Homomorphic Encryption Assignment

Christopher Chianelli and David Zolnieryk

February 11, 2019

Warm Up

Question 1: How is a homomorphic crypto system different than a traditional crypto system?

Recall the RSA crypto system:

1) Choose large primes p and q.
2) Choose encryption key e in $\{1, \ldots, (p-1)\cdot(q-1)\}$ (with $\gcd(e, (p-1)\cdot(q-1)) = 1$).
3) Use Extended Euclidean Algorithm to find $d, k \in \mathbb{Z}$ such that $1 = d \cdot e + k \cdot (p-1)\cdot(q-1)$.
4) Define the public key pk to be $(e, p\cdot q)$ and the private key sk to be $(d, p\cdot q)$.
5) $\mathsf{Enc}((e,n), m) = (m^e) \mod n$.
6) $\mathsf{Dec}((d,n), c) = (c^d) \mod n$.

Question 2:

(a) Show that the RSA crypto system is a homomorphic encryption scheme that preserves multiplication; that is $\mathsf{Eval}(\cdot, c_1, c_2) = c_1 \cdot c_2$ gives a valid encryption of the product of the original messages $a \cdot b$ (i.e. $\mathsf{Enc}((e,n), a\cdot b) = (\mathsf{Enc}((e,n), a) \cdot \mathsf{Enc}((e,n), b)) \mod n$).

(b) How would you need to modify $\mathsf{Eval}(\cdot, c_1, c_2)$ to preserve multiplication if we multiplied by 2 after encrypting? That is, $\mathsf{Enc}((e,n), m) = 2 \cdot ((m^e) \mod n)$ and $\mathsf{Dec}((d,n), c) = \left(\left(\frac{c}{2}\right)^d\right) \mod n$.

(c) Is RSA semantically secure? If it is, prove it. If it is not, explain why not.

(d) Let ξ be a semantically secure encryption scheme. Consider the crypto system that first encrypts a message m by using ξ's encryption function, then uses RSA's encryption function (that is, $\mathsf{Enc}((e,n,k), m) = (\mathsf{Enc}_\xi(k,m))^e \mod n$, where k is ξ's encryption key). The crypto system decrypts by running RSA's decryption

function, followed by ξ's decryption function
(that is, $\mathsf{Dec}((d,n,k),c) = \mathsf{Dec}_{\xi}(k,(c^d) \mod n)$, where k is ξ's decryption key).
Do you think this crypto system is semantically secure? Does this crypto system preserve multiplication using Eval in part (a)?

Homomorphic Secret Sharing

Question 3:

(a) How many lines pass through the point $(0,0)$? Draw diagrams or give equations of the line in the form of $y = mx + b$.

(b) How many lines pass through both $(1,2)$ and $(2,3)$? Prove it and give the equation(s) of the line(s).

(c) How many parabolas pass through both $(-1,0)$ and $(1,0)$? Draw diagrams or give equations of the line in the form of $y = ax^2 + bx + c$.

(d) How many n-degree polynomials pass through a given $n-1$ distinct points? How many n-degree polynomials pass through a given n distinct points? No proof required.

Question 4:

(a) Find a line that path through both $(0,1)$ and $(1,2)$.

(b) Find a line that pass through both $(0,5)$ and $(1,6)$.

(c) Find a line that pass through both $(0,6)$ and $(1,8)$. Is there any relation between the points $(0,6)$ and $(1,8)$ and the points in (a) and (b)? Is there any relation between the line found and the lines found in (a) and (b)?

Question 5: Let find_poly$((x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n))$ be a function that returns a n-degree polynomial that passes through the points $(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)$. Devise a protocol for N voters and M vote counters that use find_poly such that if all voters are not malicious and enter their vote according to the protocol, and no vote counter change their count, guarantees you cannot find out who each voter voted for and returns the correct count.

Question 6: Trace the steps of your protocol if the voter's polynomials are $3x^2 - 2x + 1$, $-5x^2 + 10x - 1$, $x^2 + 10x + 1$ and the vote counters' published numbers are 1, 2 and -1.

Fully Homomorphic Encryption

Question 7: How does fully homomorphic encryption schemes differ from traditional homomorphic encryption schemes?

Question 8:

(a) Convert the following function into a circuit that uses only AND and XOR gates:

```
sort(A : bit, B : bit)
-----------------------
if (A ≤ B)
  return [A, B]
else
  return [B, A]
```

Hints:

1. $(A \leq B) \leftrightarrow (A \rightarrow B)$
2. $(A \rightarrow B) \leftrightarrow ((\text{NOT } A) \text{ OR } B)$
3. NOT $(A$ AND $B) \leftrightarrow (\text{NOT } A)$ OR $(\text{NOT } B)$
4. NOT $A \leftrightarrow 1$ XOR A

(b) Using the encryption scheme given in the slides, what polynomial(s) represents the circuit you created in (a)?

(c) Trace an execution of encrypting $A = 1$ and $B = 0$ (without adding a multiple of the key for simplicity), evaluating the polynomial(s) from part (b), and decrypting the result.

Question 9:

(a) Explain what is *noise* what problems it can cause.

(b) Explain what it means for a homomorphic encryption scheme to be *bootstrappable*.

(c) List the steps required to remove noise from data using bootstrapping.