\kappa}$

$$TLWE_s(Sign \circ \Phi^{-1}(\mu_1, \cdots, \mu_\kappa))$$

from the κ values $c_i = TLWE_s(\mu_i) \in \mathbb{T}^{n+1}, i = 1, \cdots, \kappa$.

Definition

Consider an element $\mu \in \mathbb{T} \equiv \mathbb{R}/\mathbb{Z}$. The sign of μ is the sign of its residue modulo 1, i.e. the sign of the real $\mu' = \mu + k \in [-\frac{1}{2}, \frac{1}{2})$ with $k \in \mathbb{Z}$

$$\text{Sign}(\mu) = \begin{cases} -1 & \text{if } \exists k \in \mathbb{Z}, \quad \mu + k \in [-\frac{1}{2}, 0) \\ 0 & \text{if } \exists k \in \mathbb{Z}, \quad \mu + k = 0 \\ 1 & \text{if } \exists k \in \mathbb{Z}, \quad \mu + k \in (0, \frac{1}{2}) \end{cases}$$

Preliminary remarks in the context of a RNS

The sign of $\mu \in \mathbb{T}$ can not be determined solely from the signs of its components $(\mu_1, \cdots, \mu_\kappa)$. This can be seen on the following

Example : $p_1 = 3$ and $p_2 = 5$ (i.e. $p = 15$).

- On the one hand, both

$$\frac{2}{15} \in \mathbb{T}_{15} \quad \text{and} \quad \frac{7}{15} \in \mathbb{T}_{15}$$

have positive signs by definition.

- On the other hand, their components are respectively

$$(-\frac{1}{3}, \frac{2}{5}) \in \mathbb{T}_3 \times \mathbb{T}_5 \quad \text{and} \quad (\frac{1}{3}, \frac{2}{5}) \in \mathbb{T}_3 \times \mathbb{T}_5$$

with signs $(-1, 1)$ and $(1, 1)$ respectively.

This shows that the value of μ has to some extent to be computed through Φ^{-1} in order to evaluate its sign.

Recomposing the message is not an option

We first note that

$$c = (a, b) = \sum_{i=1}^{\kappa} v_i(a_i, b_i)$$

is an encrypted value of $\mu = \Phi^{-1}(\mu_1, \ldots, \mu_\kappa)$:

$$b - s \cdot a = \sum_{i=1}^{\kappa} v_i(b_i - s \cdot a_i) = \sum_{i=1}^{\kappa} v_i(\mu_i + e_i) = \mu + e.$$

If $|e_i| \leq \frac{1}{2p_i}$, $i = 1, \cdots, \kappa$, we have $|e| \leq \sum_{i=1}^{\kappa} p_i|e_i| \leq \frac{\kappa}{2}$ which is far too large for a correct decryption of $\mu \in \mathbb{T}_P$.

Example: $(p_1, p_2, p_3, p_4, p_5, p_6, p_7) = (7, 11, 13, 15, 17, 19, 23)$

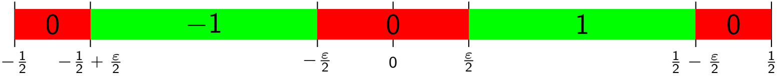
If the c_i all decrypts with probability $> 1 - 10^{-10}$, the probability of a failed decryption of sign(μ) is greater than 0.5...

Approximate sign function

Definition

Let $0 \leq \varepsilon \leq 1$. The function g_ε is defined on the torus as follows

$$g_\varepsilon(\mu) = \begin{cases} 1 & \text{if} \quad \mu \in [\frac{\varepsilon}{2}, \frac{1}{2} - \frac{\varepsilon}{2}] \\ -1 & \text{if} \quad \mu \in [-\frac{1}{2} + \frac{\varepsilon}{2}, -\frac{\varepsilon}{2}] \\ 0 & \text{else} \end{cases}$$



The function g_ε.

Tolerance with respect to errors

Proposition

Let $3 \leq \overline{p} < p$ be an odd integer and assume that $0 < \varepsilon < \frac{1}{2(\overline{p}+1)}$. Consider a noisy value of $\mu \in \mathbb{T}$ of the form

$$\tilde{\mu} = \mu + e \mod 1 \quad \textit{with} \quad |e| \leq \frac{\varepsilon}{2}.$$

The following statements hold

(i) *if $g_\varepsilon(\tilde{\mu}) = 1$, then sign$(\mu) = 1$;*

(ii) *if $g_\varepsilon(\tilde{\mu}) = -1$, then sign$(\mu) = -1$;*

(iii) *if $g_\varepsilon(\tilde{\mu}) = 0$, then $\overline{p}\mu$ and μ have the same sign.*

Main idea: rescaling (i)

One can then consider the sequence of rescalings $r = 0, 1, \ldots,$

$$\widetilde{\mu}^{[r]} := \sum_{i=1}^{\kappa} (\overline{p}^r v_i \bmod p_i) \widetilde{\mu}_i = \overline{p}^r \mu + e^{[r]} \bmod 1,$$

$$\text{with} \qquad |e^{[r]}| = \left| \sum_{i=1}^{\kappa} (\overline{p}^r v_i \bmod p_i)\, e_i \right| \leq \frac{\varepsilon}{2},$$

one has

(i) if $\forall k \leq r, g_\varepsilon(\widetilde{\mu}^{[k]}) = 0$, then $\forall k \leq r+1, \mathrm{sign}(\overline{p}^k \mu) = \mathrm{sign}(\mu)$

(ii) if in addition, $g_\varepsilon(\widetilde{\mu}^{[r+1]}) = +1$ then $\mathrm{sign}(\mu) = +1$.

(iii) if in addition, $g_\varepsilon(\widetilde{\mu}^{[r+1]}) = -1$ then $\mathrm{sign}(\mu) = -1$.

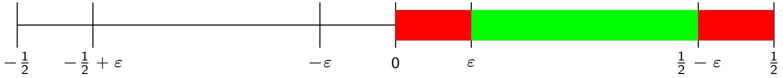
Main idea: rescaling (ii)

Lemma

Let $\overline{p} \geq 3$ *be an odd integer,* $0 < \varepsilon \leq \frac{1}{2(\overline{p}+1)}$ *and* $\mu \in [-\frac{1}{2}, \frac{1}{2})$. *The following statements are satisfied:*

(i) *if* $\mu \in [0, \varepsilon]$, *then* $\overline{p}\mu \in [0, \frac{1}{2} - \varepsilon]$ *and if* $\mu \in (0, \varepsilon)$, *then* $\overline{p}\mu \in (0, \frac{1}{2} - \varepsilon)$

(ii) $\mu \in [\frac{1}{2} - \varepsilon, \frac{1}{2})$, *then* $\overline{p}\mu \in [\varepsilon, \frac{1}{2})$



Rescaling

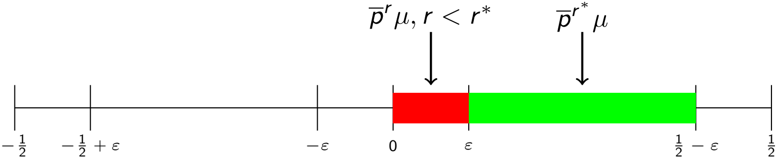
Sequence of rescaled messages (i)

Lemma

Let us now consider the sequence $\overline{p}^r\mu, r = 0, \cdots, +\infty$. The following statements are satisfied:

(i) *if $\mu \in (0, \varepsilon)$, then there exists $r^* \in \mathbb{N}^*$ such that*

$$\forall 0 \leq r < r^*, \overline{p}^r\mu \in (0, \varepsilon) \quad \textit{and} \quad \overline{p}^{r^*}\mu \in [\varepsilon, \frac{1}{2} - \varepsilon)$$



$\overline{p}^r\mu, r < r^*$
$\overline{p}^{r^*}\mu$
$-\frac{1}{2}$
$-\frac{1}{2} + \varepsilon$
$-\varepsilon$
0
ε
$\frac{1}{2} - \varepsilon$
$\frac{1}{2}$

Case (i)

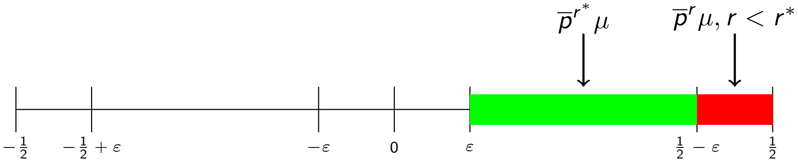
Sequence of rescaled messages (ii)

Lemma

Let us now consider the sequence $\overline{p}^r\mu, r = 0, \cdots, +\infty$. The following statements are satisfied:

(i) ...

(ii) *if $\mu \in (\frac{1}{2} - \varepsilon, \frac{1}{2})$, then there exists $r^* \in \mathbb{N}^*$ such that for all $0 \le r < r^*$, one has $\overline{p}^r\mu \mod 1 \in (\frac{1}{2} - \varepsilon, \frac{1}{2})$ and $\overline{p}^{r^*}\mu \mod 1 \in [\varepsilon, \frac{1}{2} - \varepsilon)$*



Case (ii)

Main result

Proposition

Let $3 \leq \overline{p} < p$ be odd integers and let $0 < \varepsilon \leq \frac{1}{2(\overline{p}+1)}$. Let $\mu \in \mathbb{T}_p$ and consider a sequence of real numbers $\tilde{\mu}^{[r]} \in \mathbb{T}$, defined for $r = 0, 1, \ldots, r_{max} = 1 + \left\lfloor \log_{\overline{p}} \left(\frac{p}{\overline{p}+1} \right) \right\rfloor$, and satisfying

$$|\tilde{\mu}^{[r]} - \overline{p}^r \mu| \leq \varepsilon.$$

Then, there exists $0 \leq r^* \leq r_{max}$ such that

1. *if $\mu > 0$ then $g_\varepsilon(\tilde{\mu}^{[r^*]}) = 1$ and for $0 \leq r < r^*$, $g_\varepsilon(\tilde{\mu}^{[r]}) = 0$;*
2. *if $\mu < 0$ then $g_\varepsilon(\tilde{\mu}^{[r^*]}) = -1$ and for $0 \leq r < r^*$, $g_\varepsilon(\tilde{\mu}^{[r]}) = 0$;*
3. *if $\mu = 0$ then $g_\varepsilon(\tilde{\mu}^{[r]}) = 0$ for $r \geq 0$,*

where the function g_ε was introduced above.

Weighting previous sequence gives the sign!

Let us consider the geometrically weighted sum

$$\frac{1}{4}\sum_{r=0}^{r_{max}}\frac{1}{2^k}g_\varepsilon(\tilde{\mu}^{[r]}) \in \mathbb{T}_{2^{r_{max}+2}}$$

Then the sign of μ is obtained as

$$\mathrm{sign}\left(\frac{1}{4}\sum_{r=0}^{r_{max}}\frac{1}{2^k}g_\varepsilon(\tilde{\mu}^{[r]})\right)$$

i.e.

$$\mathrm{sign}(\mu) = g_\varepsilon\left(\frac{1}{4}\sum_{r=0}^{r_{max}}\frac{1}{2^k}g_\varepsilon(\tilde{\mu}^{[r]})\right).$$

Our sign algorithm is then essentially the homomorphic implementation of previous formula.

Computational times of the sign in $\mathbb{T}_p$

Parameters used identical for all operations $\times, =, \text{Sign}, +$. Cleartexts are integers with 32 or 64 bits. All computations are made on an average laptop with Ravel's library.

Highlight example for 128 bits of security

Our algorithm delivers a correct result with a probability error below 10^{-12} in less than 140 milliseconds for 32-bit integers.

Type	$\mathbb{P}_{\text{fail}}$	$\times$	$=$	Sign	$+$
$U32$	$1.e-9$	$28.62\,ms$	$50.70\,ms$	$137.35\,ms$	$14.05\,\mu s$
$U32$	$1.e-12$	$27.98\,ms$	$51.29\,ms$	$138.33\,ms$	$13.98\,\mu s$
$U64$	$1.e-9$	$60.09\,ms$	$52.47\,ms$	$145.40\,ms$	$28.18\,\mu s$
$U64$	$1.e-12$	$61.62\,ms$	$53.56\,ms$	$145.91\,ms$	$28.16\,\mu s$

Figure: Times in ms (except for the addition) and 128 bits of security

THANK YOU FOR YOUR ATTENTION