Lecture 10: Homomorphic Encryption

Cunsheng Ding

HKUST, Hong Kong

March 5, 2024

Contents

Some Elementary Number Theory

The Order of a Modulo n

Theorem 1

Let $a \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. If $\gcd(a, n) = 1$, then there exists an integer $\ell > 0$ such that $a^\ell \equiv 1 \pmod{n}$.

Proof.

Consider the following sequence of elements of $\mathbb{Z}_n$:

$$a^0 \bmod n, a^1 \bmod n, \ldots, a^i \bmod n, \ldots$$

Since $\mathbb{Z}_n$ has n elements, there must exist two integers $0 \leq i < j$ such that $a^i \bmod n = a^j \bmod n$. Consequently, $a^i(a^{j-i} - 1) \equiv 0 \pmod{n}$. Since $\gcd(a, n) = 1$, $a^{j-i} - 1 \equiv 0 \pmod{n}$. □

The Order of a Modulo n

Definition

Let $a \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and $\gcd(a, n) = 1$. The order of a modulo n, denoted by $\operatorname{ord}_n(a)$, is defined to be the smallest positive integer ℓ such that $a^\ell \equiv 1 \pmod{n}$.

Example 2

Let $n = 15$ and $a = 2$. Then $\gcd(a, n) = 1$. Then

$$2^1 \bmod n = 2,\ 2^2 \bmod n = 4,\ 2^3 \bmod n = 8,\ 2^4 \bmod n = 1.$$

Hence, the order of 2 modulo 15 is 4.

A Special Case of Carmichael's Theorem

Set notation: $\mathbb{Z}_m^* := \{i \in \mathbb{Z}_m : \gcd(i, m) = 1\}$. By definition, $|\mathbb{Z}_m^*| = \phi(m)$, where ϕ is the Euler totient function.

Let p and q be two distinct primes. Set $n = pq$. Then $\phi(n) = (p-1)(q-1)$ and

$$|\mathbb{Z}_{n^2}^*| = \phi(n^2) = \phi(p^2 q^2) = p(p-1)q(q-1) = n\phi(n).$$

Theorem 3

Let $\lambda = \mathrm{lcm}(p-1, q-1)$. For any $\omega \in \mathbb{Z}_{n^2}^*$,

$$\omega^\lambda \equiv 1 \pmod{n} \text{ and } \omega^{\lambda n} \equiv 1 \pmod{n^2}.$$

Proof.

Available in books on elementary number theory. $\square$

A 1-to-1 Function from $\mathbb{Z}_n \times \mathbb{Z}_n^*$ to $\mathbb{Z}_{n^2}^*$

Theorem 4

Let p and q be two distinct primes. Set $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$. Assume that $\gcd(n, \phi(n)) = 1$. Let $g \in \mathbb{Z}_{n^2}^*$ such that n divides $\mathrm{ord}_{n^2}(g)$. Define a function F_g from $\mathbb{Z}_n \times \mathbb{Z}_n^*$ to $\mathbb{Z}_{n^2}^*$ by $F_g(x, y) = g^x y^n \bmod n^2$. Then F_g is a bijection.

Proof.

Since $|\mathbb{Z}_n \times \mathbb{Z}_n^*| = |\mathbb{Z}_{n^2}^*| = n\phi(n)$, it suffices to prove that F_g is injective. Suppose that $g^{x_1} y_1^n \equiv g^{x_2} y_2^n \pmod{n^2}$, where $x_1, x_2 \in \mathbb{Z}_n$ and $y_1, y_2 \in \mathbb{Z}_n^*$. It then follows that $g^{x_2 - x_1}(y_2/y_1)^n \equiv 1 \pmod{n^2}$. It then follows from Theorem 3 that

$$g^{\lambda(x_2 - x_1)}(y_2/y_1)^{\lambda n} \equiv g^{\lambda(x_2 - x_1)} \equiv 1 \pmod{n^2}.$$

Thus, $\mathrm{ord}_{n^2}(g) | \lambda(x_2 - x_1)$. Since $n | \mathrm{ord}_{n^2}(g)$, $n | \lambda(x_2 - x_1)$. It then follows from $\gcd(n, \lambda) = 1$ that $x_1 \equiv x_2 \pmod{n}$. Hence, $x_1 = x_2$ and $(y_2/y_1)^n \equiv 1 \pmod{n^2}$, which leads to $y_1 = y_2$ due to $\gcd(n, \phi(n)) = 1$. $\square$

A 1-to-1 Function from $\mathbb{Z}_n \times \mathbb{Z}_n^*$ to $\mathbb{Z}_{n^2}^*$

Theorem in the previous page

Let p and q be two distinct primes. Set $n = pq$ and $\lambda = \mathrm{lcm}(p-1, q-1)$. Assume that $\gcd(n, \phi(n)) = 1$. Let $g \in \mathbb{Z}_{n^2}^*$ such that n divides $\mathrm{ord}_{n^2}(g)$. Define a function F_g from $\mathbb{Z}_n \times \mathbb{Z}_n^*$ to $\mathbb{Z}_{n^2}^*$ by $F_g(x, y) = g^x y^n \bmod n^2$. Then F_g is a bijection.

Problem

Given λ, g, n and any $c \in \mathbb{Z}_{n^2}^*$, how does one compute the unique $x \in \mathbb{Z}_n$ such that

$$c = g^x y^n \bmod n^2?$$

Solution in a special case

In the case that $\gcd(n, ((g^\lambda - 1) \bmod n^2)/n) = 1$, x is given by

$$x = \left(\frac{(c^\lambda - 1) \bmod n^2)}{n} \right) \left(\frac{(g^\lambda - 1) \bmod n^2)}{n} \right)^{-1} \bmod n.$$

Proof of the Solution x

By Theorem 3 and the definitions of c and g, we have $c^\lambda \equiv 1 \pmod{n}$ and $g^\lambda \equiv 1 \pmod{n}$. Hence, there there are $a, b \in \mathbb{Z}_n$ such that

$$c^\lambda \bmod n^2 = an + 1 \text{ and } g^\lambda \bmod n^2 = bn + 1,$$

that is

$$a = \frac{(c^\lambda - 1) \bmod n^2}{n} \text{ and } b = \frac{(g^\lambda - 1) \bmod n^2}{n}.$$

Since F_g is bijective, there exists a unique $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ such that $c = g^x y^n \bmod n^2$. Note that $y^{n\lambda} \equiv 1 \pmod{n^2}$ by Theorem 3. Consequently, $c^\lambda \equiv (g^x y^n)^\lambda \pmod{n^2} \equiv (g^\lambda)^x \pmod{n^2}$. Thus,

$$\begin{aligned} an + 1 &\equiv c^\lambda \pmod{n^2} \equiv (g^\lambda)^x \pmod{n^2} \\ &\equiv (bn + 1)^x \pmod{n^2} \equiv xbn + 1 \pmod{n^2} \end{aligned}$$

where the last equality comes from the fact that $n^2 | \binom{x}{i} (bn)^i$ for all $i \geq 2$. Therefore, $an \equiv xbn \pmod{n^2}$ and $a \equiv xb \pmod{n}$. By assumption, $\gcd(b, n) = 1$. We have $x = ab^{-1} \bmod n$.

The Paillier Public-Key Cipher

The Paillier Public-Key Cipher

Brief information

- The Paillier public-key cipher was invented by and named after Pascal Paillier in 1999.
- Its encryption is probabilistic (i.e., nondeterministic), as the ciphertext depends on a random number.
  This is similar to the encryption of the ElGamal public-key cipher.

The Paillier Public-Key Cipher: Key Generation

1. Choose two large distinct prime numbers p and q randomly and independently of each other such that $\gcd(pq, (p-1)(q-1)) = 1$.
2. Compute $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$.
3. Select a random integer $g \in \mathbb{Z}^*_{n^2}$ such that n divides $\operatorname{ord}_{n^2}(g)$ and $\gcd(n, ((g^\lambda - 1) \bmod n^2)/n) = 1$.
4. Compute $\mu := \left(\frac{g^\lambda - 1 \bmod n^2}{n}\right)^{-1} \bmod n$.

- Public key (n, g), private key (λ, μ).

Remark: If using p, q of the same length, a simpler variant of the above key generation steps is to set $g = n + 1, \lambda = \varphi(n)$, and $\mu = \varphi(n)^{-1} \bmod n$, where $\varphi(n) = (p-1)(q-1)$.

The Paillier Public-Key Cipher: Encryption and Decryption

Encryption with the public key (n, g)

- Let $m \in \mathbb{Z}_n$ be a message to be encrypted ($\mathbb{Z}_n$ is the plaintext space).
- Select a random $r \in \mathbb{Z}_n^*$ (hence, $\gcd(r, n) = 1$).
- Compute ciphertext $c = g^m r^n \bmod n^2$ ($\mathbb{Z}_{n^2}^*$ is the ciphertext space).

Decryption with the private key (λ, μ)

- Let $c \in \mathbb{Z}_{n^2}^*$ be the ciphertext to be decrypted.
- Compute the message as $m = \left(\frac{(c^\lambda - 1) \bmod n^2)}{n}\right) \mu \bmod n$.
  The correctness of decryption was proved on Slide Number 8.

Question

- Why the encryption is probabilistic?

References and Online Demo of the Paillier Cipher

- Paillier, Pascal (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". EUROCRYPT. Springer. pp. 223–238.
- Paillier, Pascal; Pointcheval, David (1999). "Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries". ASIACRYPT. Springer. pp. 165–179.
- Paillier, Pascal (1999). Cryptosystems Based on Composite Residuosity (Ph.D. thesis). École Nationale Supérieure des Télécommunications.
- Paillier, Pascal (2002). "Composite-Residuosity Based Cryptography: An Overview" (PDF). CryptoBytes. 5 (1). Archived from the original (PDF) on October 20, 2006.

Online demo:

- http://security.hsr.ch/msevote/paillier
- https://perso.liris.cnrs.fr/omar.hasan/pprs/paillierdemo/

Motivations for Homomorphic Encryption

Motivations for Homomorphic Encryption

- The main goal of encryption is to ensure the confidentiality of data.
- Recently, in many cases it is desirable to **delegate computations to untrusted computers** (e.g., cloud service provider).
- In such case, only the encrypted version of the data is given to the untrusted computer to process. The computer will perform the computation on this encrypted data, without knowledge of the original plaintext.
- Finally, the computer will send back the computed result, and whoever has the proper deciphering key can decrypt the computed data and obtain the desired computational result.
- To this end, the encryption scheme must have a particular structure.
- Rivest, Adleman, and Dertouzous in 1978 called such encryption schemes **homomorphic encryption schemes**.

A Protocol Illustration of Homomorphic Encryption

A problem description of outsourcing computation

A client C wants a cloud server S to compute $f(m_1, m_2)$, but does not want the server S to know m_1 and m_2. The client C and the server S would use the following protocol, where a **special** encryption scheme is employed.

The protocol

- The client C chooses a secret key k and computes $E_k(m_1)$ and $E_k(m_2)$.
- The client C sends f, $E_k(m_1)$ and $E_k(m_2)$ to the server S, and asks S to return $E_k(f(m_1, m_2))$
- According to f, the server S performs computational operations on $E_k(m_1)$ and $E_k(m_2)$, and computes $E_k(f(m_1, m_2))$, and sends it to the client.
- After receiving $E_k(f(m_1, m_2))$, the client C decrypts it and recovers $f(m_1, m_2)$.

Example: $f(m_1, m_2) = m_1 + m_2$.

Definitions of Homomorphic Encryption

Definition of Partially Homomorphic Encryption

Let $\mathcal{M}$ and $\mathcal{C}$ be the message and ciphertext spaces of a cipher respectively, which are associated with two binary operations $\diamond_m$ and $\diamond_c$, respectively. The encryption scheme is said to be **homomorphic** if for any given encryption key k, the encryption function E_k satisfies

$E_k(m_1 \diamond_m m_2)$ can be computed from $E_k(m_1) \diamond_c E_k(m_2)$ $\forall m_1, m_2 \in \mathcal{M}$.

- It is called a **partially homomorphic encryption** (PHE) scheme, as it is homomorphic for only one pair $(\diamond_m, \diamond_c)$ of operations.
- A partially homomorphic encryption system may be a symmetric or asymmetric cipher!

Definition of Fully Homomorphic Encryption

Let $\mathcal{M}$ and $\mathcal{C}$ be the message and ciphertext spaces of a cipher respectively, which are associated with two pairs of binary operations $(\sqcap_m, \sqcup_m)$ and $(\sqcap_c, \sqcup_c)$, respectively. The encryption scheme is said to be **fully homomorphic** if for any given encryption key k, the encryption function E_k satisfies

$E_k(m_1 \sqcap_m m_2)$ can be computed from $E_k(m_1) \sqcap_c E_k(m_2)$ and
$E_k(m_1 \sqcup_m m_2)$ can be computed from $E_k(m_1) \sqcup_c E_k(m_2)$

for all $m_1, m_2 \in \mathcal{M}$.

Partially Homomorphic Encryption Schemes

Partially Homomorphic Encryption with RSA

RSA

The plaintext and ciphertext spaces are $\mathbb{Z}_n$, where $n = pq$. The operations associated to $\mathbb{Z}_n$ are $\oplus_n$ and $\otimes_n$.

Justification

$$
\begin{aligned}
E_{e_k}(m_1 \otimes_n m_2) &= (m_1 \otimes_n m_2)^e \bmod n \\
&= (m_1^e \bmod n) \otimes_n (m_2^e \bmod n) \\
&= E_{e_k}(m_1) \otimes_n E_{e_k}(m_2).
\end{aligned}
$$

Remark

RSA is **multiplicatively homomorphic**, and partially homomorphic.
RSA is not **additively homomorphic**.

Partially Homomorphic Encryption with ElGamal

ElGamal

ElGamal is multiplicatively homomorphic.

Proof.

It is left to students as an exercise. $\square$

Remark

Note that the message space and ciphertext space are $\mathbb{Z}_p^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$. Both spaces have only one binary operation, i.e., the multiplications.

Partially Homomorphic Encryption with Paillier

Brief information

- The message and ciphertext spaces are $\mathbb{Z}_n$ and $\mathbb{Z}^*_{n^2}$.
- The Paillier cipher is additively homomorphic.
  - This means that, given only the public key and $E(m_1, r_1)$ and $E(m_2, r_2)$, one can compute the $E(m_1 \oplus_n m_2, r_3)$.
  - See the proof in the next page.
- It is not known to be multiplicatively homomorphic.
  - This means that, given $E(m_1, r_1)$ and $E(m_2, r_2)$, there is no known way to compute $E(m_1 \otimes_n m_2, r_3)$ without knowing the private key.

The Paillier Public-Key Cipher: Homomorphic Properties

Additively homomorphic: $m_1 \oplus_n m_2$ can be computed from $E(m_1, r_1) \otimes_{n^2} E(m_2, r_2)$ using the decryption key

Proof.

Let E and D denote the encryption and decryption function of the Paillier cipher, respectively.

$$\begin{aligned} D(E(m_1, r_1) \otimes_{n^2} (E(m_2, r_2)) &= D(g^{m_1} r_1^n g^{m_2} r_2^n \bmod n^2) \\ &= D(g^{m_1 + m_2} (r_1 r_2)^n \bmod n^2) \\ &= m_1 \oplus_n m_2. \end{aligned}$$

□

Fully Homomorphic Encryption Schemes

Existence of Fully Homomorphic Encryption Scheme

Questions

- Is there a fully homomorphic encryption scheme?
- is there a cipher such that
  - it does the encryption bit by bit, and
  - one can compute $E_k(b_0 \oplus_2 b_1)$ and $E_k(b_0 \otimes_2 b_1)$ without knowing the secret key k, given $E_k(b_0)$ and $E_k(b_1)$, where b_0 and b_1 are two bits.

Remark

The questions remained open for a long time!

Several Homomorphic Encryption Schemes

Schemes

- Breakthrough scheme of Gentry in 2009, based on ideal latices.
- van Dijk, Gentry, Halevi and Vaikuntanathan's scheme over the integers in 2010.
- RLWE schemes in 2011.

Challenge

They are not practical due to low performance!

Reference

A. Acar, H. Aksu, and A. S. Uluagac, A survey on homomorphic encryption schemes: theory and implementation, 2017, arXiv:1704.03578v2 [cs.CR].

Applications of Homomorphic Encryption

Applications of Homomorphic Encryption

- Computation outsourcing
- Data mining
- Electronic voting
- Electronic cash
- Machine leaning

- Ismail San, Nuray At, Ibrahim Yakut, Huseyin Polat, Efficient paillier cryptoprocessor for privacy-preserving data mining, Security, Volume 9, Issue 11, 25 July 2016, pp. 1535–1546.
- Cuong Ngo, Secure Voting System Using Paillier Homomorphic.

  https://pdfs.semanticscholar.org/73a6/503dc37faacc96734f551719aec3392e8dc4.pdf
- Michele Minelli. Fully Homomorphic Encryption for Machine Learning. Computer Science [cs]. PSL University, 2018. English. tel-01918263. https://hal.archives-ouvertes.fr/tel-01918263

Appendix: Security of the Paillier Cipher

Security of the Paillier Cipher

DCRA

The **decisional composite residuosity assumption** (DCRA) is a mathematical assumption used in cryptography.
Informally, the DCRA states that given a composite n and an integer z, it is hard to decide whether there exists an integer y such that

$$z \equiv y^n \pmod{n^2}.$$

Security of the Paillier Cipher

It is based on the DCRA.