Chalk & Talk: 14

Paillier Encryption Scheme, DCR Assumptions and IND-CPA Security

Course Code: `CS409`

Course Name: `Introduction to Cryptography`

Instructor: Prof. Sruthi Sekar

Authors:

Pratham Agarwal (22b2111)

Anusha Dhakras (210020019)

November 27, 2024

Abstract

This report presents an in-depth analysis of the Paillier encryption scheme, a well-known cryptosystem in the field of homomorphic encryption, which allows computations to be performed on ciphertexts without needing to decrypt them first. The study begins with an introduction to the concept of homomorphic encryption, followed by an exploration of the underlying group structure $\mathbb{Z}_{N^2}^*$ and the key propositions essential to the scheme's functionality. Key aspects of the Paillier encryption process, including key generation, encryption, and decryption, are thoroughly discussed to elucidate the mechanics of this cryptosystem. Furthermore, the report delves into the Decisional Composite Residuosity Assumption (DCRA), which serves as the security foundation for Paillier encryption, and examines the IND-CPA security of the scheme through both intuitive and formal proofs. Finally, the report concludes with a summary of the findings and the implications of Paillier encryption in secure communication and privacy-preserving computations.

Contents

1 Homomorphic Encryption

Paillier's cryptosystem is a public-key homomorphic encryption scheme. Homomorphic encryption refers to encryption schemes that allow computations to be performed on encrypted data without needing to decrypt it first. This is a powerful feature for privacy-preserving computations, allowing data to remain confidential while still enabling useful operations, such as in secure voting systems, privacy-preserving machine learning, and more. The Paillier cryptosystem is additively homomorphic, meaning it supports the following operation on ciphertexts:
For $\text{Enc}(m_1) \to c_1$ and $\text{Enc}(m_2) \to c_2$

- Encrypting $m_1 + m_2$ corresponds to $c_1 \cdot c_2$
- Encrypting $k \cdot m_1$ corresponds to c_1^k

Thus, we can directly perform these operations on the ciphertexts and then perform the decryption to get the corresponding plaintext messages.

2 The Group $\mathbb{Z}_{N^2}^*$

In this section, we understand about the group $\mathbb{Z}_{N^2}^*$ and some prepositions which characterize this group. It's important to study $\mathbb{Z}_{N^2}^*$ group because Paillier Encryption Scheme utilizes this group.
The group $\mathbb{Z}_{N^2}^*$ is the multiplicative group pf elements in the range $\{1, \ldots, N^2\}$ that are relatively prime to N where N is a product of two distinct primes. We know study the following propositions of the group $\mathbb{Z}_{N^2}^*$ which will be helpful for understanding the Paillier Encryption Scheme.

2.1 Propositions

Consider $N = pq$, where p and q are two odd distinct primes having different lengths (i.e in binary representation, p and q must have same length). The following three propositions are needed to understand the encryption scheme:

1. $gcd(N, \phi(N) = 1$, i.e. N and $\phi(N)$ are coprime to each other

2. For any integer $a \geq 0$, we have $(1+N)^a = (1+aN) \mod N^2$.
   As a consequence, the order of $(1+N)$ in $\mathbb{Z}^*_{N^2}$ is N. That is, $(1+N)^N \equiv 1 \mod N^2$ and $(1+N)^a \equiv 1 \mod N^2$ for any $1 \leq a < N$.

3. $\mathbb{Z}_N \times \mathbb{Z}^*_N$ is isomorphic to $\mathbb{Z}^*_{N^2}$, with isomorphism $f : \mathbb{Z}_N \times \mathbb{Z}^*_N \to \mathbb{Z}^*_{N^2}$ given by $f(a,b) = [(1+N)^a \cdot b^N \mod N^2]$.

With N understood, and $x \in \mathbb{Z}^*_{N^2}$, $a \in \mathbb{Z}_N$, $b \in \mathbb{Z}^*_N$, let $x \leftrightarrow (a,b)$ if $f(a,b) = x$, where f is the isomorphism from the proposition above.
One way to think about this notation is that it means "x in $\mathbb{Z}^*_{N^2}$ corresponds to (a,b) in $\mathbb{Z}_N \times \mathbb{Z}^*_N$."

2.2 Proofs of the Prepositions

In this section, the proofs of the prepositions given in section 2.1 have been provided
CLAIM 1: $gcd(N, \phi(N) = 1$

Proof: Recall that $\phi(N) = (p-1)(q-1)$. Assume, without loss of generality, that $p > q$. Since p is prime and $p > p-1 > q-1$, it follows that $\gcd(p, \phi(N)) = 1$. Similarly, $\gcd(q, q-1) = 1$. Now, if $\gcd(q, p-1) = 1$, then $\gcd(q, p-1) = q$, as q is prime. However, this implies $(p-1)/q \geq 2$, which contradicts the assumption that p and q have the same length.

CLAIM 2: For any integer $a \geq 0$, we have $(1+N)^a = 1 + aN \mod N^2$. Therefore, the order of $(1+N)$ in $\mathbb{Z}^*_{N^2}$ is N.

Proof: Using the binomial expansion theorem, we have:

$$(1+N)^a = \sum_{i=0}^{a} \binom{a}{i} N^i.$$

Reducing the right-hand side modulo N^2, all terms with $i \geq 2$ become 0, and thus we have:

$$(1+N)^a = 1 + aN \mod N^2.$$

The smallest nonzero a such that $(1+N)^a = 1 \mod N^2$ is therefore $a = N$.

CLAIM 3: The group $\mathbb{Z}_N \times \mathbb{Z}_N^*$ is isomorphic to the group $\mathbb{Z}_{N^2}^*$, with the isomorphism $f : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*$ given by

$$f(a,b) = \left[(1+N)^a \cdot b^N \mod N^2\right].$$

Proof: Note that $(1+N)^a \cdot b^N$ has no common factor with N^2 since $\gcd((1+N), N^2) = 1$ and $\gcd(b, N^2) = 1$ (because $b \in \mathbb{Z}_N^*$). Thus,

$$\left[(1+N)^a \cdot b^N \mod N^2\right] \in \mathbb{Z}_{N^2}^*.$$

We now prove that f is an isomorphism. To begin, we first show that f is a bijection. Since $|\mathbb{Z}_{N^2}^*| = \phi(N^2) = p \cdot (p-1) \cdot q \cdot (q-1) = pq \cdot (p-1)(q-1)$, it suffices to demonstrate that f is one-to-one. Assume $a_1, a_2 \in \mathbb{Z}_N$ and $b_1, b_2 \in \mathbb{Z}_N^*$ such that $f(a_1, b_1) = f(a_2, b_2)$. Then,

$$(1+N)^{a_1 - a_2} \cdot \left(\frac{b_1}{b_2}\right)^N = 1 \mod N^2. \tag{1}$$

(Note that $b_2 \in \mathbb{Z}_N^*$ and thus $b_2 \in \mathbb{Z}_{N^2}^*$, so b_2 has a multiplicative inverse modulo N^2.) Raising both sides to the power of $\phi(N)$ and using the fact that the order of $\mathbb{Z}_{N^2}^*$ is $\phi(N^2) = N \cdot \phi(N)$, we obtain:

$$(1+N)^{(a_1 - a_2) \cdot \phi(N)} = 1 \mod N^2.$$

By Claim 2, $(1+N)$ has order N modulo N^2. We see that:

$$(a_1 - a_2) \cdot \phi(N) = 0 \mod N,$$

which implies that N divides $(a_1 - a_2) \cdot \phi(N)$. Since $\gcd(N, \phi(N)) = 1$ by Claim 1, it follows that N divides $a_1 - a_2$. Because $a_1, a_2 \in \mathbb{Z}_N$, this can only occur if $a_1 = a_2$.

Returning to Equation (1) and setting $a_1 = a_2$, we obtain:

$$b_1^N = b_2^N \mod N^2,$$

which implies $b_1^N = b_2^N \mod N$. Since N is relatively prime to $\phi(N)$, exponentiation to the power of N in $\mathbb{Z}_N^*$ is a bijection. Thus, $b_1 = b_2 \mod N$, and since $b_1, b_2 \in \mathbb{Z}_N^*$, we conclude that $b_1 = b_2$. This proves that f is one-to-one, and hence a bijection.
Next, we show that f is an isomorphism by proving that:

$$f(a_1, b_1) \cdot f(a_2, b_2) = f(a_1 + a_2, b_1 \cdot b_2).$$

(Note that the multiplication on the left-hand side is modulo N^2, while addition and multiplication on the right-hand side are modulo N.)
We compute:

$$f(a_1, b_1) \cdot f(a_2, b_2) = (1+N)^{a_1} \cdot b_1^N \cdot (1+N)^{a_2} \cdot b_2^N \mod N^2 = (1+N)^{a_1+a_2} \cdot (b_1 b_2)^N \mod N^2.$$

Since $(1+N)$ has order N modulo N^2 (by Claim 13.8), we apply Proposition 8.52 to get:

$$f(a_1, b_1) \cdot f(a_2, b_2) = (1+N)^{a_1+a_2} \cdot (b_1 b_2)^N \mod N^2 = (1+N)^{[a_1+a_2 \mod N]} \cdot (b_1 b_2)^N \mod N^2. \tag{2}$$

At this point, we need to ensure that $b_1 b_2$ is taken modulo N, not N^2. Let $b_1 b_2 = r + \gamma N$, where γ and r are integers with $1 \leq r < N$ (and $r \neq 0$ since $b_1, b_2 \in \mathbb{Z}_N^*$, implying that their product is not divisible by N). We note that $r = b_1 b_2 \mod N$, and thus:

$$(b_1 b_2)^N = (r + \gamma N)^N \mod N^2 = rN \mod N^2.$$

Using the binomial expansion theorem as in Claim 2, we obtain:

$$rN \mod N^2 = [b_1 b_2 \mod N] \cdot N \mod N^2.$$

Substituting this into the previous equation, we get the desired result:

$$f(a_1, b_1) \cdot f(a_2, b_2) = (1+N)^{a_1+a_2 \mod N} \cdot (b_1 b_2 \mod N)^N \mod N^2 = f(a_1 + a_2, b_1 b_2).$$

Thus, we have proven that f is an isomorphism from $\mathbb{Z}_N \times \mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$.

3 The Paillier Encryption Scheme

In this section we provide the key generation algorithm, encryption and decryption methods of the Paillier Encryption Scheme.

3.1 Key Generation

In Paillier Encryption Scheme, the key generation process starts by running the polynomial-time algorithm `GenModulus` on input 1^n, where n is the security parameter. The algorithm generates two random n-bit prime numbers, p and q, and computes their product $N = p \cdot q$. The modulus N is used as the public key. The private key consists of N and $\varphi(N) = (p-1)(q-1)$, where $\varphi(N)$ is Euler's totient function. The public key is N, while the private key is $\langle N, \varphi(N) \rangle$.

3.2 Encryption

We have described encryption previously as though it is taking place in $\mathbb{Z}_N \times \mathbb{Z}_N^*$. In fact, it takes place in the isomorphic group $\mathbb{Z}_{N^2}^*$. That is, the sender generates a ciphertext $c \in \mathbb{Z}_{N^2}^*$ by choosing a uniform $r \in \mathbb{Z}_N^*$ and then computing

$$c := \left[(1+N)^m \cdot r^N \mod N^2\right].$$

$$c = (1+N)^m \cdot 1^N \cdot (1+N)^0 \cdot r^N \mod N^2 \quad \longleftrightarrow \quad (m,1) \cdot (0,r),$$

and so $c \longleftrightarrow (m, r)$ as desired.

3.3 Decryption

Decryption can be efficiently performed given the factorization of N. For a ciphertext c constructed as described above, the message m can be recovered by following these steps:

- Compute $\hat{c} := \left[c^{\phi(N)} \mod N^2\right]$.
- Compute $\hat{m} := \frac{\hat{c}-1}{N}$, where this operation is carried out over the integers.

- Finally, compute $m := \hat{m} \cdot \phi(N)^{-1} \mod N$.

To understand why the decryption process works, let's consider a ciphertext c that corresponds to the pair (m, r), where $r \in \mathbb{Z}_N^*$. We start by computing $\hat{c} = [c^{\phi(N)} \mod N^2]$, which corresponds to $(m, r^{\phi(N)})$. By the properties of modular arithmetic, this becomes:

$$\hat{c} = [m \cdot \phi(N) \mod N], [r^{\phi(N)} \mod N].$$

Now, applying CLAIM 3, we know that:

$$\hat{c} = (1 + N)[m \cdot \phi(N) \mod N] \mod N^2.$$

Next, using CLAIM 2, we simplify:

$$\hat{c} = (1 + N)[m \cdot \phi(N) \mod N] = (1 + [m \cdot \phi(N) \mod N] \cdot N) \mod N^2.$$

Since the expression $1 + [m \cdot \phi(N) \mod N] \cdot N$ is always less than N^2, we can ignore the modulo N^2 at the end. Thus, we have the equality over integers:

$$\hat{m} = \frac{\hat{c} - 1}{N} = [m \cdot \phi(N) \mod N].$$

Finally, to recover the original message m, we compute:

$$m = [\hat{m} \cdot \phi(N)^{-1} \mod N].$$

This completes the decryption process, and the calculations are valid since $\phi(N)$ is invertible modulo N (as $\gcd(N, \phi(N)) = 1$).

4 Decisional Composite Residuosity Assumption

The Decisional Composite Residuosity Assumption states that, given:

1. A composite integer N = p · q, where p and q are large primes
2. An integer $z \in \mathbb{Z}_N^{2*}$ (the multiplicative group modulo N^2)

It is computationally hard to decide whether z is an n-th residue modulo N^2.

$$z \equiv y^N \bmod N^2$$

Thus, the decisional composite residuosity problem, roughly speaking, states that it is hard to distinguish a uniform element of $\mathbb{Z}_N^{2*}$ (z,r) from a uniform element of the set of Nth residues modulo N^2 $[r^N \bmod N^2)]$.

$$| \Pr[D(N,[r^N \bmod N^2]) = 1] - \Pr[D(N,z)=1] | \leq \text{negl(n)}$$

5 IND-CPA Security of the scheme

5.1 Intuitive proof

As we know that the group $\mathbb{Z}_N^{2*}$ is isomorphic to $\mathbb{Z}_N \ X \ \mathbb{Z}_N^*$. A consequence is that a uniform element y $\in \mathbb{Z}_N^{2*}$ corresponds to a uniform element (a,b) $\in \mathbb{Z}_N \ X \ \mathbb{Z}_N^*$. If
y = $x^N \bmod N^2$ for x $\in \mathbb{Z}_N^{2*}$, it corresponds to x $\leftrightarrow$ (a,b).

$$(a,b)^N = (\text{N}\cdot \text{ a mod N}, b^N \bmod \text{N}) = (0, b^N \bmod \text{N}).$$

Thus, Nth residues are of the form (0, r) and random elements of $\mathbb{Z}_N^{2*}$ have the form (r',r) with r' $\in \mathbb{Z}_N$ and with r $\in \mathbb{Z}_N^*$. The DCR assumption states that it is diificult to distinguish these two types of elements.
Suppose we encrypt a message m $\in \mathbb{Z}_N$ with respect to a public key N and choose a uniform Nth residue (0,r) and set the ciphertext equal to:

$$\text{c} \leftrightarrow (\text{m},1) \cdot (0,\text{r}) = (\text{m}+0,\ 1\cdot\text{r}) = (\text{m},\text{r})$$

We then construct another ciphertext c',

$$\text{c'} \leftrightarrow (\text{m},1) \cdot (\text{r'},\text{r}) = ([\text{m}+\text{r' mod N}],\text{r}).$$

Since a uniform Nth residue (0,r) cannot be distinguished from a uniform element (r',r), the two ciphertexts c and c' are indistinguishable and so the scheme is CPA secure.

5.2 Indistinguishability based proof

If the decisional composite residuosity problem is hard, then the Paillier encryption scheme is CPA-secure. Let π (Figure 1) denote the Paillier encryption scheme. We

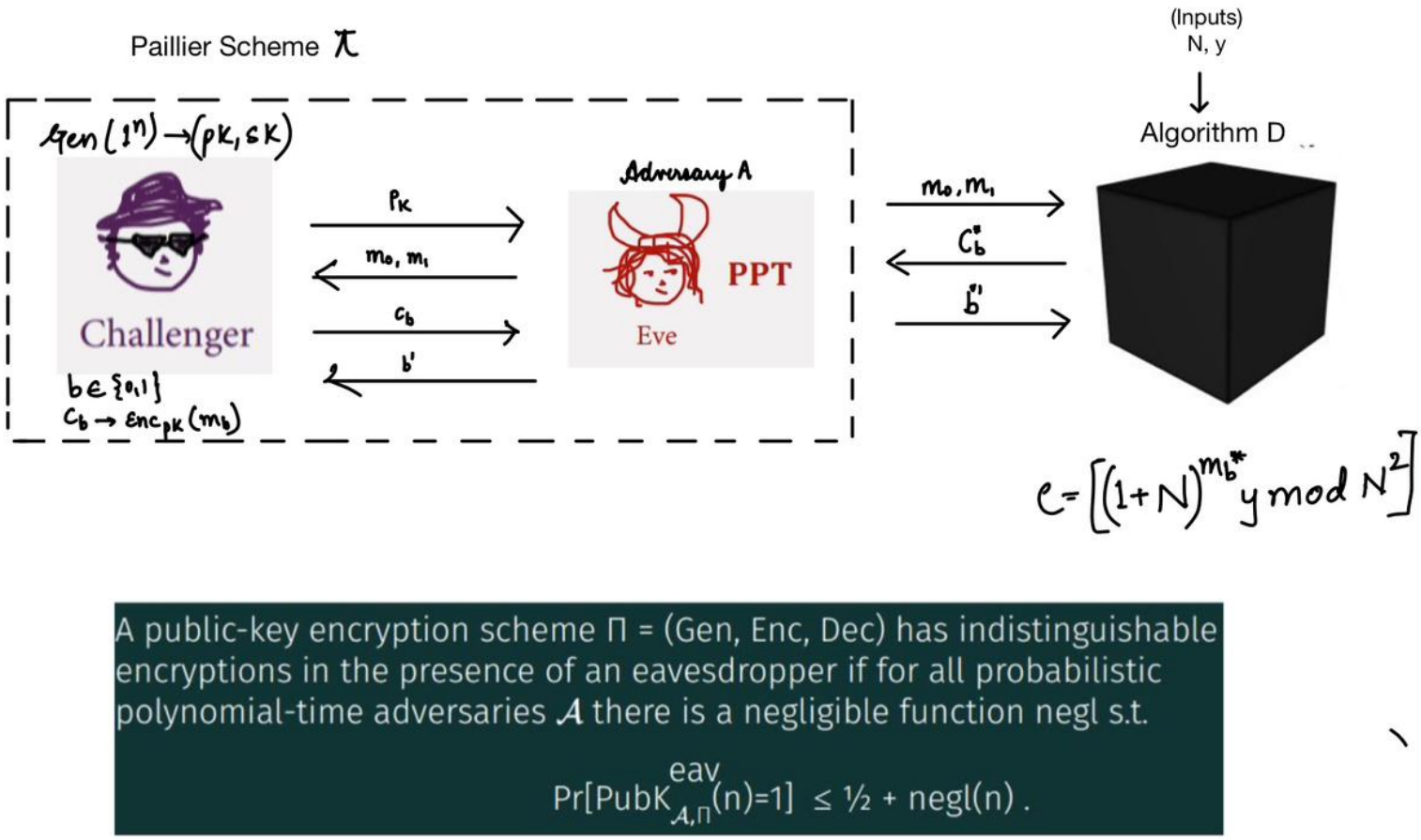

Figure 1: Computational Indistinguishability based game

prove that π has indistinguishable encryptions in the presence of an eavesdropper and thus it is CPA-secure (if a public-key encryption scheme has indistinguishable encryptions then it is CPA secure).

The eavesdropping indistinguishability experiment $\text{PubK}^{eav}_{A,\Pi(n)}$ which has a challenger and a probabilistic polynomial-time adversary A:

- Gen(1^n) is run to obtain keys (pk,sk).
- Adversary A is given pk, and outputs a pair of equal-length messages $m0, m1$ in

the message space.

- A uniform bit b ∈ {0,1} is chosen by the challenger, and then a ciphertext c ← $Enc_{pk}(m_b)$ is computed and given to A. We call c_b the challenge ciphertext.
- A outputs a bit b'. The output of the experiment is 1 if b' = b, and 0 otherwise. If b' = b we say that A succeeds.

Now let us have an PPT algorithm D that attempts to solve the decisional composite residuosity problem. The algorithm is given N,y as inputs.

- Set pk = N and run A(pk) to obtain two messages $m0, m1$.
- Choose a uniform bit b and set c = $[(1+N)^{m_b} \cdot y \bmod N^2]$
- Give the ciphertext c to A and obtain an output bit b'. If b' = b, output 1; otherwise, output 0.

Let us consider two cases here:

Case 1: Suppose the input to D was chosen to get N and some uniformly random $r \in \mathbb{Z}_N^{2*}$ and setting y = $[r^N \bmod N^2]$. Thus, the cipertext will become c = $[(1+N)^{m_b} \cdot r^N mod N^2]$. In this case the view of A when run as a subroutine by D is distributed identically to A's view in experiment $\text{PubK}^{eav}_{A,\Pi(n)}$. Since D outputs 1 exactly when the output b' of A is equal to b, we have

$$\Pr[\text{D(N,}[r^N \bmod N^2]) = 1] = \Pr[\text{PubK}^{eav}_{A,\Pi(n)}=1]$$

Case 2: Suppose the input to D was chosen to get N and some uniformly random $y \in \mathbb{Z}_N^{2*}$. Thus, the view of A in this case is independent of the bit b. Thus, the probability that b' = b in this case is exactly $\frac{1}{2}$. That is,

$$\Pr[\text{D(N,z)} = 1] = \tfrac{1}{2}$$

Combining the above we get,

$$|\ \Pr[\text{D(N,}[r^N \bmod N^2]) = 1] - \Pr[\text{D(N,z)}=1]\ | = |\ \Pr[\text{PubK}^{eav}_{A,\Pi(n)}=1] - \tfrac{1}{2}\ |$$

By the assumption that the decisional composite residuosity problem is hard, we get

$$\Pr[\text{PubK}^{eav}_{A,\Pi(n)}=1] \leq \tfrac{1}{2} + \text{negl(n)}$$

thus, proving that the Paillier Encryption scheme is IND-CPA secure.

6 Acknowledgements

We are indebted to Prof. Sruthi Sekar for giving us the opportunity to delve into this topic through this Chalk and Talk. We enjoyed the process of learning about the Paillier Encryption Scheme as well as working together on a presentation.

References

[1] Katz and Lindell, *Introduction to Modern Cryptography.*

[2] *On Homomorphic Encryption and Chosen-Ciphertext Security*
https://web.cs.ucla.edu/~rafail/PUBLIC/132.pdf

[3] *On-Line/Off-Line DCR-based Homomorphic Encryption and Applications*
https://eprint.iacr.org/2023/048.pdf

[4] *Paillier's Cryptosystem Revisited*
https://dl.acm.org/doi/pdf/10.1145/501983.502012