Public-Key Cryptosystem Based on Composite Degree Residuosity Classes

aka

Paillier Cryptosystem

Harmeet Singh

Public Key Cryptosystems Background

- Foundation of public-key encryption is **trap door one-way function** f
- Difficulty in inverting the *trap door one-way function* does not depend on the function f itself, but on the trap door information
- The inverses of trap door one-way functions are easy to compute given the trap door information
- A public key cryptosystem consists of a pair of invertible transformations:

$$E_k : M \longrightarrow C$$
$$D_k : C \longrightarrow M$$

Where E_k is the enciphering transformation and D_k is the deciphering transformation

Public Key Cryptosystems Background

- The functions $E(\cdot)$ and $D(\cdot)$ are inverses of one another

$$C = E_{K_e}(M) \text{ and } M = D_{K_d}(C)$$

- Encryption and decryption processes are **asymmetric**:

$$K_e \neq K_d$$

- K_e is **public**, known to everyone
- K_d is **private**, known only to the user
- K_e may be easily deduced from K_d
- However, K_d is **NOT** easily deduced from K_e

[1] This slide is taken from course's lecture notes

Public Key Cryptosystems Background

- **RSA:** Encryption and decryption are performed by computing

$$C = M^e \pmod{n}$$
$$M = C^d \pmod{n}$$

  where **(n,e)** is public key, **(d)** is private key and $e \cdot d = 1 \pmod{\phi(n)}$

- **Rabin-Williams:** Encryption and decryption are performed by computing

$$C = M^2 \pmod{n}$$
$$x = c^{(p+1)/4} \pmod{p}$$
$$y = c^{(q+1)/4} \pmod{q}$$
$$m_1 = a \cdot p \cdot q + b \cdot q \cdot x \pmod{n}$$
$$m_2 = a \cdot p \cdot q - b \cdot q \cdot x \pmod{n}$$

  where **n** is public key, **(p,q,a,b)** is private key and $a = p^{-1} \pmod{q}$ and $b = q^{-1} \pmod{p}$

Public Key Cryptosystems Background

ElGamal Cryptosystem

- **Setup:** A prime number p and the generator g of ${Z_p}^*$
- **Keys:** An integer **x** is picked from ${Z_p}^*$. This **x** is private key. Public key **y** is computed as $y = g^x \pmod{p}$
- **Encryption:**

$$\begin{aligned}
\text{Select a random} &: \quad r \in Z_p^* \\
c_1 &: \quad g^r \pmod{p} \\
c_2 &: \quad m \cdot y^r \pmod{p} \\
\text{Ciphertext} &: \quad c = (c_1, c_2)
\end{aligned}$$

- **Decryption**

$$\begin{aligned}
u_1 = c_1^x = (g^r)^x = (g^x)^r &= y^r \pmod{p} \\
u_2 = c_2 \cdot u_1^{-1} = y^r \cdot m \cdot y^{-r} &= m \pmod{p}
\end{aligned}$$

Public Key Cryptosystems Background

- RSA and Rabin-Williams cryptosystem combines the the intractability of factoring large numbers with polynomial-time extraction of roots of polynomials over a finite eld
- ElGamal cryptosystem combines the intractability of extracting discrete logarithms over finite groups with the homomorphic properties of the modular exponentiation

Composite Residuosity Background

Definition 1

A number z is said to be the *n-th* residue modulo n^2 if there exists a number $y \in Z^*_{n^2}$ such that

$$z = y^n \pmod{n^2}$$

- The set of n-residues forms a subgroup of $Z^*_{n^2}$ of order $\phi(n)$
- Each n-residue in $Z^*_{n^2}$ has exactly n roots of degree n

Conjecture 1 (Decisional Composite Residuosity Assumption)

There exists no polynomial time distinguisher for n-th residues modulo n^2.

- Conjecture says that problem of distinguishing *n-th residues* from *non n-th residues* (denoted by CR[n]) is **intractable**

Set Up For Paillier Cryptosystem

- Paillier Encryption scheme is based on **high degree residuosity classes**
- Set $n = pq$ where p and q are large primes
- $\Phi(n) = (p-1)(q-1)$ is the Euler function
- $\lambda(n) = lcm(p-1, q-1)$ is the Carmichael function
- Let $Z^*_{n^2}$ be the multiplicative group. $\mid Z^*_{n^2} \mid = \Phi(n^2) = n\Phi(n)$
- By Carmichael's theorem, for any $w \in Z^*_{n^2}$,

$$w^{\lambda} = 1 \pmod{n}$$
$$w^{n\lambda} = 1 \pmod{n^2}$$

- Define B as the set of elements of $Z^*_{n^2}$ of order $n\alpha$ where $\alpha = 1 \cdots \lambda$

Set Up For Paillier Cryptosystem

- For any $g \in B$, consider the mapping $\varepsilon_g : Z_n \times Z_n^* \mapsto Z_{n^2}^*$ defined as:

$$\varepsilon_g(x, y) \mapsto g^x \cdot y^n \pmod{n^2}$$

Mapping ε_g is one-to-one.

Two sets $Z_n \times Z_n^*$ and $Z_{n^2}^*$have same cardinality.

$g^{x_1} \cdot y_1^n \equiv g^{x_2} \cdot y_2^n \pmod{n^2}$

$\Rightarrow g^{x_2 - x_1}(y_2/y_1)^n \equiv 1 \pmod{n^2}$ as $y_1 \in Z_{n^2}^*$ and thus, its inverse exists

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

$\Rightarrow g^{(x_2 - x_1)\lambda} \equiv 1 \pmod{n^2}$ because of Carmichael's theorem

Thus, $(x_2 - x_1)\lambda$ is a multiple of g's order, and then a multiple of n

Since $gcd(\lambda, n) = 1$, $x_2 - x_1$ is necessarily a multiple of n.

$\Rightarrow x_2 - x_1 = 0 \pmod{n}$ and $(y_2/y_1)^n = 1 \pmod{n^2}$, which leads to the unique solution $(y_2/y_1) = 1$ over Z_n^*

$\Rightarrow x_2 = x_1$ and $y_2 = y_1$. □

Paillier Cryptosystem: Encryption

- For any $g \in B$, the mapping $\varepsilon_g : Z_n \times Z_n^* \mapsto Z_{n^2}^*$:

$$\varepsilon_g(x, y) \mapsto g^x \cdot y^n \pmod{n^2}$$

  is one-to-one.
- Paillier cryptosystem uses this mapping in creating the ciphertext.
- **Encryption**

$$\begin{aligned} \text{Plaintext} &: \quad 0 < m < n \\ \text{Select a random} &: \quad r < n \\ \text{Ciphertext} &: \quad c = g^m \cdot r^n \pmod{n^2} \end{aligned}$$

- For a given (m,r) pair, this mapping will generate a unique ciphertext
- By using the mapping ε_g, we have a mechanism to encrypt a message
- For recovering the message, a mechanism is needed to invert the mapping

Paillier Cryptosystem: Encryption

- **n-residuosity class of** $w \in Z^*_{n^2}$ **w.r.t** $g \in B$ **is denoted as** $\|w\|_g$
- **Definition of** $\|w\|_g$ **:** It is the *unique integer* $x \in Z_n$ for which there exists a $y \in Z^*_n$ such that $\varepsilon_g(x, y) = w$
- In simple language, $\|w\|_g$ denotes an integer $x \in Z_n$ such that

$$w = g^x \cdot y^n \pmod{n^2}$$

for some $y \in Z^*_n$

Paillier Cryptosystem: Definitions

- In paillier cryptosystem, recovering the message from ciphertext is exactly the problem of finding $\|w\|_g$

Definition 2 (*n-th* Residuosity Class Problem)

Given $w \in Z^*_{n^2}$ and $g \in B$, compute $\|w\|_g$. This problem is denoted as $Class[n, g]$

- $Class[n, g]$ is random-self-reducible over $g \in B$. It means that complexity of $Class[n, g]$ is independent from g. Therefore, we can focus on the following problem:

Definition 3 (Composite Residuosity Class Problem)

Given $w \in Z^*_{n^2}$ and $g \in B$, compute $\|w\|_g$. This problem is denoted as $Class[n]$

Paillier Cryptosystem: Definitions

- The ciphertext that we obtain from mapping ε_g belongs to $Z^*_{n^2}$
- By Carmichael's theorem, for any $w \in Z^*_{n^2}$,

$$w^\lambda = 1 \pmod{n}$$

- So, lets consider the set $S_n = \{u < n^2 : u = 1 \pmod{n}\}$
- This S_n is a multiplicative subgroup of integers modulo n^2
- Consider $U = w^\lambda \pmod{n^2}$ and **Note** that $1 + n \in B$

  $w^\lambda \pmod{n^2} = (1+n)^{a\lambda} b^{n\lambda} = (1+n)^{a\lambda} = 1 + a\lambda n \pmod{n^2}$

  $\Rightarrow U \pmod{n} \in S_n$
- Define a function L for $u \in S_n$ as $L(u) = \frac{u-1}{n}$ i.e. quotient of integer division

Paillier Cryptosystem: Decryption

Lemma 4

For any $w \in Z^*_{n^2}, L(w^\lambda \pmod{n^2}) = \lambda \|w\|_{1+n} \pmod{n}$

Proof.

Since $1 + n \in B, \Rightarrow \exists (a, b) \in Z_n \times Z^*_n$ such that

$w = (1+n)^a b^n \pmod{n^2}$

$\Rightarrow a = \|w\|_{1+n}$

Then,

$w^\lambda = (1+n)^{a\lambda} b^{n\lambda} = (1+n)^{a\lambda} = 1 + a\lambda n \pmod{n^2}$

Using the above value in function $L(u)$ defined as $L(u) = \dfrac{u-1}{n}$

$L(w^\lambda \pmod{n^2}) = (1 + a\lambda n - 1)/n = a\lambda = \lambda \|w\|_{1+n} \pmod{n}$ $\square$

Paillier Cryptosystem: Decryption

Lemma 5 (Change of base for $\|w\|_g$)

For $g_1, g_2 \in B, \|w\|_{g_1} = \|w\|_{g_2} \cdot \|g_2\|_{g_1} \pmod{n}$

Proof.

$\|w\|_{g_1} \Rightarrow w = g_1^{x_1} \cdot y_1^n \pmod{n^2}$

$\|w\|_{g_2} \Rightarrow w = g_2^{x_2} \cdot y_2^n \pmod{n^2}$

$\|g_2\|_{g_1} \Rightarrow g_2 = g_1^{x_3} \cdot y_3^n \pmod{n^2}$

$\Rightarrow g_1^{x_1} y_1^n \pmod{n^2} = (g_1^{x_3} . y_3^n)^{x_2} \cdot y_2^n \pmod{n^2}$

$\Rightarrow g_1^{x_1} y_1^n \pmod{n^2} = g_1^{x_2 . x_3} \cdot y_3^{n . x_2} \cdot y_2^n \pmod{n^2}$

$\Rightarrow g_1^{x_1} y_1^n = g_1^{x_2 . x_3 \pmod{n}} \cdot \{(g_1^{x_2 . x_3 \text{ div n}}) \cdot y_3^{x_2} \cdot y_2\}^n \pmod{n^2}$

$\Rightarrow x_1 = x_2 \cdot x_3 \pmod{n}$ □

From above lemma, we can show that $\|g_1\|_{g_2}^{-1} = \|g_2\|_{g_1}$ modulo n

Paillier Cryptosystem: Decryption

- For any $g \in B$ and $w \in Z^*_{n^2}$,

$$\frac{L(w^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} = \frac{\lambda \|w\|_{1+n}}{\lambda \|g\|_{1+n}} = \frac{\|w\|_{1+n}}{\|g\|_{1+n}} = \|w\|_g \pmod{n}$$

by using previous two lemmas

Paillier Encryption: Complete Setup

- Key generation: p, q be prime numbers. Let $n = p \cdot q$ and $g \in B$. Pair (n, g) is public key and (p, q, λ) is private key
  Note: To check if $g \in B$, check whether $gcd(\ L(g^{\lambda}\ mod\ n^2), n) = 1$
- Encryption

$$\begin{aligned} \text{Plaintext} &: \quad 0 < m < n \\ \text{Select a random} &: \quad r < n \\ \text{Ciphertext} &: \quad c = g^m \cdot r^n \pmod{n^2} \end{aligned}$$

- Decryption

$$\begin{aligned} \text{ciphertext} &: \quad c < n^2 \\ \text{plaintext} &: \quad m = \frac{L(c^{\lambda} \pmod{n^2})}{L(g^{\lambda} \pmod{n^2})} \pmod{n} \end{aligned}$$

Paillier Encryption: An Example

- $p = 7$ and $q = 11$ and $n = 77$, $n^2 = 5929$
- $\mathrm{g} = 78$, as $78^{77} \pmod{77^2} = 1$
- Public key : $(77, 78)$, Private key : $(7, 11, \lambda = lcm(6, 10) = 30)$
- Encryption

$$\begin{aligned} \text{Plaintext} \quad &: \quad m = 23 \\ \text{Select a random} \quad &: \quad r = 51 \\ \text{Ciphertext} \quad &: \quad c = 78^{23} \cdot 51^{77} \pmod{5929} = 193 \end{aligned}$$

- Decryption

$$\begin{aligned} \text{ciphertext} \quad &: \quad c = 193 \\ \text{plaintext} \quad &: \quad m = \frac{L(193^{\lambda} \pmod{5929})}{L(78^{\lambda} \pmod{5929})} \pmod{77} \\ &= \quad 74 \cdot 30^{-1} \pmod{77} = 74 \cdot 18 \pmod{77} \\ &= \quad 23 \end{aligned}$$

Paillier Encryption: Discussion

- It is a probabilistic encryption scheme i.e. randomness is used while encrypting the message
- Therefore, a same message will be mapped to different cipertexts with high probability
- If message $m = 0$, the encryption will be:

$$\begin{aligned} \text{Plaintext} &: \quad m = 0 \\ \text{Select a random} &: \quad r < n \\ \text{Ciphertext} &: \quad c = g^0 \cdot r^n \pmod{n^2} = r^n \pmod{n^2} \end{aligned}$$

- As we can observe, different ciphertexts will be generated each time 0 is encrypted
- This encryption is secure by Conjecture **Decisional Composite Residuosity Assumption** given on slide 7

Paillier Encryption: Properties

- $p = 7$, $q = 11$, $n = 77$, $n^2 = 5929$, $g = 78$ and $\lambda = 30$
- Compute $L(78^{\lambda} \pmod{5929})^{-1} \pmod{77} = 18$
- Message $m_1 = 23$ and Message $m_2 = 31$
- **Homomorphic addition**: For all $m_1, m_2 \in Z_n$, and $k \in N$

$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m_1)\ \mathbf{E}_{PE}(m_2) \pmod{n^2}) = m_1 + m_2 \pmod{n}$$
$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m_1)\ g^{m_2} \pmod{n^2}) = m_1 + m_2 \pmod{n}$$

- **Example:** $(c_1 = 193, r_1 = 51)$, $(c_2 = 822, r_2 = 61)$

$c_1 * c_2 \pmod{5929} = 4492$
$\mathbf{D}_{PE}(4492) = L(4492^{\lambda} \pmod{5929}) * 18 \pmod{77} = 3.18 = 54$

- **Example:** $g^{m_2} = 78^{31}$

$c_1 * g^{m_2} \pmod{5929} = 4351$
$\mathbf{D}_{PE}(4351) = L(4351^{\lambda} \pmod{5929}) * 18 \pmod{77} = 3.18 = 54$

Paillier Encryption: Properties

- **Homomorphic multiplication**: For all $m_1, m_2 \in Z_n$, and $k \in N$

$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m_1)^{m_2} \pmod{n^2}) = m_1 \cdot m_2 \pmod{n}$$
$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m_2)^{m_1} \pmod{n^2}) = m_1 \cdot m_2 \pmod{n}$$
$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m_1)^{k} \pmod{n^2}) = k \cdot m_1 \pmod{n}$$

- **Example:** $c_1^{m_2} \pmod{n^2} = 193^{31} \pmod{5929} = 3042$

  $\mathbf{D}_{PE}(3042) = L(3042^{\lambda} \pmod{5929}) * 18 \pmod{77} = 61.18 = 20$
- **Example:** $c_1^{-1} \pmod{n^2} = 193^{-1} \pmod{5929} = 5161$

  $\mathbf{D}_{PE}(5161) = L(5161^{\lambda} \pmod{5929}) * 18 \pmod{77} = 3.18 = 54$

Paillier Encryption: Properties

- **Self-Blinding**: Any ciphertext can be publicly changed into another without affecting plaintext: For all $m \in Z_n$, and $r \in N$

$$\mathbf{D}_{PE}(\ \mathbf{E}_{PE}(m)\ r^n \pmod{n^2}) = m$$

- **Example:** $r = 46$

$$c_1 * r^n \pmod{5929} = 193 * 46^{77} \pmod{5929} = 5300$$
$$\mathbf{D}_{PE}(5300) = L(5300^{\lambda} \pmod{5929}).18 = 74.18 = 1332 = 23 = m_1$$

Security of Paillier Encryption

Theorem 6

Class[n] $\Leftarrow$ Fact[n] i.e. Class[n] problem is polynomially reducible to Fact[n]

- If factors of n are known, then $\lambda(n) = lcm(p-1, q-1)$ can be computed.
- **RSA problem**: It is denoted by $RSA[n, e]$. For a given RSA public key (n, e) and a ciphertext $C = M^e \pmod{n}$, compute M

Theorem 7

Class[n] $\Leftarrow$ RSA[n,n] i.e. Class[n] problem is polynomially reducible to RSA[n,n]

- Above theorem means that solving RSA[n,n] problem will solve the Class[n] problem

Security of Paillier Encryption

Theorem 8

Class[n] $\Leftarrow$ RSA[n,n] i.e. Class[n] problem is polynomially reducible to RSA[n,n]

Proof.

Let us be given an oracle for RSA[n,n].
We know that $w = (1+n)^x \cdot y^n \pmod{n^2}$ for some $x \in Z_n$ and $y \in Z_n^*$.
$\Rightarrow w = y^n \pmod{n}$
$\Rightarrow y = RSA[n,n] \longleftarrow w \pmod{n}$
Using the y that we computed from RSA[n,n] oracle, we can compute w

$$\frac{w}{y^n} = (1+n)^x = 1 + nx \pmod{n^2}$$

which discloses $x = \|w\|_{1+n}$
Since all instances of $Class[n,g]$ are computationally equivalent
$\Rightarrow Class[n] \Leftarrow RSA[n,n]$ □

One-Way Trapdoor Permutation

- Encryption:

$$\begin{aligned} \text{Plaintext} \quad & m < n^2 \\ \text{split m into } m_1, m_2 \text{ such that} \quad & m = m_1 + nm_2 \\ \text{Ciphertext} \quad & c = g^{m_1} \cdot m_2^n \pmod{n^2} \end{aligned}$$

- Decryption

$$\begin{aligned} \text{ciphertext} \quad & c < n^2 \\ \text{Step 1.} \quad & m_1 = \frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} \pmod{n} \\ \text{Step 2.} \quad & c' = cg^{-m_1} \pmod{n} \\ \text{Step 3.} \quad & m_2 = c'^{\,n^{-1} \pmod{\lambda}} \pmod{n} \\ \text{plaintext} \quad & m = m_1 + nm_2 \end{aligned}$$

One-Way Trapdoor Permutation

- The scheme defined above is one-way iff RSA[n,n] is hard
- Scheme is permutation because ε_g is bijective
- By definition of ε_g, it is required that $m_2 \in Z_n^*$
- Thus, the scheme defined above cannot be used for encrypting messages smaller than n