Multiparty Computation based on Ring-LWE

Mikkel Gaba, Marcus Sellebjerg, Kasper Ilsøe

Project Report (10 ECTS) in Computer Science
Advisor: Ivan Damgård
Department of Computer Science, Aarhus University
May 22th, 2022

AARHUS UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Abstract

...

Mikkel Gaba, Marcus Sellebjergen, Kasper Ilsøe
Aarhus, May 22th, 2022.

Contents

Abstract **ii**

1 Introduction **1**

2 Review of literature **2**

2.1 Ring LWE - A somewhat homomorphic encryption scheme 2

2.1.1 Polynomial learning with errors 2

2.1.2 Symmetric version 2

2.1.3 Public key version 3

2.2 Circuit privacy 4

2.3 Multiparty Computation 4

2.4 Protocol for MPC based on SHE 4

2.4.1 Abstract SHE scheme 5

2.4.2 Concrete instantiation of abstract SHE scheme 5

2.4.3 Preprocessing phase 7

2.4.4 Online phase 7

2.4.5 Parameter setting 8

2.5 Reuse of unrevealed secret-shared data 8

3 Implementation **9**

3.1 Polynomials (`poly.rs`) 9

3.2 Quotient ring (`quotient_ring.rs`) 9

3.2.1 `Rq` 9

3.2.2 `reduce` 9

3.2.3 `add`, `times`, `neg`, `mul` 10

3.3 Public-key encryption scheme (`encryption.rs`) 10

3.3.1 `generate_key_pair` 10

3.3.2 `encrypt` 10

3.3.3 `decrypt` 10

4 Conclusion **12**

Acknowledgments **13**

Bibliography **14**

A First appendix **15**

Chapter 1

Introduction

...

Chapter 2

Review of literature

2.1 Ring LWE - A somewhat homomorphic encryption scheme

In the paper "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages" written by Zvika Brakerski and Vinod Vaikuntanathan [1] they describe a method for converting the Ring Learnig with errors (RingLWE) problem into an encryption scheme which reduces to the worst-case hardness of problems on ideal lattices. We'll shortly describe the encryption scheme here but will omit proofs and detailed discussions. Both system will be over the message space of $R_t = \mathbb{Z}_t[x]/\langle f(x) \rangle$.

2.1.1 Polynomial learning with errors

The polynomial learning with errors problem is made as a decision problem and is defined by in the Hermite normal form as the following.

The PLWE Assumption - Hermite Normal Form. for all $\kappa \in \mathbb{N}$, let $f(x) = f_\kappa(x) \in \mathbb{Z}[x]$ be a polynomial of degree n = n(κ), let $q = q(\kappa) \in \mathbb{Z}$ be a prime integer, let the ring $R = \mathbb{Z}[x]/\langle f(x) \rangle$ and $R_q = R/qR$ with χ denoting a distribution over the ring R. Then the Polynomial learning with error ($PLWE_{f,q,\chi}$) assumption can be defined as

$$\{(a_i, a_i \cdot s + e_i)\}_{i \in [l]} \approx^c \{(a_i, u_i)\}_{i \in [l]}\}$$

where s is sampled from χ, a_i is uniform in R_q, the error polynomials e_i are sampled from χ and u_i are random ring elements from R_q.

2.1.2 Symmetric version

Let κ be the security parameter and let further q and t be prime numbers where $t \in \mathbb{Z}_n^*$. We also need a polynomial of degree n $f(x) \in \mathbb{Z}[x]$ and an error distribution χ over the ring $R_q = \mathbb{Z}_q[x]/\langle f(x) \rangle$, then we can define the following operations.

Key-gen

Let our secret key be a randomly sampled element from the error distribution $s \xleftarrow{\$} \chi$ Then given the security parameter κ sample a ring element s uniformly at random from κ and define the secret key vector by $(s^0, s^1, s^2, \ldots, s^D) \in R_q^{D+1}$.

Encryption

Rememer that all messages are encodeable in our message space R_t, thus we will encode our message m as a n degree polynomium with coefficient mod t. To encrypt we sample $(a, b = a \cdot s + t \cdot e)$ where $a \leftarrow^{\$} R_q$ and $e \leftarrow^{\$} \chi$, then compute

$$c_0 \coloneqq b + m \qquad\qquad c_1 \coloneqq -a$$

and from this output the ciphertext $\mathbf{c} \coloneqq (c_0, c_1) \in R_q^2$.

Decryption

Note that a ciphertext is on the form $(c_0, c_1, \ldots, C_D) \in R_q^{D+1}$. Define the inner product over R_q as

$$\langle c, s \rangle = \sum_{i=0}^{D} c_i \cdot s^i$$

Then to decrypt, simply set m as the inner product of c and s and take modulo t.

$$m = \langle c, s \rangle \bmod t$$

m will then be the decrypted message.

Eval

To obtain the homomorphic abilities of the encryption scheme, Zvika Brakerski and Vinod Vaikuntanathan show how to obtain homomorphic addition and multiplication of ciphertexts.

Addition: Assume we have 2 ciphertexts $c \in R_q^{D+1}$ and $c' \in R_q^{D+1}$, then an encryption of the sum of the 2 underlying messages will be

$$c_{Add} = c + c' = (c_0 + c'_0, c_1 + c'_1, \ldots, c_d + c'_d) \qquad\qquad c_{Add} \in R_q^{D+1}$$

The decryption of c_{Add} will then be the sum of the unencrypted messages from c and c'.

Multiplication: Assume we have 2 ciphertexts $c \in R_q^{D+1}$ and $c' \in R_q^{D'+1}$ and let v be a symbolig value then calculate the updated ciphertext
$(\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_d + d') \in R_q^{D+D'+1}$ by

$$c_{mul} = (\sum_{i=0}^{D} c_i \cdot v^i) \cdot (\sum_{j=0}^{D'} c'_i \cdot v^i) = \sum_{i=0}^{D+D'} \hat{c}_i \cdot v^i \qquad\qquad c_{mul} \in R_q^{D+D'+1}$$

The output of the multiplication operation will then be $c_{mul} = (\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{D+D'})$

2.1.3 Public key version

To achieve a public scheme instead, we can make the following changes

- In the key generation we generate in addition to the secret key $sk = s \leftarrow^{\$} \chi$, we output a public key $pk = (a_0, b_0 = a_0 \cdot s + t \cdot e_0)$, where $a_0 \leftarrow^{\$} R_q, e_0 \leftarrow^{\$}$

- In the encryption algorithm, instead we use $(a_0 \cdot v + t \cdot e', b_0 \cdot v + t \cdot e'')$ where $v, e' \xleftarrow{\$} \chi$ and $e'' \xleftarrow{\$} \chi'$.

where we have then obtained a public key $pk = (a_0, a_0 \cdot s + t \cdot e_0)$ corresponding to the secret key $sk =$.

2.2 Circuit privacy

Each time we add or multiply ciphertexts the error term grows. As a result of this the error term will be larger for a ciphertext output by a call to **eval**, than for a ciphertext output by **encrypt**. This poses a problem, as an adversary might be able to derive information about the function computed by looking at the ciphertexts produced. To deal with this problem we would like the output distributions of the ciphertexts output by **eval** and **encrypt** to be identical, which is known as *circuit privacy*. This property along with how to achieve it has been described in [2].

To achieve *circuit privacy* we can make an encryption of 0 with a very large error term, and then add this ciphertext to the original ciphertext. By doing this we esentially drown out information about the error vector of the original ciphertext. This will not modify the encrypted data, as the new error term will be removed by the (mod t) computation done in **decrypt** anyways.

2.3 Multiparty Computation

The Multiparty Computation (MPC) problem is the problem where n players each with some private input x_i, want to compute some function f on the input, without revealing anything but the result.

2.4 Protocol for MPC based on SHE

In [] the authors describe a protocol for MPC based on a SHE scheme. The protocol is able compute arithmetic formulas consisting of up to a single multiplication, along with a relatively large number of additions, while being statistically UC-secure against an active adversary and $n-1$ corruptions.

The protocol proceeds in two phases. In the first phase, preprocessing, a global key $[\![\alpha]\!]$, random values in two representations $[\![r]\!], \langle r \rangle$, and a number of multiplicative triples $\langle a \rangle, \langle b \rangle, \langle c \rangle$ satisfying $c = ab$ are generated.

In the second phase, the online phase, the players use the global key and random values generated in the preprocessing phase to do the actual computations, aswell as multiplicative triples if a multiplication is to be performed.

Thus the online phase only makes indirect use of the SHE scheme, as it is only used in the preprocessing phase to generate input for the online phase.

These two phases are described in further detail in section 2.4.3 & 2.4.4.

Representations of shared values

The protocol makes use of two different representations of shared values $[\![\cdot]\!], \langle\cdot\rangle$. For a shared value $a \in F_{p^k}$ the $\langle\cdot\rangle$ representation is defined as follows:

$$\langle a\rangle := (\delta, (a_1, ..., a_n), (\gamma(a)_1, ..., \gamma(a)_n))$$

where $a = \sum_i a_i$ and $\alpha(\delta + a) = \sum_i \gamma(a)_i$. The $\gamma(a)_i$ values are thus MAC values used to authenticate a. Such a value is shared s.t. each party P_i has access to the global value δ along with shares $(a_i, \gamma(a)_i)$.

The second representation used for the protocol, $[\![\cdot]\!]$, is defined in the following way:

$$[\![a]\!] = ((a_1, ..., a_n), (\beta_i, \gamma(a)^i_1, ..., \gamma(a)^i_n)_{i=1,...,n})$$

where $a = \sum_i a_i$ and $a\beta_i = \sum_j \gamma(a)^j_i$. Thus the $\gamma(a)^j_i$ values are used to authenticate a under P_i's personal key β_i. Each player P_i then has the shares $(a_i, \beta_i, \gamma(a)^i_1, ..., \gamma(a)^i_n)$. To open a $[\![\cdot]\!]$ value a player ...

2.4.1 Abstract SHE scheme

The cryptosystem used as the SHE scheme in the protocol has to have certain properties. In particular, such a cryptosystem consists of the algorithms (ParamGen, KeyGen, KeyGen*, Enc, Dec) which behave as follows

ParamGen Parameter generation algorithm.

KeyGen Outputs a keypair pk, sk.

KeyGen* Randomized algorithm outputting a public key $\widehat{pk}$, s.t. an encryption of any message is statistically indistinguishable from an encryption of 0. Additionally, we want a public key generated using **KeyGen** to be statistically indistinguishable from $\widehat{pk}$. This implies IND-CPA security.

Enc

Dec

2.4.2 Concrete instantiation of abstract SHE scheme

The authors also present a concrete instantiation of the abstract SHE scheme described, namely based on the Ring-LWE based public key encryption scheme by Zvika Brakerski and Vinod Vaikuntanathan [] described in section x.x. The **KeyGen**, **Enc**, and **Dec** algorithms of the scheme behave precisely as as the key-gen, encryption, and decryption algorithms described in section x.x. The rest of the algorithms are then defined as follows

ParamGen

KeyGen* Sample $\widehat{a}, \widehat{b} \leftarrow R_q$ and return $\widehat{pk} := (\widehat{a}, \widehat{b})$

2.4.3 Preprocessing phase

The preprocessing phase is implemented by the Prep protocol, which consists of the steps **initialize**, **pair**, and **triple**. These steps use the additional protocols Reshare, PAngle, and PBracket as subroutines.

Reshare:

Protocol PAngle:

PBracket:

Initialize: In the **initialize** step we generate the global and personal keys. This is acheived by the players first calling "start" on $\mathscr{F}_{KeyGenDec}$, so that every player obtains the public key pk. Then the players sample $\alpha_i, \beta_i \in \mathbb{F}_{p^k}$. Following this the players broadcast $e_{\alpha_i} \leftarrow Enc_{pk}(Diag(\alpha_i))$ and $e_{\beta_i} \leftarrow Enc_{pk}(Diag(\beta_i))$, where $Diag(a) = (a, a, ..., a) \in (\mathbb{F}_{p^k})^s$. ZK bla bla bla. Finally, the players homomorphically add the encrypted shares e_{α_i} to get e_α, which they use along with their share $Diag(\alpha_i)$ to generate $[\![Diag(\alpha)]\!]$ using a call to PBracket.

Pair: In **pair** the players generate random values in the two representations $[\![r]\!], \langle r \rangle$. This is done by first sampling a share $r_i \in (\mathbb{F}_{p^k})^s$. Each player then encrypts their share to get $e_{r_i} \leftarrow Enc_{pk}(r_i)$, which they then broadcast. ZK bla bla bla. The players then homomorphically add the encrytped shares to get e_r, which they use along with their share r_i as input to PBracket and PAngle to get $[\![r]\!], \langle r \rangle$.

Triple: The **triple** step generates triples $(\langle a \rangle, \langle b \rangle, \langle c \rangle)$ satisfying $c = ab$. To do this the players start off by sampling shares $a_i, b_i \in (\mathbb{F}_{p^k})^s$. The players then encrypt their shares $e_{a_i} \leftarrow Enc_{pk}(a_i)$, $e_{b_i} \leftarrow Enc_{pk}(b_i)$, and broadcast e_{a_i}, e_{b_i}. ZK bla bla bla. The players then homomorphically add the encrypted shares to get e_a and e_b, and use these along with their shares a_i, b_i to generate $\langle a \rangle$, $\langle b \rangle$ using calls to PAngle. Following this each player homomorphically multiplies e_a and e_b to get e_c, which the players use as input to Reshare to get shares of c along with a new ciphertext $(c_1, ..., c_n, e_{c'})$. Then the players then use their shares of c along with $e_{c'}$ to generate $\langle c \rangle$ by calling PAngle. Finally, the triple $(\langle a \rangle, \langle b \rangle, \langle c \rangle)$ is output.

2.4.4 Online phase

The Online protocol implements the online phase, and consists of the steps **initialize**, **input**, **add**, **multiply**, and **output**. These steps are executed as needed to evaluate the arithemtic circuit that we wish to evaluate.

Initialize: The **initialize** step simply consists using the Prep protocol to generate a global key, along with enough multiplicative triples and random values in the two representations showed earlier, for the circuit that we want to evaluate.

Input: The *input* step lets a player P_i share their private input x_i. The input is shared by taking a pair $[\![r]\!], \langle r \rangle$, and then opening $[\![r]\!]$ to P_i so that P_i gets r. Following this P_i computes and broadcasts $\varepsilon \leftarrow x_i - r$. All players finally set $\langle x_i \rangle \leftarrow \langle r \rangle + \varepsilon$.

Add: To add two values $\langle x \rangle, \langle y \rangle$, we simply perform the component-wise addition $\langle x \rangle + \langle y \rangle$, meaning that each player adds their shares locally.

Multiply:

Output:

2.4.5 Parameter setting

In section D of the paper the authors give example parameter sets and explain how to choose the parameters, s.t. the previously described Ring-LWE public key encryption scheme meets the requirements of the MPC protocol.

2.5 Reuse of unrevealed secret-shared data

Chapter 3

Implementation

We implemented a somewhat-homomorphic public-key encryption scheme in the Rust programming language, as well as functions for adding and multiplying ciphertexts for that encryption scheme.

Dette skal nok opdateres når vi er færdige med implementationen. Skal inkludere det om MPC.

3.1 Polynomials (`poly.rs`)

Since our public-key encryption scheme uses polynomials to represent all of the values we work on (messages, ciphertexts, secret keys, and public keys), we made an implementa

Hvor meget skal forklares her? At det er Brakersky-Vaikuntanathan vi implementerede? At det er baseret på Ring-LWE? Eller bliver det alt sammen beskrevet et andet sted?

3.2 Quotient ring (`quotient_ring.rs`)

Encryption, decryption, and key generation involves adding, subtracting, multiplying, and negating elements in the quotient ring $R_q = Z_q[x]/\langle x^n + 1\rangle$. To be able to do these computations we made a quotient ring implementation, which can be found in `quotient_ring.rs`.

3.2.1 `Rq`

The quotient ring module contains a struct definition `Rq`, which represents an instantiation of a quotient ring $Z_q[x]/\langle f(x)\rangle$. It therefore has fields q and *modulo*, where q is a `BigInt`, and *modulo* is a `Polynomial` representing $f(x)$. The **`new`** function takes q and *modulo* as input, and is used to make a new instantiation of `Rq`.

3.2.2 `reduce`

The `reduce` method found in the quotient ring module is called on an `Rq` struct, takes a polynomial `pol` as input, and returns the normal form of the element `pol` with respect to `modulo`.

To achieve this the method first does polynomial long division with `pol` as the dividend and the `modulo` from the `Rq` struct as the divisor. The remainder computed in this way is then stored in the variable r.

Lastly, we reduce the coefficients of the resulting polynomial r modulo q, by using the remainder operation(%) defined in the `poly.rs` module, and then return the result.

3.2.3 `add`, `times`, `neg`, `mul`

The methods `add`, `times`, `neg`, `mul` are called on an `Rq` struct. These methods first use the addition, scalar multiplication, negation, and polynomial multiplication methods defined in the the `poly.rs` module on the input. Then a reduce call is done with the result as input to get a new R_q element.

3.3 Public-key encryption scheme (`encryption.rs`)

The encryption scheme, as usual, has three major components:

- the `generate_key_pair` function
- the `encrypt` function
- and the `decrypt` function

3.3.1 `generate_key_pair`

The `generate_key_pair` function takes as input an instance of the `Parameters` struct. This struct essentially just defines the parameters that nearly all functions in the encryption scheme use in some form or another. This includes r, n, q, t, and the quotient ring R_q, which are all relevant for the key generation function.

The function starts by sampling polynomials sk and e_0 from a Gaussian distribution with standard deviation r, and the polynomial a_0 uniformly from $\mathbb{Z}_q$.

It then calculates the public-key as $pk = (a_0, a_0 \cdot sk + e_0 \cdot t)$, and finally returns the key pair (pk, sk).

3.3.2 `encrypt`

The `encrypt` function takes a `Parameters` instance, as described above, and additionally takes a polynomial m and a public key pk.

We extract the two polynomials of the public key, a_0 and b_0.

First, we make sure that the message polynomial we are trying to encrypt is in R_t. Then, we sample polynomials v and e' from a Gaussian distribution with standard deviation r, and the polynomial e'' from a Gaussian distribution with standard deviation r' (which is also defined in the `Parameters` struct).

We then calculate $a = a_0 \cdot v + e' \cdot t$ and $b = b_0 \cdot v + e'' \cdot t$. Finally, we create the ciphertext as a `Vec` (a contiguous growable array type) $c = [b + m, a]$ and return it.

3.3.3 `decrypt`

The `decrypt` function takes a `Parameters` instance, as well as a ciphertext $c = [c_0, c_1, \ldots]$ and a secret key sk.

We start by constructing the secret key vector $\mathbf{s} = [1, s, s^2, \ldots]$ from the secret key. We only create the first $|c|$ entries of the secret key vector, as those are the only ones we'll need.

We then initialize a polynomial $msg = 0$, which will become the decrypted message. Then, iterating over each element c_i in the ciphertext, we add $c_i \cdot \mathbf{s}_i$ to msg, where $\mathbf{s}_i$ is the i'th entry (zero-indexed) in the secret key vector.

Currently, the message has coefficients in $\mathbb{Z}_q$, but we need them to be in the range $-\frac{q}{2}$ to $\frac{q}{2}$. Therefore, we iterate through all coefficients x and map them to the new range such that if $x > \frac{q}{2}$, then we let $x' = x - q$, and otherwise $x' = x$.

Finally, we reduce the message modulo t to remove the $e \cdot t$ part of the encryption, and return the result.

Skal nok lige have nogle andre til at tilpasse denne - jeg har svært ved at finde ud af hvordan man forklarer det.

Er det inklusive eller eksklusive i intervallet?

Chapter 4

Conclusion

...

Acknowledgments

…

Bibliography

[1] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Annual cryptology conference*, pages 505–524. Springer, 2011.

[2] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

Appendix A

First appendix