Homomorphic Encryption

Aaron Geelon So

February 12, 2019

In the following part of the lecture, we will describe how Craig Gentry solved the fully homomorphic encryption problem. Before that, we will need to introduce some definitions and review some abstract algebra.

Definition 1 (Encryption scheme)**.** *An* encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt}, \mathsf{Evaluate})$ *is a tuple of functions:*

1. KeyGen *generates a key-pair* $(\mathrm{sk}, \mathrm{pk})$*,*

2. $\mathsf{Encrypt}(\mathrm{pk}, \pi)$ *maps a plaintext message* π *to a corresponding ciphertext* ψ*,*

3. $\mathsf{Decrypt}(\mathrm{sk}, \psi)$ *decrypts the ciphertext* ψ *back to* π*, and*

4. $\mathsf{Evaluate}(\mathrm{pk}, C, \Psi)$ *applies a function* C' *on the input ciphertexts* $\Psi = \langle \psi_1, \dots, \psi_t \rangle$ *where* C' *is constructed based on an input circuit* C*. We say that* $\mathcal{E}$ *is* correct *for* C *if:*

$$C(\pi_1, \dots, \pi_t) = \mathsf{Decrypt}(\mathrm{sk}, \mathsf{Evaluate}(\mathrm{pk}, C, \Psi)).$$

Definition 2 (Homomorphic encryption)**.** *An encryption scheme* $\mathcal{E}$ *is* homomorphic *for circuits in* $\mathcal{C}_{\mathcal{E}}$ *if* $\mathcal{E}$ *is correct for* $\mathcal{C}_{\mathcal{E}}$*. We say that* $\mathcal{E}$ *is* fully homomorphic *if it is homomorphic for all circuits.*

As a roadmap, we will construct a fully homomorphic encryption scheme by boostrapping off of an encryption scheme that is homomorphic on a smaller set of circuits. This will create a so-called “leveled fully homomorphic encryption scheme” that we’ll define later.

To motivate the theory, we’ll solve $2 + 2 \mod 3$ over and over: first to get a preview of what is to come. Then, to build up intuition about rings and homomorphisms. And finally, to describe the scheme that Gentry defined in [G2009].

1 Spirit of homomorphic encryption

When we perform computations mod 3, we can equivalently describe our computations in the space $\mathbb{Z}/3\mathbb{Z}$. Visually, we represent $\mathbb{Z} \subset \mathbb{R}$ as a 1-dimensional lattice on the real line (for now, I’ll use the term *lattice* informally). Now, consider the sublattice $3\mathbb{Z} \subset \mathbb{Z}$ of integer multiples of 3. We then construct $\mathbb{Z}/3\mathbb{Z}$ by wrapping the real line back on itself.

Of course, $2 + 2 \mod 3 \equiv 1 \mod 3$. And perhaps the easiest way to see this is to unwrap $\mathbb{Z}/3\mathbb{Z}$ back to $\mathbb{Z}$. We know that $2 + 2 = 4$ in the integers. Then, we just map back down to mod 3; we obtain the answer since $4 \mod 3 \equiv 1 \mod 3$.

But what if instead of performing the computation in the integers, we temporarily wrapped the integers up using a different base, say modulo 5? If we used the representatives $\{0, 1, 2, 3, 4\}$ to perform this computation, then we'd obtain $2+2 \mod 5 \equiv 4$, which coincides with the computation that would have occured on $\mathbb{Z}$. Then, taking $4 \mod 3$ again yields the correct answer.

The insight for homomorphic encryption is that we don't need to work with the representatives $\{0,1,2,3,4\}$ to perform this computation. Let's say instead we chose the representatives $\{5,6,7,8,9\}$. Then, 2 would be encoded as 7, so the computation would yield $14 \mod 5$, which is represented by 9. Now, if you tried to transform 9 back into base 3, you'd obtain $2+2 \mod 3 \equiv 0$, which is incorrect. But, if you knew to map 9 mod 5 to the particular representative 4 (hint: this might be kept secret), then we would arrive at the correct answer again, *even though you performed the computation using other representatives.*

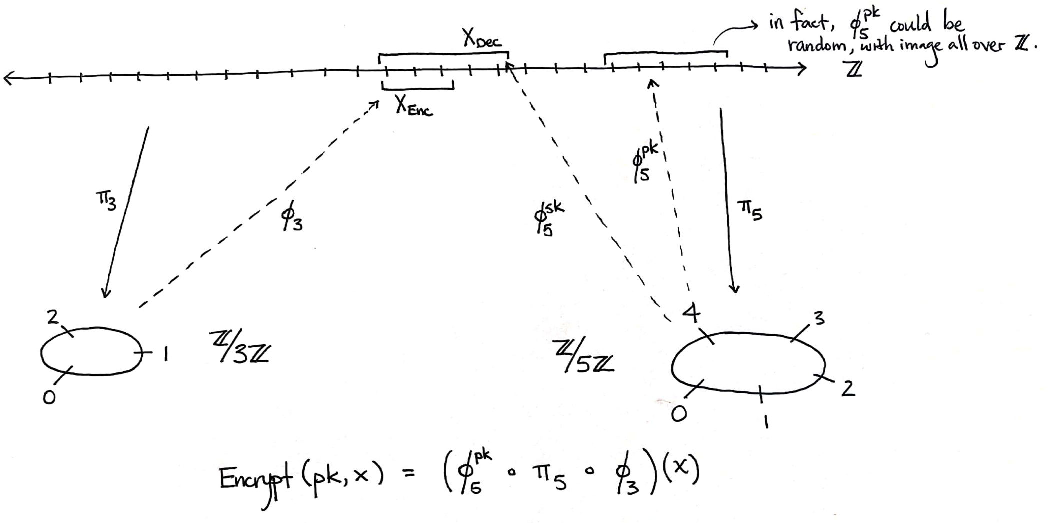

Figure 1: Homomorphic encryption in one dimension.

Notice that in this example, it was vital that the computation $2+2$ in $\mathbb{Z}$ output an answer that was within our representative set $\{0,1,2,3,4\}$. If instead, we computed $2+3=5$, then the 5 would have wrapped back around, represented by 0. It follows that the relationship between the representatives of $\mathbb{Z}/3\mathbb{Z}$ and the representatives of $\mathbb{Z}/5\mathbb{Z}$ within $\mathbb{Z}$ will limit what sort of computations are possible using this technique. This example illustrates the spirit of the homomorphic encryption scheme that Gentry defined in [G2009].

However, this scheme we defined would not be able to provide any privacy; in particular, there are essentially only 3 possible secret keys, so an attacker could just try all three. This is the problem of having defined this scheme on $\mathbb{Z}$, a 1-dimensional space: the space $\mathbb{Z}/3\mathbb{Z}$ has only 3 points. However, if we look at $\mathbb{Z}^n$, the analogous space "$\mathbb{Z}^n/3\mathbb{Z}$" has 3^n points, exponential in n. In the following section, we'll define rings, ideals, and lattices rigorously, which will enable us to give a more concrete construction of [G2009].

2 Review of ring theory

As our goal is ultimately about general computation, we would like a Turing-complete system. One such system is $\{\oplus, \otimes\}$ over the field $\mathbb{F}_2$ (i.e. arithmetic modulo 2). In particular, we would like to generalize the notion of addition/multiplication that we're familiar with over spaces like $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc. Informally, we will call any space R with sensible addition and multiplication operations an *ring.*

Definition 3 (Ring)**.** *A* commutative ring *(with unit) R is a set with two binary operations, $+$ and $\times$, which we call* addition *and* multiplication*, and an element $1 \in R$, which we call the unit, such that:*

(i) addition and multiplication are commutative,

(ii) 1 is a multiplicative unit,

(iii) multiplication distributes over addition.

We can think of a commutative ring as a generalization of a field, except that multiplicative inverses no longer necessarily exist (e.g. integers). In fact, all fields are rings. On the other hand, one important ring that is not a field is $\mathbb{Z}[X]$, the collection of polynomials with integer coefficients over the indeterminant X:

$$\mathbb{Z}[X] := \left\{ \sum_{i=0}^{n} a_i X^i : a_i \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}.$$

Exercise 4. *Define addition and multiplication over $\mathbb{Z}[X]$ through usual polynomial addition and multiplication. Verify that $\mathbb{Z}[X]$ is indeed a ring.*

Just as we generalized a field, we can generalize the concept of a vector space. Usually, we think of a vector space V over the field k as a set such that (i) V is closed under vector addition, (ii) V is closed under scalar multiplication by all elements of k, and (iii) scalar multiplication distributes over vector addition.

Definition 5 (Ideal)**.** *Let R be a ring. A subset $I \subset R$ is an* ideal *if (i) it is closed under addition and (ii) it is closed under multiplication by all elements of R.*

As an example, the set $3\mathbb{Z} = \{3z : z \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$. In fact, all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

Exercise 6. *Show that the only ideals of a field k are the set $\{0\}$ and k itself. For concreteness, let $k = \mathbb{R}$.*

Outline for rest of talk:

1. define quotient rings
2. define ring homomorphism
3. show how $\pi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is a ring homomorphism, relate back to above example
4. give example of quotient ring $\mathbb{Z}[X]/f$ for monic, irreducible polynomial
5. show how if f is monic, degree n, then $\mathbb{Z}[X]/f$ is isomorphic as additive groups to $\mathbb{Z}^n$
6. give intuition for how this adjoins to $\mathbb{Z}$ the roots of f
7. give concrete example $\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i]$
8. give intuition for how to think about the relationship between $\mathbb{Z}[X]/f$ as a ring as $\mathbb{Z}[X]/f$ as a lattice (i.e. addition as translations, multiplication as linear transformations)
9. R/I as the construction of a n-torus, relate back to above example
10. give example of R/I where $I = 3R$
11. define basis, show how they define a natural collection of representatives, define $\mod \mathbf{B}_M$

12. example: $R = \mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[i]$. Let's suppose we want to perform computation over $R/3R$ (i.e. $I = 3R$). Let's use an encryption in $J = 5R$. Let's define public and private bases $\mathbf{B}_J^{\text{sk}} = \{5, 5i\}$ and $\mathbf{B}_J^{\text{pk}} = \{5+15i, 5+5i\}$. Let's compute $2+2$.

    - $\mathsf{Encrypt}(\mathbf{B}_J^{\mathbf{pk}}, 2)$ computed by letting:

    $$2 = a(5+15i) + b(5+5i)$$

    to determine their representation in the public key basis. It follows that:

    $$a = \frac{-2}{10} \qquad b = \frac{6}{10}$$

    However, because our representatives are those vectors within the $[0,1) \times [0,1)$ square, we need to map 2 into that square, thus obtaining the representation:

    $$\left(\frac{8}{10}, \frac{6}{10}\right)$$

    - performing $2+2$ yields:

    $$\left(\frac{8}{10}, \frac{6}{10}\right) + \left(\frac{8}{10}, \frac{6}{10}\right) = \left(\frac{16}{10}, \frac{12}{10}\right) \equiv \left(\frac{6}{10}, \frac{2}{10}\right)$$

    - this represents the vector:

    $$\frac{6}{10}(5+15i) + \frac{2}{10}(5+5i) = 4+10i.$$

    - if we naively take $4+10i \mod \mathbf{B}_I$, we get the answer $1+i$, which is wrong
    - if we know the secret key $\mathbf{B}_J^{\text{sk}}$, then we know to look at the representation 4, which upon applying mod $\mathbf{B}_I$, we obtain the correct answer of 1.

13. summarize intuition: want to perform computation over an integer lattice in the n-torus. The technique is to first unwrap the torus, and wrap it up into a different torus; the original and new tori coincide in some secret location. This is known only through the secret key. To perform computations, you twist the torus so that the two no longer coincide, but if you have the secret key, you can always untwist after the computation.

14. in actual construction: rotation basis, Hermite normal form, and $[-1/2, 1/2)^n$, security related to hardness to the shortest vector problem (and then the shortest n linearly independent set problem)

15. drawing should show the propagation how the vector will tend toward the edge of the secret key basis indicating a need for bootstrapping

References

[G2009] Gentry, C. *"Fully homomorphic encryption using ideal lattices"*. STOC'09. (2009).