Integer Functions Suitable for Homomorphic Encryption over Finite Fields

I. Iliashenko, C. Nègre, **V. Zucca**

LIRMM-DALI, Université de Perpignan Via Domitia

Workshop on Encrypted Computing & **A**pplied **H**omomorphic **C**ryptography

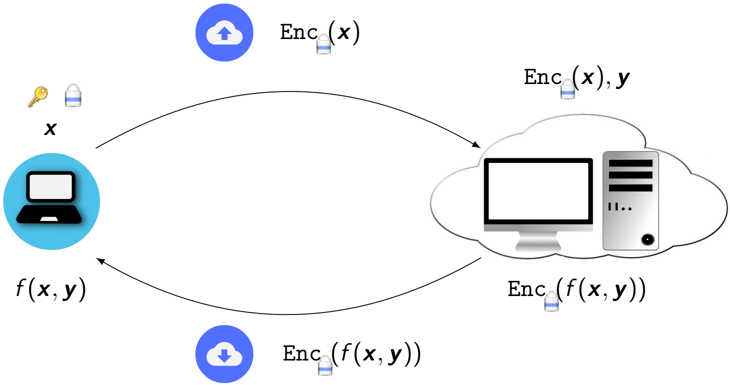
November 15th 2021

What is Homomorphic Encryption (HE)?

HE allows to compute over encrypted data without the decryption key

Applications:

- Private search queries;
- Secure multi-party computations;
- Delegation of computations over sensitive data.



SHE model of computation

- SHE schemes can compute arithmetic circuits ($+$ and $\times$) of bounded multiplicative depth over encrypted messages.
- For security reasons HE ciphertexts contain noise components
  - noise grows after each homomorphic operation
  - noise must remain small enough to guarantee decryption's correctness
- Complexity of homomorphic operations should be assessed regarding
  - their running time
  - the amount of noise introduced
- The complexity to evaluate an arithmetic circuit homomorphically is analyzed with relation to
  - the number of (non-scalar) homomorphic multiplications
  - its multiplicative depth

Purpose of this work

- Our work focuses on the case where the plaintext space is a prime field $\mathbb{F}_p$ for an odd prime p (e.g. BGV, BFV).
- Study some functions having a particular structure when interpolated over $\mathbb{F}_p$ allowing to speed-up their homomorphic evaluation.
  - multiplicative depth will remain unchanged
  - we only reduce the number of homomorphic multiplications
- In [IZ21] we noticed that the comparison function has a particular structure over $\mathbb{F}_p$ permitting to speed-up its homomorphic evaluation
  - natural question: is this true for others functions?
  - proof of some results of [IZ21] which were ommitted
- Similarly to [IZ21] we expect a speed-up proportional to the number of homomorphic multiplications saved.

Interpolation over finite fields

The equality function can be evaluated over $\mathbb{F}_p^2$ as

$$\mathtt{EQ}(x, y) = 1 - (x - y)^{p-1} = \begin{cases} 1 \text{ if } x = y \\ 0 \text{ otherwise} \end{cases}$$

Lemma (Lagrange Interpolation)

Every function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ can be interpolated by a unique polynomial $P_f(X_1, \ldots, X_n)$ of degree at most $p - 1$ in each variable

$$P_f(X_1, \ldots X_n) = \sum_{\boldsymbol{a} \in \mathbb{F}_p^n} f(\boldsymbol{a}) \prod_{i=1}^{n} (1 - (X_i - a_i)^{p-1})$$

The case of unary functions

- A function $f : \mathbb{F}_p \rightarrow \mathbb{F}_p$ can be interpolated with Lagrange as

$$P_f(X) = f(0) - \sum_{i=1}^{p-1} X^i \left(\sum_{a=0}^{p-1} f(a) a^{p-1-i} \right)$$

Complexity: $\mathcal{O}\left(\mathrm{supp}(P_f) \log(p-1)\right)$ multiplications

- Paterson-Stockmeyer algorithm gives an generic bound on the number of non-scalar multiplications to evaluate a polynomial.

Complexity: $\sqrt{2p-2} + \mathcal{O}\left(\log p\right)$ multiplications

- **Goal** : find functions whose interpolation polynomial can be evaluated more efficiently.

The case of unary functions

$$P_f(X) = f(0) - \sum_{i=1}^{p-1} X^i \underbrace{\sum_{a=0}^{p-1} f(a) a^{p-1-i}}_{P_{f,i}}$$

- $\sum_{a=0}^{p-1} a^{p-1-i} = 0 \bmod p$ if $i \neq 0$. f constant $\implies P_f(X) = f(0)$
- What if f is constant on some subsets of $\mathbb{F}_p$?

Example $f(x) = |x|_2 = \begin{cases} 1 \text{ if } x \text{ is odd} \\ 0 \text{ if } x \text{ is even} \end{cases}$ then $P_{f,i} = \sum_{a \text{ odd}} a^{p-1-i}$.

$$i \text{ even} \implies P_{f,i} = \sum_{a \text{ odd}} ((p-a)^2)^{(p-1-i)/2} = \sum_{a \text{ even}} a^{p-1-i}$$

$$\sum_{a=0}^{p-1} a^{p-1-i} = 2 \sum_{a \text{ odd}} a^{p-1-i} = 0 \Leftrightarrow P_{f,i} = 0$$

The case of unary functions

$$i \in [1, p-1) \cap 2\mathbb{Z} \Leftrightarrow P_{f,i} = 0$$

$P_f(X)$ has only odd degree coefficients plus the constant and leading terms

$$P_f(X) = f(0) - P_{f,p-1}X^{p-1} + Xg(X^2)$$

This observation on $|\cdot|_2$ can be generalized with the following lemma

Lemma

Let $\mathbb{F}_p$ be a prime field, $f : \mathbb{F}_p \to \mathbb{F}_p$ and γ a primitive k-th root of unity ($k > 0$). Let $\mathcal{S}_0$, $\mathcal{S}_1$, ..., $\mathcal{S}_{k-1}$ be disjoint subsets of $\mathbb{F}_p$ such that

- $\mathcal{S}_j = \gamma^j \mathcal{S}_0$ for $0 \leq j < k$
- $\mathbb{F}_p^\times = \mathcal{S}_0 \cup \cdots \cup \mathcal{S}_{k-1}$
- f is constant on each subset S_j with $0 \leq j < k$

Then for any $i \in [1, p-2]$ such that $k \mid i$ $P_{f,i} = 0 \bmod p$.

The modulo function $f_m(x) = |x|_m$

Consider the modulo m function over $\mathbb{F}_p$ $f(x) = |x|_m$

Proposition

Let $m > 1$ be an integer and p an odd prime such that $p \equiv m - 1 \mod m$

$$P_{f_m}(X) = \frac{(p+1)(m-1)}{2} X^{p-1} + X \cdot g(X^2)$$

where g is a degree $(p-3)/2$ polynomial.

Complexity $\sqrt{p-3} + \mathcal{O}(\log p)$ homomorphic multiplications.

The "Is power of b" function

Let $b > 1$ be an integer and $f_b : [0, p) \to \{0, 1\}$ such that

$$f_b(x) = \begin{cases} 1 \text{ if } x = b^a \text{ for some } a \geq 0 \\ 0 \text{ otherwise} \end{cases}$$

Let $\ell = \lfloor \log_b p \rfloor$, using Lagrange interpolation we get

$$P_{f_b}(X) = \sum_{a=0}^{\ell} (1 - (X - b^a)^{p-1})$$

Complexity $\mathcal{O}(\ell \log p) = \mathcal{O}(\log^2 p)$ homomorphic multiplications

Can we do better?

The "Is power of b" function

$$P_{f_b}(X) = -\sum_{i=1}^{p-1} X^i \sum_{a=0}^{\ell} (b^a)^{p-1-i}$$

Assuming $b^{\ell+1} = 1 \bmod p$, $P_{f_b,i} \neq 0 \Leftrightarrow i = 0 \mod \ell + 1$.

Proposition

If $p = (b^r - 1)/k$ for some integers $k < b$ and $r \geq 1$ then

$$P_{f_b}(X) = (p - r) \sum_{i=1}^{(p-1)/r} (X^r)^i$$

Example for $b = 2$ and $p = 31 = (2^5 - 1)/1$ we have:

$$P_{f_2}(X) = 26(X^{30} + X^{25} + X^{20} + X^{15} + X^{10} + X^5)$$

The "Is power of b" function

Complexity :

1. Start by computing $Y = X^r$
2. Compute $g_e(Y) = Y + Y^2 + \ldots + Y^e$ with $e = (p-1)/r$
   - Precompute the elements $Y^2, Y^4, \ldots, Y^{2^k}$ with $k = \lfloor \log_2(e) \rfloor$
   - Compute the following
     - $S_1 = (Y + Y^2)$
     - $S_2 = S_1(1 + Y^2) = Y + Y^2 + Y^3 + Y^4$
     - ...
     - $S_k = S_{k-1}(1 + Y^{2^{k-1}}) = \sum_{i=1}^{2^k} Y^i = g_{2^k}(Y)$
   - $g_e(Y) = S_{k-1} + Y^{2^k} \sum_{i=1}^{e-2^k} Y^i = S_{k-1} + Y^{2^k} g_{e-2^k}(Y)$
     - g_e can be computed recursively in $\log_2(e)$ steps

Overall

- $\lfloor \log_2 r \rfloor + \mathtt{HW}(r) + k + k - 1 + \mathtt{HW}(e) - 1 = \mathcal{O}(\log p)$ mults
- $\lceil \log_2 r \rceil + \lceil \log_2 e \rceil \approx \log_2(p-1)$ depth

The less than function

Let $\mathcal{S} \subset [0, p) \hookrightarrow \mathbb{F}_p$, the less than function is defined over $\mathcal{S}^2$ as

$$\mathtt{LT}_{\mathcal{S}}(x, y) = \begin{cases} 1 \text{ if } x < y \\ 0 \text{ otherwise} \end{cases}$$

Taking $\mathcal{S} = [0, p)$, using Lagrange interpolation we obtain

$$P_{\mathtt{LT}_{\mathcal{S}}}(X, Y) = \sum_{a=0}^{p-2}(1 - (X - a)^{p-1}) \sum_{b=a+1}^{p-1} (1 - (Y - b)^{p-1})$$

- It was shown in [IZ21] that $P_{\mathtt{LT}_{\mathcal{S}}}$ has only total degree p
- [IZ21] claimed $P_{\mathtt{LT}_{\mathcal{S}}}$ could be evaluated using $2p - 6$ homomorphic mutiplications for $p \geq 5$
- Previous work required $3p - 5$ multiplications [TLW+20].

The less than function

$$P_{\mathrm{LT}_{\mathcal{S}}}(X,Y)=\sum_{a=0}^{p-2}(1-(X-a)^{p-1})\sum_{b=a+1}^{p-1}(1-(Y-b)^{p-1})$$

- From the definition of $P_{\mathrm{LT}_{\mathcal{S}}}$ we know that:
  - $P_{\mathrm{LT}_{\mathcal{S}}}(X,0)=0 \implies Y \mid P_{\mathrm{LT}_{\mathcal{S}}}(X,Y)$
  - $P_{\mathrm{LT}_{\mathcal{S}}}(p-1,Y)=0 \implies (X+1) \mid P_{\mathrm{LT}_{\mathcal{S}}}(X,Y)$
- It can be shown that $P_{\mathrm{LT}_{\mathcal{S}}}(X,X)=0$ i.e. $(X-Y) \mid P_{\mathrm{LT}_{\mathcal{S}}}(X,Y)$

Theres exist a polynomial $f \in \mathbb{F}_p(X,Y)$ of total degree $p-3$ such that

$$P_{\mathrm{LT}_{\mathcal{S}}}(X,Y)=Y(X+1)(X-Y)f(X,Y)$$

The less than function

What does f look like? Below is the table of values of f for $p = 7$.

$x \backslash y$	0	1	2	3	4	5	6
0	**0**	6	5	3	3	5	6
1	**4**	**4**	5	4	2	4	5
2	**2**	0	**2**	3	2	2	3
3	**2**	0	0	**2**	3	4	3
4	**2**	0	0	0	**2**	5	5
5	**4**	0	0	0	0	**4**	6
6	**0**	**4**	**2**	**2**	**2**	**4**	**0**

- It can be shown that $f(X,0) = f(X,X)$
  $\implies Y(X-Y)$ divides $g(X,Y) = f(X,Y) - f(X,0)$
- This property can be applied recursively to g so that

$$f(X,Y) = \sum_{n=0}^{(p-3)/2} f_n(X)Z^n \text{ with } Z = Y(X-Y)$$

Conclusions and perspective

- This work proves that several non-trivial functions can be evaluated efficiently over prime fields
  - Familly of functions that can be evaluated in $\mathcal{O}(\sqrt{p})$ hom. mults
    - "Modulo m" function with $p = -1 \mod m$
  - All one polynomial over $\mathbb{F}_p$ can be evaluated in $\mathcal{O}(\log p)$ hom. mults
    - "Is power of b" function with $p = (b^r - 1)/k$
  - When $p = 2^q - 1$ is a Mersenne prime then the "Hamming weight" and `Mod2` functions can be evaluated in $\mathcal{O}(\sqrt{p/\log p})$
  - The less-than function can be evaluated in $2p - 5$ instead of $3p - 6$ hom. mults
- Future possible interesting lines of work could include
  - extend the search of such functions to extension fields $\mathbb{F}_{p^d}$
    - take fully advantage of SIMD packing
  - study interpolation over rings $\mathbb{Z}_{p^e}$
    - current results limited to $f(x) = x - |x|_p$