Paillier Cryptosystem: A Mathematical Introduction

Tobias Volkhausen

March 10, 2006

1 Introduction

Public-key cryptography has been an important research topic in recent years. The number of convincingly secure asymmetric cryptosystems is rather small.

RSA and ElGamal are representatives of two different types of asymmetric cryptosystem classes. In 1999, Pascal Paillier[2] proposed an additional, different class of asymmetric cryptosystems.

In this paper one of Paillier's encryption schemes will be illustrated. The focus will be on the mathematical details. In particular, the correctness of encryption and decryption will be proven. For security analysis, a well studied computational problem will be used.

Notation and mathematical properties, used in this paper, will be introduced in Section 2. In Section 3, the security of the encryption function is analyzed. The method of decryption and its correctness is proven in Section 4.

2 Notation and Mathematical Properties

In this section notation and mathematical properties, required for the following sections, will be addressed.

Definition 1. *Let $k \in \mathbb{Z}$ be some number. The sets $\mathbb{Z}_k$ and $\mathbb{Z}_k^*$ are defined as*

$$\mathbb{Z}_k = \{z | z \in \mathbb{Z}, 0 \leq z < n\}$$
$$\mathbb{Z}_k^* = \{z | z \in \mathbb{Z}, 0 \leq z < n, gcd(z, k) = 1\}.$$

The corresponding multiplicative group will be denoted $(\mathbb{Z}_k^*, \cdot)$, with modulo k multiplication $\cdot$.

Definition 2. *Throughout this paper $n = pq$ will be the product of two primes p and q.*

Definition 3. *A number $z \in \mathbb{Z}_{n^2}^*$ is said to be an n-th residues modulo n^2 if there exists a number $y \in \mathbb{Z}_{n^2}^*$ such that*

$$z = y^n \mod n^2$$

Let NR be the set of n-th residues modulo n^2.

Definition 4 (Problem $CR(n)$)**.** *Given $z \in \mathbb{Z}^*_{n^2}$, decide whether or not z is n-th residue modulo n^2.*

Assumption 5. *There does not exist an algorithm that solves problem $CR(n)$ in polynomial time.*

The cryptosystem and its security are based on n-th residues and their properties. The problem $CR(n)$ is a well studied mathematical problem. It is believed that it cannot be solved in polynomial time. During security analysis, in Section 3, it will be proven that breaking the encryption in polynomial time would also allow solving $CR(n)$ in polynomial time.

The following lemmata and theorems will stepwise lead to Lemma 13, which is be essential for further proofs in Section 3.

Definition 6 (Euler's Φ–Function)**.** *Let $x = \prod_i p_i^{l_i}$ with p_i pairwise different prime numbers.*
Euler's Φ–Function is defined as

$$\Phi(x) = \prod_i p_i^{l_i-1}(p_i - 1).$$

Lemma 7.

$$\Phi(x^2) = x\Phi(x)$$

Proof.

$$\begin{aligned}\Phi(x^2) &= \prod_i p_i^{2l_i-1}(p_i-1)\\ &= \prod_i p_i^{l_i} p_i^{l_i-1}(p_i-1) = (\prod_i p_i^{l_i})(\prod_i p_i^{l_i-1}(p_i-1))\\ &= x\prod_i p_i^{l_i-1}(p_i-1) = x\Phi(x)\end{aligned}$$

□

Lemma 8. *For any $x \in \mathbb{Z}_n$,*

$$(1+n)^x = 1 + xn \mod n^2. \tag{1}$$

These are roots of unity in $(\mathbb{Z}^*_{n^2}, \cdot)$.

Proof by induction over x. Basis $x = 0$ is obviously true.
Inductive step $x \to x+1$:

$$\begin{aligned}(1+n)^x &= 1 + xn \mod n^2\\ \Rightarrow (1+n)^{x+1} &= (1+xn)(1+n) \mod n^2\\ &= 1 + xn + n + xn^2 = 1 + (x+1)n \mod n^2\end{aligned}$$

These are roots of unity because

$$\begin{aligned}(1+n)^{nx} &= 1 + (nx)n \mod n^2 \qquad \text{(by Equation 1)} \\ &= 1 \mod n^2\end{aligned}$$

Note that $(n+1)^x \in \mathbb{Z}^*_{n^2}$, since $gcd(1+n, n^2) = gcd(1+n, n) = 1$. □

Lemma 9. *Let u be the number of n-th roots of unity in* $(\mathbb{Z}^*_{n^2}, \cdot)$.

$$|\mathbb{Z}^*_{n^2}| \geq |NR|u$$

Proof. For every n-th residue r, there are at least as many n-th roots as there are n-th roots of unity, because an n-th root of r multiplied with an n-th root of unity is again an n-th root of r. Therefore

$$\begin{aligned}|\mathbb{Z}^*_{n^2}| &= \sum_{x \in NR} |\{\text{n-th root modulo } n^2 \text{ of x}\}| \\ &\geq \sum_{x \in NR} u = |NR|u\end{aligned}$$

□

Lemma 10.

$$|NR| = \Phi(n)$$

Proof.

"≤" There are at least n n-th roots of unity (by Lemma 8) in $(\mathbb{Z}^*_{n^2}, \cdot)$.
This result can be used to state

$$\begin{aligned}n\Phi(n) &= \Phi(n^2) \qquad \text{(by Lemma 7)} \\ &= |\mathbb{Z}^*_{n^2}| \geq |NR|n \qquad \text{(by Lemma 9)}\end{aligned}$$

Therefore, by dividing n

$$|NR| \leq \Phi(n)$$

"≥" Consider the cyclic groups $(\mathbb{Z}^*_{p^2}, \cdot)$ and $(\mathbb{Z}^*_{q^2}, \cdot)$ with generators g_p and g_q. Examine g_p^{in} for $0 \leq i < p-1$. The numbers g_p^{in} are obviously n-th residues modulo p^2. Furthermore, the numbers g_p^{in} are pairwise different.

Proof that g_p^{in} are pairwise different.
$Assumption$: $\exists r \neq s : g_p^{rn} = g_p^{sn}$ with $0 \leq s \leq r < p-1$.

$$\begin{aligned}&\Rightarrow g_p^{(r-s)n} = 1 \mod n^2) \\ &\Rightarrow \Phi(p^2) | (r-s)n \Rightarrow p(p-1) | (r-s)pq \\ &\Rightarrow (p-1) | (r-s) \Rightarrow r - s = 0 \quad \text{(because } r - s < p-1\text{)} \\ &\Rightarrow r = s\end{aligned}$$

This contradicts $r \neq s$. □

The numbers g_q^{jn} for $0 \leq j < q-1$ have the same properties.
Hence, it can be written

$$|\{g_p^{in} | 0 \leq i < p-1\}| = p-1$$
$$|\{g_q^{jn} | 0 \leq j < q-1\}| = q-1.$$

Applying the Chinese Remainder Theorem yields

$$|NR| \geq (p-1)(q-1) = \Phi(n).$$

□

Lemma 11. *There are exactly n n-th roots of unity in $(\mathbb{Z}_{n^2}^*, \cdot)$.*

Proof. There are at least n n-th roots of unity (by Lemma 8).
Next, it is poven that there are at most n n-th roots of unity in $(\mathbb{Z}_{n^2}^*, \cdot)$.
$Assumption$: There are $> n$ n-th roots of unity in $(\mathbb{Z}_{n^2}^*, \cdot)$.
Let u be the number of n-th roots of unity in $(\mathbb{Z}_{n^2}^*, \cdot)$.

$$\begin{aligned}\Phi(n^2) = |\mathbb{Z}_{n^2}^*| &\geq |NR|u \quad \text{(by Lemma 9)} \\ &> |NR|n = \Phi(n)n = \Phi(n^2)\end{aligned}$$

This is a contradiction. □

Corollary 12. *There exists exactly one n-th root of unity in $(\mathbb{Z}_{n^2}^*, \cdot)$ strictly smaller than n, namely 1.*

Proof. Lemma 11 states that there are exactly n n-th roots of unity by $\mathbb{Z}_{n^2}^*$. These n n-th roots of unity are explicitly given by Lemma 8. Only one of those roots is strictly smaller than n, namely 1. □

Lemma 13. *The function*

$$\begin{aligned} f : \mathbb{Z}_n^* &\longrightarrow NR \\ x &\longmapsto x^n \mod n^2 \end{aligned}$$

is a bijection.

Proof. Lemma 10 states $|NR| = \Phi(n)$. Furthermore $|\mathbb{Z}_n^*| = \Phi(n)$ and therefore $|NR| = |Z_n^*|$, which means it is sufficient to show that f is injective.
By Corollary 12, in $(\mathbb{Z}_{n^2}^*, \cdot)$ there is exactly one root of unity smaller than n, namely 1.
This means $kernel(f) = \{1\}$, which is equivalent to f being injective.

□

3 Encryption

An encryption function has to fulfill three requirements. It has to be a bijection, which is hard to invert and efficiently to evaluate in polynomial time. The given function can obviously be evaluated in polynomial time. The other properties will be proven in this section.

3.1 The Encryption Function is a Bijection

One property, needed for the actual proof, will be examined first. This property is a special case of Carmichael's Theorem.

Lemma 14. *Set $\lambda = lcm(p-1, q-1)$. Consider the group $(\mathbb{Z}^*_{n^2}, \cdot)$. For any $x \in \mathbb{Z}^*_{n^2}$,*

$$x^{n\lambda} = 1 \mod n^2.$$

Proof. This is a direct consequence of the Chinese Remainder Theorem. The orders of $Z^*_{p^2}$ and $Z^*_{q^2}$ are given by

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

For any $x \in \mathbb{Z}^*_{n^2}$,

$$x^{n\lambda} = x^{p*q*lcm(p-1,q-1)} = 1 \mod p^2$$
$$x^{n\lambda} = 1 \mod q^2.$$

Use of the Chinese Remainder Theorem results in

$$x^{n\lambda} = 1 \mod p^2q^2 (= n^2).$$

□

Definition 15 (Encryption function E_g)**.**
Let $\mathcal{B} = \{u \in \mathbb{Z}^*_{n^2} \mid ord(u) = kn, k \in \{1, \ldots, \lambda\}\}$ and $g \in \mathcal{B}$. The encryption function is defined as

$$E_g : \mathbb{Z}_n \times \mathbb{Z}^*_n \longrightarrow \mathbb{Z}^*_{n^2}$$
$$(m, r) \longmapsto g^m r^n \mod n^2.$$

Theorem 16. *The encryption function E_g is bijective.*

Proof.

$$\begin{aligned} |\mathbb{Z}_n \times \mathbb{Z}^*_n| &= n\Phi(n) \\ &= \Phi(n^2) \qquad \text{(by Lemma 7)} \\ &= |\mathbb{Z}^*_{n^2}| \end{aligned}$$

Therefore it is sufficient to show that E_g is injective.
Choose some $(m_1, r_1), (m_2, r_2) \in \mathbb{Z}_n \times \mathbb{Z}^*_n$ with $E_g(m_1, r_1) = E_g(m_2, r_2)$.

$$\begin{aligned} g^{m_1} r_1^n = E_g(m_1, r_1) = E_g(m_2, r_2) = g^{m_2} r_2^n \mod n^2 \\ \Rightarrow g^{m_1 - m_2} r_1^n = r_2^n \mod n^2 \\ \Rightarrow g^{(m_1-m_2)\lambda} r_2^{n\lambda} = r_1^{n\lambda} \mod n^2 \\ \Rightarrow g^{\lambda(m_1-m_2)} = 1 \mod n^2 \qquad \text{(by Lemma 14)} \end{aligned}$$

- This means $ord(g)|\lambda(m_1 - m_2)$ and therefore $n|\lambda(m_1 - m_2)$, by choice of g.
- Furthermore $n|(m_2 - m_1)$, since $gcd(\lambda, n) = 1$. This can be rewritten as

$$\begin{aligned} m_1 - m_2 &= 0 \mod n \\ \Rightarrow m_1 &= m_2 \mod n \\ \Rightarrow m_1 &= m_2. \end{aligned}$$

- Substituting this into the previous equation yields

$$r_1^n = r_2^n \mod n^2.$$

The bijection f, of Lemma 13, is used to rewrite this equation.

$$\begin{aligned} &f(r_1) = f(r_2) \\ &\Rightarrow r_1 = r_2 \qquad (f \text{ is injective}) \end{aligned}$$

□

3.2 Security of E_g

Security will be proven by reduction and will be based on Assumption 5. First, some short notation, and related properties of n-th residues modulo n^2, will be introduced.

Definition 17. *For any $g \in \mathcal{B}$, define function $[.]_g$ as*

$$\begin{aligned} [.]_g : \mathbb{Z}_{n^2}^* &\longrightarrow \mathbb{Z}_n \\ c &\longmapsto E_g^{-1}(c)[1]. \end{aligned}$$

Where $E_g^{-1}(c)[1]$ means the first component of $E_g^{-1}(c)$.

Lemma 18. *Let $g \in \mathcal{B}$.*

$$c \in NR \Longleftrightarrow [c]_g = 0$$

Proof.

"⇒" Let $c \in NR$.
By Lemma 13, there exists a number $r \in \mathbb{Z}_n^*$, such that

$$c = r^n \mod n^2.$$

This means, that for any $g \in \mathcal{B}$

$$c = r^n = E_g(0, r) \mod n^2.$$

Moreover, this can be rewritten as

$$[c]_g = E_g^{-1}(c)[1] = 0.$$

"⇐" Let $c \in \mathbb{Z}_{n^2}^*$ with $[c]_g = 0$.
For appropriate $r \in \mathbb{Z}_n^*$ it can be written

$$\begin{aligned} E_g^{-1}(c) &= (0, r) \\ \Rightarrow c &= r^n \mod n^2. \end{aligned}$$

Hence $c \in NR$.

□

Lemma 19. *For any $c \in \mathbb{Z}_{n^2}^*$ and $g_1, g_2 \in \mathcal{B}$,*

$$\begin{aligned} [c]_{g_1} &= [c]_{g_2}[g_2]_{g_1} \mod n \\ [c]_{g_2} &= [c]_{g_1}[g_2]_{g_1}^{-1} \mod n. \end{aligned}$$

Proof. Any number $c \in \mathbb{Z}_{n^2}^*$ can be written in two different ways. On the one hand

$$\left.\begin{aligned} c &= g_2^{[c]_{g_2}} r_2^n \mod n^2 \\ g_2 &= g_1^{[g_2]_{g_1}} r_3^n \mod n^2 \end{aligned}\right\} \Rightarrow c = (g_1^{[g_2]_{g_1}} r_3^n)^{[c]_{g_2}} r_2^n \mod n^2$$

$$\Rightarrow c = g_1^{[c]_{g_2}[g_2]_{g_1}} (r_2 r_3^{[c]_{g_2}})^n = E_{g_1}([c]_{g_2}[g_2]_{g_1}, r_2 r_3^{[c]_{g_2}}) \mod n^2.$$

On the other hand

$$c = E_{g_1}([c]_{g_1}, r_1).$$

Joining these equation by c yields

$$\begin{aligned} E_{g_1}([c]_{g_1}, r_1) &= E_{g_1}([c]_{g_2}[g_2]_{g_1}, r_2 r_3^{[c]_{g_2}}) \\ \Rightarrow [c]_{g_1} &= [c]_{g_2}[g_2]_{g_1} \mod n \qquad (E_g \text{ is injective}). \end{aligned} \tag{2}$$

With similar arguments, it can be deduced

$$[c]_{g_2} = [c]_{g_1}[g_1]_{g_2} \mod n. \tag{3}$$

Substituting Equation 3 into Equation 2 results in

$$\begin{aligned} [c]_{g_1} &= ([c]_{g_1}[g_1]_{g_2})[g_2]_{g_1} \mod n \\ \Rightarrow 1 &= [g_1]_{g_2}[g_2]_{g_1} \mod n. \end{aligned}$$

This means that $[g_2]_{g_1}$ is invertible and Equation 2 can be rewritten to

$$[c]_{g_2} = [c]_{g_1}[g_2]_{g_1}^{-1} \mod n.$$

□

Encryption Process

- private parameter: p, q prime
- public parameter: $n = pq$, $g \in \mathcal{B}$
- Steps to encrypt plaintext $m \in \mathbb{Z}_n$ into ciphertext $c \in \mathbb{Z}_{n^2}^*$:
  1. Choose $r \in_R \mathbb{Z}_n^*$.
  2. Compute $c = E_g(m, r) = g^m r^n \mod n^2$.

The problem $Class(n, g)$ is defined to analyze the security of the encryption process. The problem describes a situation, in which an adversary tries to decode a cipher text without knowledge of the private key.

Definition 20 (Problem $Class(n, g)$)**.** *Given ciphertext $c \in \mathbb{Z}_{n^2}^*$, compute $[c]_g$.*

It will be shown that the complexity of $Class(n, g)$ does not depend on parameter g.

Theorem 21.

$$\forall g_1, g_2 \in \mathcal{B}: \quad Class(n, g_1) \equiv Class(n, g_2)$$

Proof. A direct consequence of Lemma 19. □

Definition 22 (Problem $Class(n)$)**.** *Given $c \in \mathbb{Z}_{n^2}$ and $g \in \mathcal{B}$, compute $[c]_g$.*

Definition 23 (Problem D–$Class(n)$)**.** *Given $c \in \mathbb{Z}_{n^2}$, $g \in \mathcal{B}$ and $m \in \mathbb{Z}_n$. Decide whether $[c]_g = m$.*

For further security analysis, the problem $Class(n)$ is defined. Motivated by Theorem 21, problem $Class(n)$ describes the same situation as $Class(n, g)$, but does no longer depend on g. The actual reduction will use the problem D–$Class(n)$, the decisional form of problem $Class(n)$.

Theorem 24.

$$CR(n) \leq D\text{–}Class(n)$$

Proof. Let A be an algorithm that solves the problem D–$Class(n)$ in polynomial time. The following algorithm will use A and solve $CR(n)$ in polynomial time.

- Input: $c \in \mathbb{Z}_{n^2}^*$
- Set $g \in \mathcal{B}$.
  (one possible choice could be $n + 1$, since $ord(n + 1) = n$ by Lemma 8 and therefore $n + 1 \in \mathcal{B}$).
- Set $m = 0$.
- Output: The answer given by A, started with input (c, g, m).

Correctness Parameters c, g, m are chosen such that A answers the question $[c]_g = 0$? This in turn is equivalent to the question whether or not $c \in NR$ (by Lemma 18). □

Corollary 25.

$$CR(n) \leq Class(n)$$

Proof. The ability to solve the computational problem always directly solves the decisional problem. Therefore

$$D\text{–}Class(n) \leq Class(n).$$

Applying Theorem 24 results in

$$CR(n) \leq D\text{–}Class(n) \leq Class(n).$$

□

4 Decryption

In this section, the decryption process will be phrased and its correctness shown. At first, a function for short notation is defined and some of its properties illustrated.

Definition 26. *Let S_n be the set*

$$\mathcal{S}_n = \{u < n^2 \mid u = 1 \mod n\}.$$

Define function $L(u)$ for $u \in \mathcal{S}_n$:

$$L(u) = \frac{u-1}{n}$$

Lemma 27. *For any $w \in \mathbb{Z}^*_{n^2}$,*

$$L(w^\lambda \mod n^2) = \lambda[w]_{n+1} \mod n.$$

Proof. The order of $n+1$ in $(\mathbb{Z}^*_{n^2}, \cdot)$ is n, by Lemma 8. Therefore $n+1 \in \mathcal{B}$.
The number $w \in \mathbb{Z}^*_{n^2}$ can be written as

$$\begin{aligned} w &= E_{n+1}([w]_{n+1}, y) \qquad (y \in \mathbb{Z}^*_n \text{ appropriately}) \\ &= (n+1)^{[w]_{n+1}} y^n \mod n^2 \\ \Rightarrow w^\lambda &= (n+1)^{\lambda[w]_{n+1}} y^{n\lambda} \mod n^2 \\ &= (n+1)^{\lambda[w]_{n+1}} \mod n^2 \\ &= 1 + \lambda[w]_{n+1} n \mod n^2 \qquad \text{(by Lemma 8)} \end{aligned}$$

Applying function L yields

$$L(w^\lambda \mod n^2) = \lambda[w]_{n+1} \mod n.$$

□

Decryption process

- private key: p, q prime
- public key: $n = pq$, $g \in \mathcal{B}$
- Steps to decrypt ciphertext $c \in \mathbb{Z}_{n^2}^*$ into plaintext $m \in \mathbb{Z}_n$:

  1. Compute $m = \frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n$.

Correctness of decryption will be shown. Given a ciphertext $c \in \mathbb{Z}_{n^2}^*$ for plain text $m \in \mathbb{Z}_n$. The following is computed for decryption of c

$$\begin{aligned}\frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} &= \frac{\lambda[c]_{n+1}}{\lambda[g]_{n+1}} \mod n \quad \text{(by Lemma 27)} \\ &= \frac{[c]_{n+1}}{[g]_{n+1}} \mod n \\ &= [c]_g = m \mod n \quad \text{(by Lemma 19)}\end{aligned}$$

5 Conclusion

The cryptosystem proposed by Pascal Paillier introduces a new class of public-key cryptosystems. The illustrated encryption scheme was proven to be secure under appropriate assumptions. A decryption method was stated and proven to be correct.

The encryption scheme can be examined further with regards to encryption/decryption efficiency and setup costs. It is then possible to improve efficiency by manipulating parameters in the encryption process[1].

References

[1] A. Kumlehn. Paillier Kryptosystem: Analyse und Verbesserungen. *Seminar Public-Key Kryptographie (WS 05/06) bei Prof. Dr. J. Blömer*, 2006.

[2] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Eurocrypt 99, LNCS 1592*, pages 223–238, 1999.