Chapter 3

Paillier's Cryptosystem

In this chapter we describe the public key cryptosystem presented by Paillier at Eurocrypt99 [47]. This cryptosystem constitutes the starting point for the results that are going to be presented in the next chapters and, consequently, we provide here a complete description of it.

3.1 Introduction

Despite the huge amount of research that has been carried so far in cryptography, very few convincing trapdoor mechanisms have been proposed. Many encryption schemes have been presented, but they are all, more or less, variants of very few basic ideas. In principle it is possible to distinguish two main types of cryptosystems: the ones based on RSA (or related assumptions) and those based on discrete log (or related assumptions).

Of course some different solutions have been proposed, but either they suffer from inefficiency, or security flaws. To this "class" belong almost all lattice based cryptosystems (for example [1], subsequently broken by [44]) and the knapsack-type schemes (for example [16], later broken by [57]).

Another promising direction is the one of cryptography based on the theory of *braid groups* [37], but, again, this is a too insufficiently studied area to be completely reliable.

At the very end all the "trusted" schemes are RSA or Discrete log based schemes.

In a nutshell the main difference between the two approaches can be described as follows. The schemes based on RSA related assumptions take advantage of the fact that RSA is a (conjectured) trapdoor function. The underlying idea is then to conjugate the feasibility of extracting roots of polynomials over finite fields when the trapdoor information is available with the intractability of the same problem when such an information is not available. The discrete log, on the other hand, is conjectured to be just a one-way function, and the underlying idea of the schemes that rely on such assumption is, in general, to use Diffie-Hellman variants to securely encrypt and decrypt. A positive side of discrete log related schemes is that they can, in general, take advantage of the homomorphic property of the exponentiation function. This is a very useful property especially in contexts like electronic voting, e-commerce and distributed cryptography in general.

An interesting question is if it is possible to conjugate the two approaches in order to get the positive aspects of both. In this sense what would be really appreciated is a trapdoor mechanism that is based on an homomorphic function as well.

In recent years a new direction of research started to give a positive answer to the above question. The developed methods, known as trapdoor discrete log, arise from the algebraic setting of high degree residuosity classes. In such schemes, the message space is a ring $\mathcal{M}$ of modular residues and ciphertexts are in the group $\mathcal{G}$ (denoted multiplicatively) of invertible elements of some particular ring of integers modulo a number hard to factor. The encryption of a message m is always a group element of the form $E(m,r) = g^m r^e \in \mathcal{G}$ where e is some public integer, g some fixed public element in $\mathcal{G}$, and r is chosen at random in some particular multiplicative subgroup $\mathcal{R}$ of $\mathcal{G}$. Since $\mathcal{R}$ is a subgroup, such schemes have the additive homomorphic property: an encryption of $m_1 + m_2$ can be obtained from any encryption of m_1 and m_2, as $E(m_1, r_1)E(m_2, r_2) \equiv E(m_1 + m_2, r_1 r_2)$.

This idea was proposed for the first time by Golwasser and Micali [30] when they introduced the notion of probabilistic encryption. The Goldwasser-Micali scheme [30] is based on quadratic residues: it selects $\mathcal{M} = \mathbb{Z}_2$, $\mathcal{G} = \mathcal{R} = \mathbb{Z}_N^*$ where $N = pq$ is an RSA-type modulus, $e = 2$ and the base g as a pseudo-square modulo N. The semantic security follows from

the *quadratic residuosity assumption* [1]. The Benaloh-Fischer scheme [3, 17] later improved the very limited bandwidth of the Goldwasser-Micali scheme by using higher-order residues: it uses the same groups $\mathcal{G} = \mathcal{R} = \mathbb{Z}_N^*$ where $N = pq$ is a product of two large primes, but this time, $\mathcal{M} = \mathbb{Z}_e$, e is a small prime number dividing $\phi(N)$ such that e^2 does not divide $\phi(N)$, and g is a non e-th residue modulo N. The semantic security is proved under the *prime residuosity assumption*. However, the decryption is inefficient as it applies some kind of exhaustive search, implying that e must be very small. In 1998, Naccache and Stern [42] proposed a variant of the Benaloh-Fischer scheme which allows high bandwidth. This is achieved by taking e not as a prime but as a product of small primes $e_1, \ldots, e_p$ such that $\phi(N)$ is divisible by e but by none of the e_i^2's, and g is non e_i-th residue modulo N, for all i. The

[1] A number $x \in Z_N^*$ is said to be a *quadratic residue* modulo N if there exists another element $y \in Z_N^*$ such that $x = y^2 \bmod N$.

Now let X be the subgroup of Z_N^* of elements having Jacobi symbol equal to 1 (see [39] for a definition of Jacobi symbol). It is possible to prove that every quadratic residue in Z_N^* is in X. The *Quadratic Residuosity Assumption* states that, given N (without its factorization), it is computationally infeasible to distinguish quadratic residues (in Z_N^*) from random elements in X.

The above can be generalized as follows.

Let p be an integer such that $p|ord(Z_N^*)$. We say that $x \in Z_N^*$ is a *p-residue* if there exists another element $y \in Z_N^*$ such that $x = y^p \bmod N$. The *p-residuosity Assumption* states that, given N without its factorization, it is computationally infeasible to distinguish random elements from p-residues.

semantic security is still proved under the *prime residuosity assumption*.

At the same time, Okamoto and Uchiyama [46] proposed a very different improvement of the Benaloh-Fischer scheme by changing of group structure. They selected $\mathcal{G} = \mathcal{R} = \mathbb{Z}_N^*$ with $N = p^2q$ instead of $N = pq$ as in Goldwasser-Micali, Benaloh-Fischer and Naccache-Stern. And they use $\mathcal{M} = \mathbb{Z}_p$, $e = N$ and g such that the order of g^p modulo p^2 is p. If the scheme is not one-way, one can factor N. The semantic security is proved under the *p-subgroup assumption* [2], but there exist very simple chosen-ciphertext attacks that can recover the factorization of N. The scheme reaches bandwidths similar to Naccache-Stern, however the decryption is more efficient.

Paillier recently proposed in [47] an extension of the Okamoto-Uchiyama scheme where N is an usual RSA-modulus and working in a different group. More precisely, $N = pq$, $\mathcal{M} = \mathbb{Z}_N$, $\mathcal{G} = \mathbb{Z}_{N^2}^*$, $\mathcal{R} = \mathbb{Z}_N^*$, $e = N$ and g is an element of order divisible by N. The semantic security is proved under the *decisional composite residuosity assumption*: Given $N = pq$, it is hard to decide whether an element in $\mathbb{Z}_{N^2}^*$ is an N-th power of an element in $\mathbb{Z}_{N^2}^*$. The resulting system is more efficient than the previously mentioned schemes. Besides, no adaptive chosen-ciphertext attacks recovering the secret key is known. For those reasons, Paillier's cryptosystem is currently the best

[2]The *p-subgroup assumption* informally states that given $N = p^2q$, without its factorization, it is infeasible to decide if a radom element $z \in Z_N^*$ has order $p-1$ in $Z_{p^2}^*$ or not.

candidate of a cryptosystem with additive homomorphy.

The rest of the chapter is organized as follows. First we will go through all the mathematics underlying the new scheme and then we will introduce the scheme itself.

3.2 Mathematical preliminaries

In this section we introduce some definitions and we discuss some useful facts from number theory.

Let $N = pq$ where p and q are large primes. ¿From basic number theory we know the following facts.

1. $\phi(N) = (p-1)(q-1) = |Z_N^*|$
2. $\lambda(N) = lcm(p-1, q-1)$
3. $|Z_{N^2}^*| = \phi(N^2) = N\phi(N)$
4. $\forall x \in Z_{N^2}^*$ the following relations are true

$$\begin{cases} x^{\lambda(N)} \equiv 1 \bmod N \\ x^{N\lambda(N)} \equiv 1 \bmod N^2 \end{cases}$$

Definition 9 *An element $x \in Z_{N^2}^*$ is said to be an N^{th} residue if there exists another element $y \in Z_{N^2}^*$ such that*

$$y = x^N \bmod N^2$$

Theorem 2 *Every N^{th} residue has exactly N different N^{th} roots in $Z^*_{N^2}$.*

Proof It is a well known fact from number theory [39, 59] that in every finite cyclic group G, the equation $x^d = a$ has $gcd(d, ord(G))$ different solutions. This fact, however, cannot be immediately applied to $Z^*_{N^2}$ because it is not a cyclic group, but can be applied to the cyclic groups $Z^*_{q^2}$ and $Z^*_{p^2}$ having order, respectively, $\phi(q^2) = q(q-1)$ and $\phi(p^2) = p(p-1)$ (see [39] for details).

So from the equation $y = x^N \bmod N^2$, consider the equations

$$y = x^N \bmod p^2 \tag{3.2.1}$$

and

$$y = x^N \bmod q^2 \tag{3.2.2}$$

Equation 3.2.1 has then $gcd(N, p(p-1)) = p$ different solutions and equation 3.2.2 has $gcd(N, q(q-1)) = q$ different solutions. Using the Chinese Remainder Theorem [39], these can be combined to yield $pq = N$ different solutions modulo N^2. ■

Since N divides the order of $Z^*_{N^2}$ it follows that the set of N^{th} residues is a subgroup of $Z^*_{N^2}$. Moreover it is possible to prove that this subgroup has cardinality $\phi(N)$.

For now, however, let us investigate the rich mathematical structure of the group $Z^*_{N^2}$, by considering another, extremely interesting, subgroup.

Theorem 3 *The set*

$$T = \{(1 + xN) \bmod N^2 \ : \ x \in Z_N^*\}$$

is a subgroup of $Z_{N^2}^*$ of cardinality $\phi(N)$. Moreover every element in T has order N.

Proof Since T and Z_N^* have the same cardinality, $|T| = \phi(N)$. Moreover it is easy to check that T is a multiplicative group. Note that for every element in $(1 + yN) \in T$ the following relation is satisfied

$$(1 + yN)^z \bmod N^2 = (1 + yzN) \bmod N^2$$

This immediately implies that $\forall (1 + yN) \in T \ (1 + yN)^N = 1 \bmod N^2$, and then the order of all the elements in T has to be a divisor of N. However the only possible divisors of N (apart from N itself) are the two primes p and q and since for every $(1 + yN) \in T$, $gcd(y, N) = 1$, the only possibility for the equation

$$(1 + yN)^z = 1 \bmod N^2$$

to be satisfied is for $z = N$. This completes the proof. ■

Remark 1 *Observe that if we consider the set*

$$T' = \{(1 + xN) \bmod N^2 \ : \ x \in Z_N\}$$

T' has cardinality N and for all $x \in T'$, $x^N = 1 \bmod N^2$

As an immediate consequence of the previous theorems (combined with the previous remark) we have that if y is an N^{th} residue of the form

$$y = w^N \bmod N^2 \tag{3.2.3}$$

there are N distinct elements of the form

$$(1+N)^x w = (1+xN)w \bmod N^2 \;\; x \in Z_N$$

that are N^{th} roots of y.

Note also that if $w = 1$ in 3.2.3 then $y = 1$. Consequently the N^{th} roots of unity are all the elements in $Z^*_{N^2}$ of the form

$$(1+N)^x = (1+xN) \bmod N^2$$

Now we are ready to prove the following theorem

Theorem 4 *Let y be an N^{th} residue modulo N^2 and $w \in Z^*_{N^2}$ such that $w^N = y \bmod N^2$. Consider the following set*

$$R = \{(1+xN)w \bmod N^2,\ x \in Z_N\}$$

then there exists only one element in R that is smaller than N.

Proof First notice that if $w \in Z^*_{N^2}$ then $w \bmod N \in Z^*_N$. Then assume w.l.o.g. that $w = a + bN$, $a \neq 0$. The elements of R can be written as

$$(a+bN)(1+xN) = a + (ax+b)N \bmod N^2$$

Now let us fix x. Since $w \bmod N = a$ is an invertible element of Z_N we can put

$$x = -(a^{-1})b \bmod N \tag{3.2.4}$$

and, for this position, we obtain

$$a + (ax + b)N \bmod N^2 = a + (-a^{-1}ab + b) \bmod N^2 = a \bmod N^2$$

The uniqueness comes from the fact that equation 3.2.4 has an unique solution. ■

Consider now the following problem. Given a random element $w \in Z^*_{N^2}$, decide if w is an N^{th} residue or not. We denote this problem with $CR[N]$.

How hard (or easy) is this problem?

It is possible to prove (and we will do it shortly) that knowing the factorization of N is a sufficient condition for solving it in probabilistic polynomial time. However it is not known if the factorization of the modulus is necessary to decide N^{th} residuosity as well. Moreover, if the factorization is not known, no polynomial strategy to solve the problem has, so far, been discovered. This leads to the following (informal) conjecture

Assumption 5 *If N is a modulus of unknown factorization, there exists no probabilistic polynomial time algorithm for the problem $CR[N]$.*

According to Paillier's [47] notation we will refer to this assumption as the *Decisional Composite Residuosity Assumption* (DCRA)

3.3 Computing Composite Residuosity

Now we pass to describing the computational composite residuosity classes that constitute the basic building blocks for Paillier's scheme.

Let $g \in Z^*_{N^2}$ and consider the function

$$\mathcal{E}_g : Z_N \times Z^*_N \to Z^*_{N^2}$$

defined as follows

$$\mathcal{E}_g = g^x y^N \bmod N^2 \tag{3.3.5}$$

It is possible to prove the following

Lemma 1 *If the order of g is a non zero multiple of N then $\mathcal{E}_g$, defined as above, is a bijection.*

Proof Since the sets $Z_N \times Z^*_N$ and $Z^*_{N^2}$ have the same cardinality we just need to prove that $\mathcal{E}_g$ is injective.

Assume we have

$$g^x y^N \equiv g^{x'} y'^N \bmod N^2 \tag{3.3.6}$$

If we raise to the power $\lambda(N)$ the both sides of the above equation we get

$$g^{\lambda(N)x} \equiv g^{x'\lambda(N)} \bmod N^2$$

Note that since g has order multiple of N and $\gcd(N, \lambda(N)) = 1$, $g^{\lambda(N)}$ has order N. Consequently we can write it as $(1 + zN)$ for some $z \in Z_N, z \neq 0$.

The previous relation becomes

$$(1 + zN)^x \equiv (1 + zN)^{x'} \bmod N^2$$

This immediately implies $x \equiv x' \bmod N$. Thus, back to equation 3.3.6, we can write it as

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

$$(\frac{y}{y'})^N \equiv 1 \bmod N^2$$

By Theorem 4 this is satisfied for $y \equiv y' \bmod N$. ■

We will denote with $\mathcal{B}_\alpha$ the subgroup of $Z^*_{N^2}$ whose elements have order αN $(\alpha \neq 0)$, and with $\mathcal{B}$ the disjoint union of $\mathcal{B}_\alpha$, $(\alpha = 1, \ldots, N,\ \alpha|\lambda(N))$.

Definition 10 *Let $g \in \mathcal{B}$. Given $w \in Z^*_{N^2}$ we call the N^{th} residuosity class of w, with respect to g, the unique $x \in Z_N$ for which there is $y \in Z^*_N$ such that $\mathcal{E}_g(x, y) = w$*

Using a notation that is similar to that adopted by Benaloh [3], we denote with $[w]_g$ the class of w with respect to the base g.

Given a base g and a random element $w \in Z^*_{N^2}$, the N^{th} *Residuosity Class problem* is defined as the problem of computing the class to which w belongs with respect to the base g. We denote this problem as $Class[N, g]$. With the following theorem we will provide some useful properties of the function $Class$.

Theorem 5 *Let g be an element in $\mathcal{B}$. The following properties are satisfied.*

1. *For every $w \in Z^*_{N^2}$, $[w]_g = 0$ if and only if w is an N^{th} residue modulo N^2.*

2. *For every $w \in Z^*_{N^2}$, the function that associates to w its corresponding class $[w]_g$ is an homomorphism from $(Z^*_{N^2}, \times)$ to $(Z_N, +)$.*

   Formally $\forall w_1, w_2 \in Z^*_{N^2}$

$$[w_1 w_2]_g = [w_1]_g + [w_2]_g \bmod N$$

Proof

1. If $[w]_g = 0$ then w can be written as $w = g^0 y^N \bmod N^2$ and then it is an N^{th} residue modulo N^2. Conversely, if w is an N^{th} residue modulo N^2 it will be of the form $w = y^N \bmod N^2$. If y is less than N we are done, because, being $\mathcal{E}_g$ a permutation, this implies $[w]_g = 0$. On the other hand if $y > N$, it can be written as $y = a + bN$ with $a \in Z_N$ and consequently $w = y^N \bmod N^2 = (a+bN)^N \bmod N^2 = a^N \bmod N^2$ and we can reduce to the previous case.

2. Given $w_1 = g^x y^N \bmod N^2$ and $w_2 = g^a b^N \bmod N^2$, we have $w_1 w_2 = g^{a+x}(yb)^N \bmod N^2$. Since $a, x < N$, $a + x < 2N$. In particular $a + x$ can be written as $(a + x \bmod N) + cN$, where c can be either 0 or 1, (depending on if $a + x < N$ or not). By this position we have

$$w_1 w_2 = g^{a+x}(yb)^N \bmod N^2 = g^{a+x \bmod N}(ybg^c)^N \bmod N^2$$

This implies that $[w_1 w_2]_g = [g^{a+x}(yb)^N]_g = a+x \bmod N$ and, of course, $[w_1]_g + [w_2]_g = a + x \bmod N$.

■

With the next theorem we prove that the function $Class$ is *random self reducible* [5] over $w \in Z^*_{N^2}$. Informally random self reducibility guarantees that, if a significant fraction (a polynomial fraction) of the instances of a given problem (even if we don't know which ones) can be efficiently answered correctly, then every individual instance can be (efficiently) answered correctly (with the same probability).

Theorem 6 *$Class[N, g]$ is random self reducible [5] over $w \in Z^*_{N^2}$.*

Proof Assume we have an algorithm CC that computes the function $Class[N, g]$ (for a fixed g) for a polynomial fraction of its inputs. Given an arbitrary value $w = g^a b^N \bmod N^2$, we have to prove that we can use the algorithm CC to compute $Class[N, g](w)$ with non negligible probability. Let $q(n)$ be a polynomial ($n = |N|$) and assume that

$$Pr[CC(N, g, y) = Class[N, g](y) \ : \ y \leftarrow Z^*_{N^2}] = \frac{1}{q(n)}$$

First note that the element w can be easily transformed into a random element $w' \in Z^*_{N^2}$ as follows.

Choose uniformly and at random two elements $r \in Z_N$ and $s \in Z^*_N$ and set $z = g^r s^N \bmod N^2$. Such z is random and uniformly distributed and then

also $w' = wz \bmod N^2$ is random and uniformly distributed. Consequently CC can compute the class of w' with probability $\frac{1}{q(n)}$. Note that once the class of w' is known it is easy to compute the class of w since we know r. ■

Theorem 7 *$Class[N, g]$ is self reducible over $g \in \mathcal{B}$.*

Proof Assume to have an oracle to compute $Class[N, g_1]$ for some fixed $g_1 \in \mathcal{B}$ and we want to prove this is sufficient to compute $Class[N, g_2]$ for any other $g_2 \in \mathcal{B}$. To do this consider an element $w \in Z^*_{N^2}$. We want to compute $[w]_{g_2}$. Using the oracle we have access to we can compute $[w]_{g_1}$ and $[g_2]_{g_1}$. Let us write

$$w = g_1^a b^N \bmod N^2$$

$$g_2 = g_1^c d^N \bmod N^2$$

(Notice that we do not know b and d). Moreover w can be written, relatively to the base g_2 as

$$w = g_2^x y^N \bmod N^2$$

for some $x \in Z_N$ and $y \in Z^*_N$, even though we do not know how to compute such an x yet. However, using the fact that we can compute the class of g_2, we have that

$$w = g_2^x y^N = g_1^{cx} (d^x y)^N \bmod N^2$$

and then

$$[w]_{g_1} = [w]_{g_2} [g_2]_{g_1} \bmod N$$

If we put $w = g_1$ in the above relation we get

$$[g_1]_{g_2}[g_2]_{g_1} = 1 \bmod N$$

and then $[g_2]_{g_1}$ is invertible. Finally we can write

$$[w]_{g_2} = [w]_{g_1}[g_2]_{g_1}^{-1} \bmod N$$

■

Note that the above theorem, tells us that if we have on oracle to compute the function $Class$ with respect to a specific base g, we can use the same oracle to compute the function with respect to every base. In this sense we can look at the problem of computing class as a computational problem whose difficulty solely depends on N. More precisely

Definition 11 *Given $w \in Z_{N^2}^*$ and $g \in \mathcal{B}$, we define the Composite Residuosity Class Problem the problem to compute $[w]_g$. We call this problem $Class[N]$.*

Once having presented the properties of the function $Class$ we move to studying its computational complexity.

Consider the following set

$$S_N = \{u < N^2 \mid u \equiv 1 \bmod N\}$$

It is easy to see that S_N is a subgroup of $Z_{N^2}^*$.

We can define on it the following function (having integer values)

$$L(u) = \frac{u-1}{N} \quad \forall u \in S_N$$

Note that L is well defined, since every $u \in S_N$ is such that $u-1 \equiv 0 \bmod N$.

We prove the following result

Lemma 2 $\forall w \in Z^*_{N^2}$, $L(w^{\lambda(N)} \bmod N^2) = \lambda(N)[w]_{1+N} \bmod N$.

Proof Being $(1+N) \in \mathcal{B}$, there exist a and b such that

$$w = (1+N)^a b^N \bmod N^2$$

Consequently $w^{\lambda(N)} = (1+N)^{a\lambda(N)} \bmod N^2$, and then

$$L(w^{\lambda(N)} \bmod N^2) = a\lambda(N) \bmod N = \lambda(N)[w]_{1+N} \bmod N$$

■

Now, we can prove the following theorem

Theorem 8 $Class[N] \Leftarrow Factoring[N]$

Proof Since we know the factorization of N, we can easily compute $\lambda(N)$. For any given base g and a random $w \in Z^*_{N^2}$ we compute $[w]_g$ as follows. First we calculate $L(w^{\lambda(N)} \bmod N^2)$ and $L(g^{\lambda(N)} \bmod N^2)$. This leads to the values $\lambda(N)[w]_{1+N} \bmod N$ and $\lambda(N)[g]_{1+N} \bmod N$ respectively. By Theorem 7, $[g]_{1+N} = [1+N]_g^{-1} \bmod N$ is invertible. Consequently $L(g^{\lambda(N)} \bmod N^2)$ is invertible. Then

$$\frac{L(w^{\lambda(N)} \bmod N^2)}{L(g^{\lambda(N)} \bmod N^2)} = \frac{\lambda(N)[w]_{1+N}}{\lambda(N)[g]_{1+N}} = [w]_g \bmod N$$

■

Theorem 9 $Class[N] \Leftarrow RSA[N, N]$

Proof We prove that having an algorithm to invert $RSA[N, N]$ is sufficient to compute $Class[N]$. Given a base $g \in \mathcal{B}$ and a random $w \in Z^*_{N^2}$, we know that, since $\mathcal{E}_{1+N}$ is a permutation there exist $a, x \in Z_N$ and $b, y \in Z^*_N$ such that

$$w = (1 + aN)b^N \bmod N^2$$

and

$$g = (1 + xN)y^N \bmod N^2$$

Computing $w \bmod N$ and $g \bmod N$ we get the values $w' = b^N \bmod N$ and $g' = y^N \bmod N$.

From these values, using the given RSA$[N, N]$ inverter, is then possible to retrieve b and y.

Finally we compute a and x as

$$a = \frac{[w(b^{-1})^N \bmod N^2] - 1}{N}$$

and

$$x = \frac{[g(y^{-1})^N \bmod N^2] - 1}{N}$$

At the very end the $Class[N, g](w)$ is given by (theorem 7)

$$Class[N, g](w) = ax^{-1} \bmod N$$

■

We do not know if having an $RSA[N, N]$ oracle is a necessary condition to compute $Class[N]$ as well. In his paper, Paillier assumes that computing $Class[N]$, when such an oracle is not provided is hard. Informally this can be conjectured as follows. (We will give a precise formalization of this statement in the next chapter).

Assumption 6 *There is no probabilistic polynomial time algorithm that computes* $Class[N]$

However it is possible to prove that the related problem of inverting the function $\mathcal{E}_g$ is equivalent to $RSA[N, N]$

Theorem 10 *Given an RSA modulus N, consider the function* $\mathcal{E}_g$ *defined as in equation 3.3.5.* $\mathcal{E}_g$ *is a one-way function if and only if RSA[N,N] is a one-way function.*

Proof That an algorithm that inverts $RSA[N, N]$ can be used to invert $\mathcal{E}_g$ is evident from Theorem 9. Here we prove the inverse direction.
Assume to have an inverter for $\mathcal{E}_g$ and a random challenge $z \in Z_N$ we have to find the unique $x \in Z_N$ such that $z = x^N \bmod N$.
Using the given algorithm is possible to compute the values $a, c \in Z_N$ and $b, d \in Z_N^*$ such that

$$(1 + N) = g^a b^N \bmod N^2 \tag{3.3.7}$$

$$z = g^c d^N \bmod N^2 \tag{3.3.8}$$

Note that since $(1+N) \in \mathcal{B}$ any element $w \in Z^*_{N^2}$ can be expressed as $w = (1+\alpha N)\beta^N \bmod N^2$, for some $\alpha \in Z_N$ and $\beta \in Z^*_N$. In particular our challenge z can be written as $z = (1+N)^s x^N \bmod N^2$, even though we don't know such s and x.

Note that $z \bmod N = x^N \bmod N$ and then x is exactly the value we need to compute. Then we can write

$$z = g^c d^N \bmod N^2 = (1+N)^s x^N \bmod N^2 =$$

and by equation 3.3.8

$$= (g^a b^N)^s x^N \bmod N^2 = g^{as}(b^s x)^N \bmod N^2$$

Note that since a and s are elements smaller than N, the product as can be written as $r + tN$ for some r, t smaller than N.

$$= g^r (b^s g^t x)^N \bmod N^2$$

Since $\mathcal{E}_g$ is a permutation we must have that

$$c \equiv r \bmod N^2$$

and

$$d \equiv b^s g^t x \bmod N$$

and then

$$x \equiv d(b^s g^t)^{-1} \bmod N$$

■

To the computational problem $Class[N]$ it is possible to associate a corresponding decisional problem.

Definition 12 *We call D-Class[N] the decisional problem associated to Class[N]. More precisely, we define D-Class[N] as the problem of deciding, given* $w \in Z^*_{N^2}$, $x \in Z_N$ *and* $g \in \mathcal{B}$, *if* $x = [w]_g$ *or not.*

Of course an algorithm that computes the function $Class[N]$ is sufficient for deciding $D\text{-}Class[N]$, but the inverse is not known to be true. This leads to the following conjecture

Assumption 7 *If* N *is a modulus of unknown factorization, there exists no probabilistic polynomial time algorithm for the problem* $D\text{-}Class[N]$.

It is possible to prove the following

Theorem 11 $CR[N] \equiv D\text{-}Class$

Before proving the theorem we provide here a more formal description of assumptions 5 and 7.

Assumption 8 *Let N be a randomly chosen n-bit long RSA modulus. For every probabilistic polynomial time algorithm $\mathcal{A}$, define the following probabilities:*

$$P_{random} = \Pr\left[\begin{array}{l} x \leftarrow Z^*_{N^2}; \\ \\ \mathcal{A}(N,x) = 1 \end{array}\right]$$

and

$$P_{residue} = \Pr\left[\begin{array}{l} x \leftarrow Z^*_{N^2};\ \ y = x^N \bmod N^2; \\ \\ \mathcal{A}(N,y) = 1 \end{array}\right]$$

then, there exists a negligible function $\texttt{negl}()$ *such that*

$$|P_{random} - P_{residue}| < \texttt{negl}(n)$$

Assumption 9 *Let N be a randomly chosen n-bit long RSA modulus and g an element in $\mathcal{B}$. For every probabilistic polynomial time algorithm $\mathcal{A}$, define the following probabilities:*

$$P'_{random} = \Pr\left[\begin{array}{l} w \leftarrow Z^*_{N^2};\ \ x \leftarrow Z_N \\ \\ \mathcal{A}(N,g,w,x) = 1 \end{array}\right]$$

and

$$P'_{Class} = \Pr\left[\begin{array}{l} w \leftarrow Z^*_{N^2};\ \ x = Class[N,g](w) \bmod N^2; \\ \\ \mathcal{A}(N,g,w,x) = 1 \end{array}\right]$$

then, there exists a negligible function $\texttt{negl}()$ *such that*

$$|P'_{random} - P'_{Class}| < \texttt{negl}(n)$$

Proof [of theorem 11] Informally the proof goes by contradiction: we assume to have an efficient algorithm A (a decider) that decides $CR[N]$ and we prove that it is possible to construct another efficient algorithm A' that, using A as a black box, decides $D\text{-}Class[N]$. Then by a similar reasoning we prove the converse statement.

So assume to have an efficient decider D that contradicts assumption 8. This means that, for such an algorithm,

$$|P^D_{residue} - P^D_{random}| > \alpha(n)$$

where $\alpha(n) = 1/p(n)$ for some polynomial $p(n)$ and

$$P^D_{random} = \Pr\left[\begin{array}{l} x \leftarrow Z^*_{N^2}; \\ \\ D(N,x) = 1 \end{array}\right]$$

$$P^D_{residue} = \Pr\left[\begin{array}{l} x \leftarrow Z^*_{N^2};\ \ y = x^N \bmod N^2; \\ \\ D(N,y) = 1 \end{array}\right]$$

Now we show how to "use" D to construct a new algorithm D' that given as input a quadruple (N, g, w, x), where $w \in_R Z^*_{N^2}$, has to decide if $Class[N,g](w) = x$ with probability significantly larger than $1/2$. The algorithm D' is constructed as follows

$D'(N, g, w, x)$

$y \leftarrow Z_N^*$

$w' \leftarrow wg^{-x}y^N \bmod N^2$

Let $ans \in \{YES, NO\}$ the response of D on input (N, w')

if $and = YES$ return YES

else return NO

Analysis. We define

$$P'^{D'}_{random} = \Pr\left[\begin{array}{l} w \leftarrow Z_{N^2}^*; \;\; x \leftarrow Z_N \\ \\ D'(N, g, w, x) = 1 \end{array}\right]$$

and

$$P'^{D'}_{Class} = \Pr\left[\begin{array}{l} w \leftarrow Z_{N^2}^*; \;\; x = Class[N, g](w) \bmod N^2; \\ \\ D'(N, g, w, x) = 1 \end{array}\right]$$

If $x = Class[N, g](w)$, w' is an N^{th} residue, moreover it is uniformly distributed in the subgroup of N^{th} residues modulo N^2. This implies that

$$P'^{D'}_{Class} = P^D_{residue}$$

On the other hand if x is a random element in Z_N w' is uniformly distributed in $Z_{N^2}^*$. In this case

$$P'^{D'}_{random} = P^D_{random}$$

At the very end we get

$$|P'^{D'}_{Class} - P'^{D'}_{random}| > \alpha(n)$$

thus contradicting the intractability of the *D-Class* problem.

Conversely we are given a decider D' that contradicts assumption 9, again, meaning with this that

$$|P'^{D'}_{Class} - P^{D'}_{random}| > \beta(n)$$

(again $\beta(n) = 1/q(n)$ for some polynomial $q(n)$).

This time we have to use D' to construct a new algorithm D that given as input a couple (N, z), where $z \in_R Z^*_{N^2}$, has to decide if z is an N^{th} residue or not, with probability significantly larger than 1/2. The algorithm D is the following

$D(N, z)$

Choose an arbitrary $g \in \mathcal{B}$

$x \leftarrow Z_N$

$y \leftarrow Z^*_N$

$w' \leftarrow wg^x y^N \bmod N^2$

Let $ans \in \{YES, NO\}$ the response of D' on input (N, g, w', x)

if $and = YES$ return YES

else return NO

Analysis. If w is an (uniformly distributed) N^{th} residue in $Z^*_{N^2}$ then w' is an uniformly distributed element in $Z^*_{N^2}$, such that $[w]_g = x$. This implies that

$$P^D_{residue} = P'^{D'}_{Class}$$

On the other hand if w is a uniformly distributed element in $Z^*_{N^2}$, w' is uniformly distributed in $Z^*_{N^2}$ (and, in this case, $[w]_g \neq x$ of course). For such a situation

$$P^D_{random} = {P'}^{D'}_{random}$$

At the very end we get

$$|P^D_{residue} - P^D_{random}| > \beta(n)$$

thus contradicting the intractability of the CR problem. ■

3.4 The proposed scheme

Now we are ready to present the actual scheme.

Key Generation. Let k be the security parameter. Choose uniformly and at random two k-bit primes p and q and set $N = pq$. Choose a random base $g \in \mathcal{B}$. (Note that, if we know the factorization of N, checking if a given element g is in $\mathcal{B}$ can be done efficiently by simply checking whether $\gcd(L(g^{\lambda(N)} \bmod N^2), N) = 1$).

Encryption. To encrypt a message $m < N$, one chooses a random value $r \in Z^*_N$ and computes the ciphertext as

$$c = g^m r^N \bmod N^2$$

Decryption. When receiving a ciphertext c, check that $c < N^2$. If yes, retrieve the message m as

$$m = \frac{L(c^{\lambda(N)} \bmod N^2)}{L(g^{\lambda(N)} \bmod N^2)} \bmod N$$

.

The correctness and the one-wayness of the scheme clearly follows from the results presented in the previous section.
Moreover it is possible to prove that it is semantically secure under the assumption that the Decisional Composite Residuosity Assumption holds [47].

Theorem 12 *The above scheme is semantically secure if and only if assumption 9 holds.*

Proof The proof goes by contradiction. First we assume the scheme not to be semantically secure and then we prove that this lead to an efficient distinguisher for the $DCRA$. Conversely we assume the $DCRA$ not to be valid and then we prove that this fact implies that the scheme cannot be semantically secure.

Assume the scheme is not semantically secure. This means that it is not polynomially indistinguishable either, i.e. that there exists an adversary T that can choose two messages m_0, m_1 whose encryptions he can (efficiently) distinguish between. More precisely T arbitrarily chooses two messages m_0 and m_1 and asks an encryption oracle to produce the ciphertext c, from either m_0 or m_1. The encryption oracle works as follows. He chooses a random bit

b and encrypts m_b. Then he sends the obtained ciphertext c to T. The goal of T is to "understand" if c is an encryption of m_0 or of m_1. By saying that T can efficiently succeed in this operation, formally we mean

$$Pr[T(m_0, m_1, c, N, g) = m \,|\, m \in_R \{m_0, m_1\};\ r \in_R Z_N^* c = g^m r^N \bmod N^2] > \frac{1}{2} + \frac{1}{Q(n)}$$

for some polynomial $Q(\cdot)$ (where $n = |N|$). Our goal, now, is to design an efficient algorithm T' that, taking advantage of the "ability" of T, can efficiently decide if a given couple (w, x) is such that $[w]_g = x$ or not.

T' works as follows

$T'(N, w, x)$

Choose an arbitrary $g \in \mathcal{B}$

$r = wg^{-x} \bmod N^2$

$b \leftarrow \{0, 1\}$

$c = g^{m_b} r \bmod N^2$

Let $b' \in \{0, 1\}$ be the response of T on input (m_0, m_1, c, N, g)

if $b' = b$ then return YES

else return NO

The underlying idea of the above algorithm is that if x is the class of w, then the value $r = wg^{-x} \bmod N^2$ is an N^{th} residue in $Z_{N^2}^*$ and the produced ciphertext c is a valid one for m_b. In this case we know that T has a non negligible advantage in guessing b. On the other hand if $x \neq [w]_g$, c is an invalid ciphertext (moreover it is a random element) and T cannot guess b better than at random.

More formally if $x = [w]_g$ then $c = g^{m_b} r \bmod N^2$ is a valid encryption of m_b

and then the probability that T' returns YES is exactly the probability that T guesses the message c came from.

$$P_{Class}^{T'} > \frac{1}{2} + \frac{1}{Q(n)}$$

If x is a random element in Z_N (remember w is a random element in $Z_{N^2}^*$) the quantity $r = wg^{-x} \bmod N^2$ is a random element in $Z_{N^2}^*$. This means that r can be written as $g^a b^N \bmod N^2$ where a is uniformly distributed in Z_N. The ciphertext c is then

$$c = g^{m_b+a} b^N \bmod N^2$$

Note that, in the above relation, a hides m_b perfectly and thus T cannot guess b better than at random. In this case the success probability of the algorithm T' is then

$$P_{random}^{T'} = \frac{1}{2}$$

At the very end

$$|P_{Class}^{T'} - P_{random}^{T'}| > \frac{1}{2} + \frac{1}{Q(n)} - \frac{1}{2} = \frac{1}{Q(n)}$$

Conversely, assume, for the sake of contradiction, to have a decider T' for the Decisional Class problem. For such an algorithm we have

$$P'^{T'}_{Class} - P_{random}^{T'} > \beta(n)$$

(where $\beta(n) = 1/q(n)$ for some polynomial $q(n)$. Note that we have dropped the absolute value from the above inequality. This can be done without loss

of generality. The proof can be done similarly in the case on which the other direction of the inequality is true).

This time we have to use T' to construct a new algorithm T that given as input a quintuple (m_0, m_1, c, N, g), has to decide if c is the encryption of either m_0 or m_1 (where m_0 and m_1 are arbitrarily chosen) with non negligible probability. In particular we choose $m_0, m_1 \in_R Z_N$. For such a choice we pass querying an encryption oracle to receive a ciphertext c that is either an encryption of m_0 or an encryption of m_1. Here we provide the algorithmic description for T

$T(m_0, m_1, c, N, g)$

Let $b' \in \{0, 1\}$ be the response of T' on input (N, g, c, m_1)

if $b' = 1$ then return YES

else return NO

The underlying intuition is that if c is an encryption of m_1 then $m_1 = [c]_g$.

More formally we have that

$$\begin{aligned} Pr[T \text{ succeeds}] &= Pr[T'(N, g, c, m_1) = 1 \mid [c]_g = m_1] Pr[[c]_g = m_1] + \\ &\quad Pr[T'(N, g, c, m_1) = 0 \mid [c]_g \neq m_1] Pr[[c]_g \neq m_1] = \\ &= \tfrac{1}{2}[P^{T'}_{Class} + (1 - P^{T'}_{random})] = \\ &= \tfrac{1}{2} + \tfrac{1}{2}(P^{T'}_{Class} - P^{T'}_{random}) > \tfrac{1}{2} + \tfrac{1}{2\beta(n)} \end{aligned}$$

This completes the proof. ■

A discussion about efficiency and implementation aspects of the cryptosystem can be founded in [47].

3.5 Properties

Before concluding this chapter we would like to stress some of the most interesting aspects of Paillier's Cryptosystem.

- **Additive Homomorphic Property**

  The functions $\mathcal{E}_g(x,y) = g^x y^N \bmod N^2$ and $Class_g(w) = [w]_g$ presented in the previous section have the very interesting property to be additively homomorphic. Since the proposed scheme is based on such functions it "inherits" the property.

  From a practical point of view an homomorphic cryptosystem has an enormous amount of applications like electronic voting, watermarking and threshold cryptography just to cite a few.

- **Self Blinding**

  Another very useful property of a cryptosystem is the so-called *self-blinding*, i.e. the property by which any ciphertext can randomly be changed into another without affecting the plaintext. This property is achieved as follows. For any given message $m \in Z_N$ and random integer r, let $E(m)$ be a valid encryption of m. We have $D(E(m)) = m)$ and $D(E(m)r^N \bmod N^2) = m$.