The CKKS Cryptosystem
Part 1: Background

Introduction to Homomorphic Cryptosystems – Lecture 3

What is CKKS?

- Full homomorphic encryption scheme
- Introduced in 2017 by **C**heon, **K**im, **K**im and **S**ong
- Supports fixed-point arithmetic
- Currently the most capable and therefore best working FHE scheme

➡ Many functions (square root, division, …) can be implemented using the CKKS basis

POLYNOMIAL RING

Polynomial Ring

Ring

A ring is a set R, combined with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following axioms

- $(R, +)$ is an abelian group
- $(R, \cdot)$ is a monoid
  - $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ ($\cdot$ is associative)
  - $\exists e \in R: \forall a \in R: e \cdot a = a = a \cdot e$ (multiplicative identity)
  - $\forall a, b \in R: (b \cdot a) \in R$ (closed)
- Multiplication is distributive with respect to addition
  $\forall a, b, c \in R$:
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (left distributivity)
  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (right distributivity)

Reminder group:
- identity
- inverse
- operation is associative
- group is closed under the operation
- abelian: operation is commutative

Example

The integers together with the operations $+$ and $\cdot$ build the ring $(\mathbb{Z}, +, \cdot)$:

Note

$\cdot$ is not necessarily commutative, but if so, we call it a "commutative ring".

Polynomial Ring

From last lecture

Integers modulo m
The set of all congruence classes modulo m is called the **ring** of integers modulo m.

Notation

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{a}_m | a \in \mathbb{Z}\} = \{\bar{0}_m, \bar{1}_m, \bar{2}_m, \dots, \overline{m-1}_m\}$$

$\mathbb{Z}/m\mathbb{Z}$ is also a ring, when we define these operations:

- $\bar{x} + \bar{y}$ is the remainder when the integer $x + y$ is divided by m
- $\bar{x} \cdot \bar{y}$ is the remainder when the integer xy is divided by m

$\bar{x}$ and $\bar{y}$ are $\in \mathbb{Z}/m\mathbb{Z}$

We also call $\mathbb{Z}/m\mathbb{Z}$ a **residue class ring** or **quotient ring**

You can use the same arguments as for $(\mathbb{Z}, +, \cdot)$, to show, that all ring axioms are fulfilled

Polynomial Ring

Polynomial Ring

A polynomial ring is a ring which is formed from the set of polynomials with coefficients from another ring and a variable.

To define a polynomial ring, we need:

- ring R
- variable X

Mathematical Definition

The polynomial ring in X over R (denoted as $\mathrm{R}[X]$) is the set of expressions (polynomials in X) of the form

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m$$

$p_0, \ldots, p_m$ (the coefficients of p) are $\in R$

$p_m \neq 0$ if $m > 0$

X is a symbol and has no value

Polynomial Ring

Operations in a Polynomial Ring

Addition and multiplication of polynomials are defined according to the ordinary rules for algebraic expressions.

Take the two polynomials

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m$$

$$q = q_0 + q_1 X + q_2 X^2 + \cdots + q_{n-1} X^{n-1} + q_n X^n$$

Then addition and multiplication are defined as follows

if $m < n$, then $p_i = 0$ for $m < i \leq n$
if $n < m$, then $q_i = 0$ for $n < i \leq m$

Addition

$$p + q = (p_0 + q_0) + (p_1 + q_1)X + (p_2 + q_2)X^2 + \cdots + (p_k + q_k)X^k$$

$$k = \max(m, n)$$

Multiplication

$$pq = s_0 + s_1 X + s_2 X^2 + \cdots + s_l X^l$$

$$s_i = p_0 q_i + p_1 q_{i-1} + \cdots + p_i q_0$$

$$l = m + n$$

What about the ring axioms?
→ Exercise!

Polynomial Ring

Terminology for polynomials
Take the polynomial

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m$$

We define the following terminology:

The **constant term** of p is p_0 The **degree** of p (written $\deg(p)$) is m. (the largest k such that the coefficient of X^k is not zero) The **leading coefficient** of p is p_m	A **constant** polynomial is either the zero polynomial or of degree zero. Two polynomials are **associated** if either one is the product of the other by a unit. A polynomial is **irreducible** if it's not the product of two non-constant polynomials.

Polynomial Ring

Polynomial Quotient Ring
We can also use a polynomial ring to define a corresponding quotient ring.
This is similar to the definition of $\mathbb{Z}/m\mathbb{Z}$, but for polynomial rings it’s easier to think of them like this:

Given a polynomial p of degree d and a polynomial ring $R[X]$, the quotient (or residue class) ring $R[X]/p$ contains all polynomials with degree less than d.

We need the generally known long division of polynomials for this

Multiplication in $R[X]/p$ is defined the same way as in $\mathbb{Z}/m\mathbb{Z}$:
Given $q, h \in R[X]/p$, then $q \cdot h$ is the remainder when the polynomial $qh \in R[X]$ is divided by p.

Addition
Works the same as in a “normal” polynomial ring.

Polynomial Ring

Polynomial Quotient Ring – Examples

$$\boxed{\mathbb{Z}[X]/(2 + \mathrm{X} + 5\mathrm{X}^3)}$$

This ring contains elements of the form:

$$a_0 + a_1X + a_2X^2 : a_i \in \mathbb{Z}$$

We take two polynomials from the ring:
$p = 3X - 10X^2$, $q = 7 + 4X$

Multiplication

$$h = pq = 21X - 58X^2 - 40X^3$$

Now we calculate $h/(2 + X + 5X^3)$ and take the remainder.
This gives $16 + 29X - 58X^2$ which is the result of the multiplication over the ring.

Addition
We can just calculate $p + q = 7 + 7\mathrm{X} - 10\mathrm{X}^2$

Polynomial Quotient Ring – Examples

$$\mathbb{R}[X]/(X^2+1)$$

irreducible

This ring contains elements of the form:

$$a_0 + a_1 X : a_i \in \mathbb{R}$$

We take two polynomials from the ring:
$p = a + bX$, $q = c + dX$

Multiplication

$$h = pq = ac + adX + bcX + bdX^2$$

Now we calculate $h/(X^2+1)$ and take the remainder:

$$ac + adX + bcX - bd = (ac - bd) + (ad + bc)X$$

If you swap X with i, this exactly corresponds to the definition of multiplication and addition of complex numbers. This means:

$$\mathbb{R}[X]/(X^2+1) = \mathbb{C}$$

Addition

$$p + q = (a + c) + (b + d)X$$

MORE BACKGROUND

Root of Unity

Definition
Given $n \in \mathbb{N}$, we call a number $z \in \mathbb{C}$ the nth root of unity if

$$z^n = 1$$

Every nth root of unity has the form

$$\left(e^{\frac{2\pi i}{n}}\right)^k : k \in \mathbb{N}_0$$

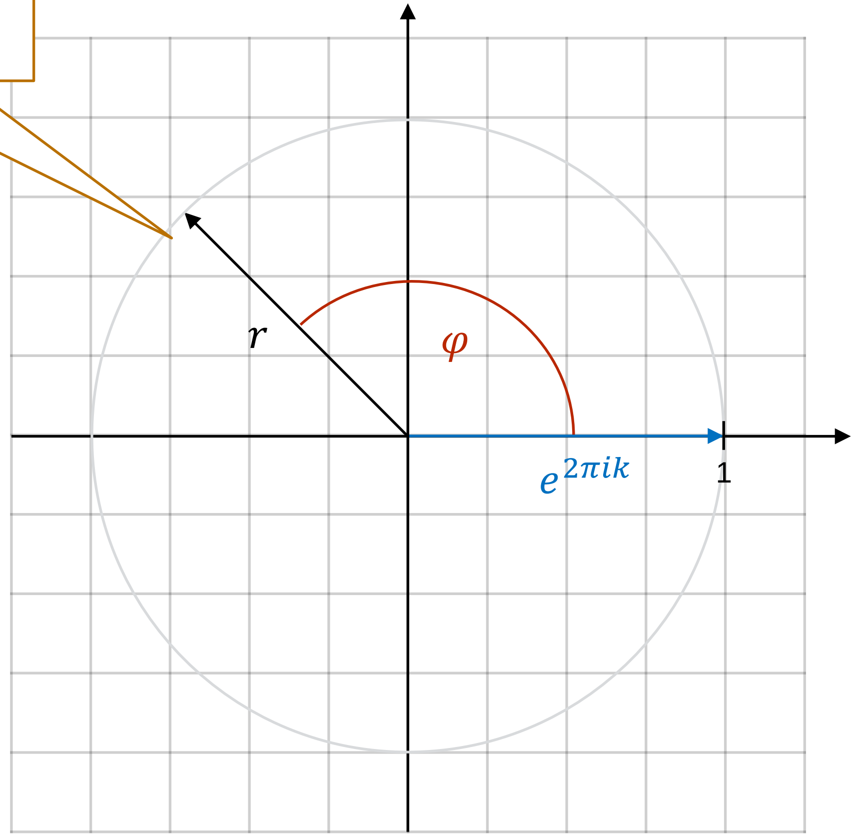
And we define

$$\xi_n := e^{\frac{2\pi i}{n}}$$

There are exactly n different nth roots of unity, because

$$(\xi_n)^n = (\xi_n)^0, (\xi_n)^{n+1} = (\xi_n)^1, \dots$$

Polar form of a complex number:
$re^{\varphi i}$



Root of Unity

Example

$n = 4$

$$(\xi_4)^0 = \left(e^{\frac{2\pi i}{4}}\right)^0 = e^0 = 1$$

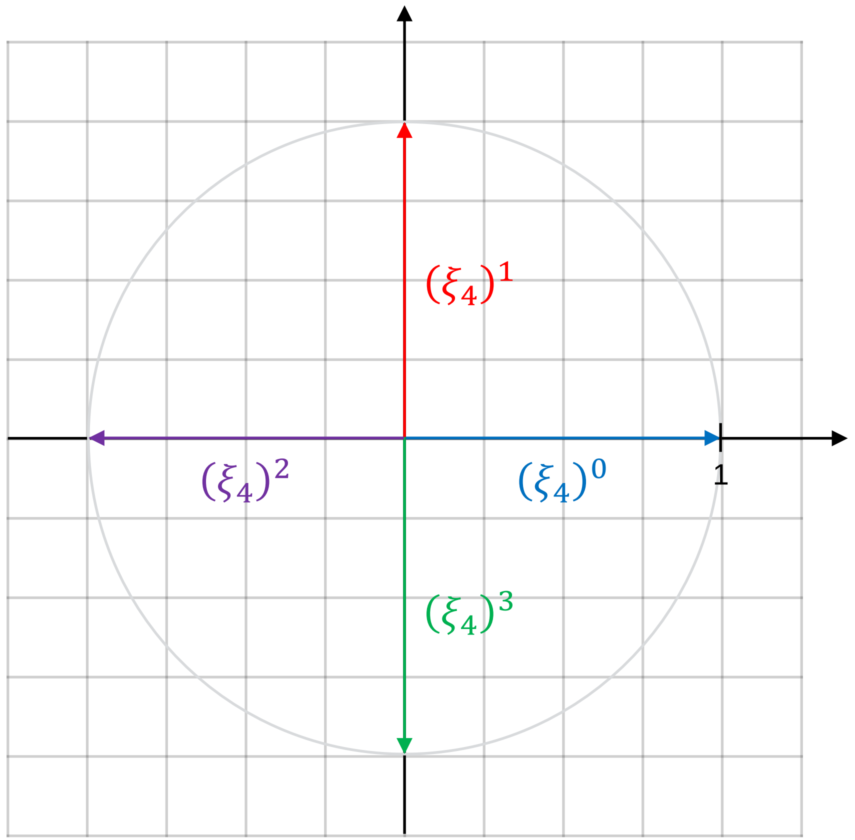
$$(\xi_4)^1 = \left(e^{\frac{2\pi i}{4}}\right)^1 = e^{\frac{1}{2}\pi i} = i$$

$$(\xi_4)^2 = \left(e^{\frac{2\pi i}{4}}\right)^2 = e^{\pi i} = -1$$

$$(\xi_4)^3 = \left(e^{\frac{2\pi i}{4}}\right)^3 = e^{\frac{3}{2}\pi i} = -i$$

$$(\xi_4)^4 = \left(e^{\frac{2\pi i}{4}}\right)^4 = e^{2\pi i} = e^0 = (\xi_4)^0$$

...



Root of Unity

Example

$n = 6$

$$(\xi_6)^0 = \left(e^{\frac{2\pi i}{6}}\right)^0 = e^0 = 1$$

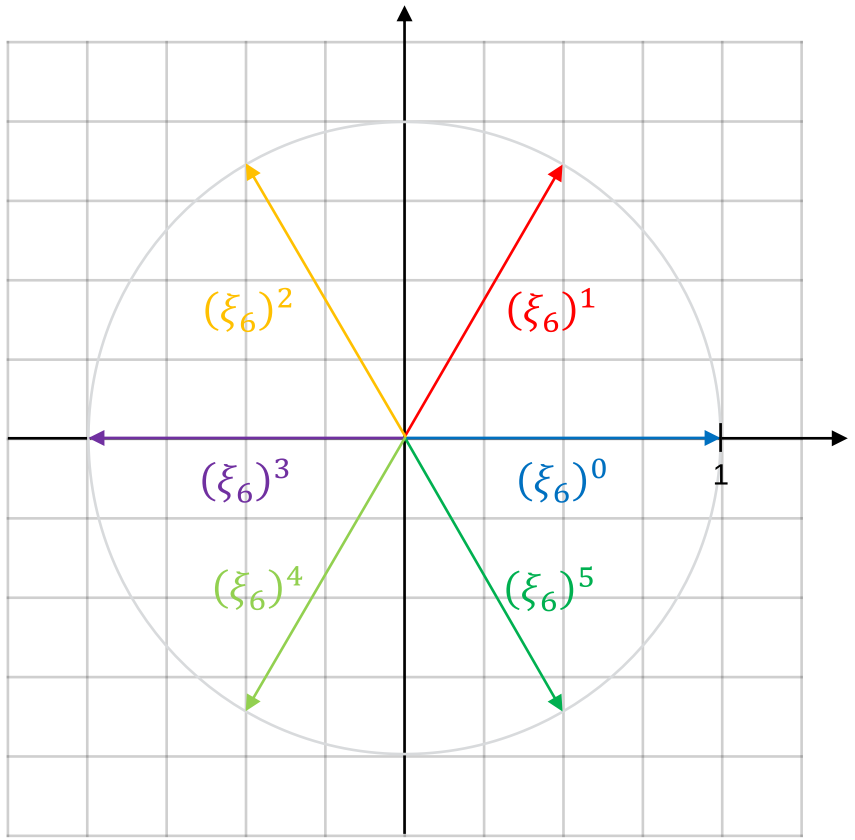
$$(\xi_6)^1 = \left(e^{\frac{2\pi i}{6}}\right)^1 = e^{\frac{1}{3}\pi i}$$

$$(\xi_6)^2 = \left(e^{\frac{2\pi i}{6}}\right)^2 = e^{\frac{2}{3}\pi i}$$

$$(\xi_6)^3 = \left(e^{\frac{2\pi i}{6}}\right)^3 = e^{\pi i} = -1$$

$$(\xi_6)^4 = \left(e^{\frac{2\pi i}{6}}\right)^4 = e^{\frac{4}{3}\pi i}$$

$$(\xi_6)^5 = \left(e^{\frac{2\pi i}{6}}\right)^5 = e^{\frac{5}{3}\pi i}$$



Antisymmetrical Vectors

Definition
Given an even $n \in \mathbb{N}$, a vector v of the form

$$v = \left(v_1, v_2, \dots, v_{\frac{n}{2}-1}, v_{\frac{n}{2}}, \overline{v_{\frac{n}{2}}}, \overline{v_{\frac{n}{2}-1}}, \dots, \overline{v_2}, \overline{v_1}\right) : v_i \in \mathbb{C}$$

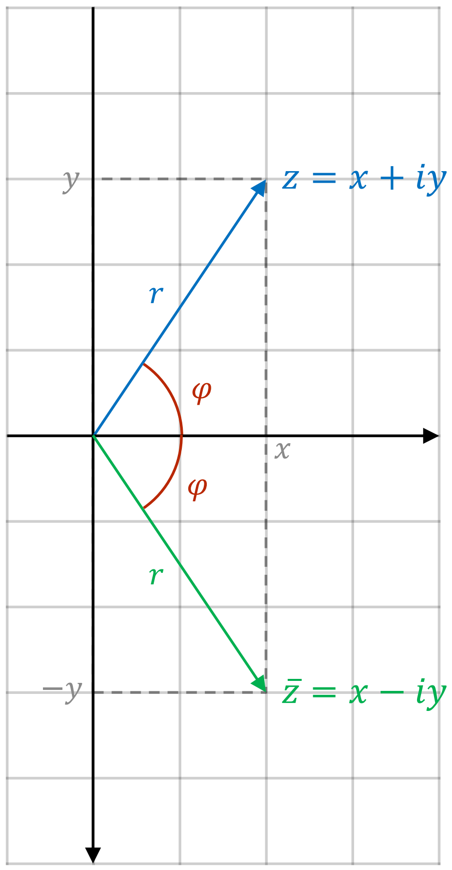
is called an antisymmetric vector in $\mathbb{C}^n$.

$\mathbb{H}_n$represents the set of all antisymmetrical vectors.

We also define the function $\pi : \mathbb{H}_n \to \mathbb{C}^{\frac{n}{2}}$, which takes an antisymmetrical vector and constructs the "normal vector":

$$\mathrm{x} = \left(v_1, \dots, v_{\frac{n}{2}}, \overline{v_{\frac{n}{2}}}, \dots, \overline{v_1}\right)$$
$$\pi(x) = \left(v_1, \dots, v_{\frac{n}{2}}\right)$$

Complex conjugate



Vandermonde Matrix & Coordinate Wise Random Rounding

Vandermonde Matrix
Given a vector $(x_1, \dots, x_n)$, the Vandermonde Matrix is defined as

$$V\big((x_1, \dots x_n)\big) \coloneqq \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

This matrix can be used for polynomial interpolation.

Coordinate Wise Random Rounding
We define *random rounding* as

$$\mathrm{round}\colon \mathbb{R} \to \mathbb{Z},$$
$$x \mapsto \mathrm{round}(x) \coloneqq \begin{cases} \lfloor x \rfloor \text{ with probability } 1 - |x - \lfloor x \rfloor| \\ \lceil x \rceil \text{ with probability } 1 - |x - \lceil x \rceil| \end{cases}$$

Coordinate Wise Random Rounding applies this operation to every component (of a vector, matrix, …).

CKKS OVERVIEW

Notations and Abbreviations

In the following, elements $\in \mathrm{R}_{n,q_L}$ are treated as vectors ($\mathbb{Z}^n$). The coefficients of the polynomial are the vector elements

$$q_L \in \mathbb{N},\ n \in \{2^k \mid k \in \mathbb{N}\},$$
$$h, P \in \mathbb{Z},\ \sigma \in \mathbb{R}^+$$

$\mathbb{Z}_p \coloneqq \mathbb{Z}$ modulo p

$\mathrm{R}_{n,q_L} \coloneqq \mathbb{Z}_{q_L}[X]/(X^n + 1)$

$A * z$

$\coloneqq$ Matrixmultiplication of Matrix A with vector z

$\mathbb{H}_n \coloneqq \left\{\left(v_1, v_2, \dots, v_{\frac{n}{2}}, \overline{v_{\frac{n}{2}}}, \dots, \overline{v_2}, \overline{v_1}\right) \in \mathbb{C}^n\right\}$

$\pi: \mathbb{H}_n \to \mathbb{C}^{\frac{n}{2}}$

$\langle v, w\rangle \coloneqq$ inner product of the vectors $v, w \in \mathbb{C}^n$

$$\langle v, w\rangle \coloneqq \sum_{i=1}^{n} v_i \overline{w_i}$$

$v \odot w, v \oplus w \coloneqq$ coordinate wise $\cdot, +$

$v^\perp \coloneqq$ transpose of v

$$\xi_n \coloneqq e^{\frac{2\pi i}{n}}$$

$V\big((x_1, \dots, x_n)\big) \coloneqq$ Vandermonde Matrix

$$V_n \coloneqq V\left(\left(\xi_{2n}^1, \xi_{2n}^3, \dots, \xi_{2n}^{2n-1}\right)\right)$$

$V_n[i] \coloneqq i$th column of V_n

round $\coloneqq$ random rounding

Summary – What did we learn today?

Rings and Polynomials

A ring consists of a set and two operations (addition and multiplication).

A polynomial ring contains polynomials.

A quotient ring is a special ring, in which after the operation a certain modulus is applied.

More Mathematical Background

Root of Unity

Antisymmetrical Vectors

Vandermonde Matrix

Coordinate Wise Rounding

CKKS

What is CKKS?

Overview over Notations and Abbreviations

Overview over the Algorithms and how information is represented in CKKS.