University of Crete

Department of Mathematics and Applied Mathematics

Diploma Thesis

Homomorphic Cryptography: Paillier's Cryptosystem

Styliani Chamilaki

Supervisor: Theodoulos Garefalakis

Heraklion
Ac. Year: 2019-2020

Abstract

This thesis describes Paillier's cryptosystem, a form of homomorphic encryption. Based on composite residuosity, it proposes a trapdoor mechanism leading to three encryption schemes; two homomorphic probabilistic schemes and one trapdoor permutation, which will be examined separately. All three of them will be proven valid and secure. Modular arithmetics and number theory will be our main tools used.

Contents

Acronyms & Notations

Class$[n, g]$

n-th Residuosity Class Problem
the problem of computing the class function in base g

CCRA

Computational Composite Residuosity Assumption
the hypothesis that $Class[n]$ *is intractable*

CR$[n]$

the problem of deciding n-th residuosity

CRCP

Composite Residuosity Class Problem
the computational problem $Class[n]$
given $w \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$, *compute* $[\![w]\!]_g$

D-Class$[n]$

the decisional problem associated to Class$[n]$
given $w \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$, $x \in \mathcal{Z}_n$, *decide whether* $[\![w]\!]_g = x$

DCRA

Decisional Composite Residuosity Assumption
the hypothesis that $CR[n]$ *is intractable*

D-PDL$[n, g]$

the decisional problem associated to PDL$[n, g]$
given $w \in \langle g \rangle$, $g \in \mathcal{B}$, $x \in \mathcal{Z}_n$, *decide whether* $[\![w]\!]_g = x$

PDL$[n, g]$

Partial Discrete Logarithm Problem
given $w \in \langle g \rangle$, $g \in \mathcal{B}$, *compute* $[\![w]\!]_g$

RSA$[n, e]$

the problem of extracting e-th roots $\mod n$.

RSR

Random Self Reducible

$[\![\boldsymbol{w}]\!]_g$

n-th Residuosity Class of w with respect to g
the unique $x \in \mathcal{Z}_n$ for which $\exists y \in \mathcal{Z}^*_n$ s.t. $\mathcal{E}_g(x, y) = w$

Introduction

Since the discovery of public-key cryptography by Diffie and Hellman in the 1970s, very few convincingly secure asymmetric schemes have been discovered, despite considerable research efforts.

Two major species of trapdoor techniques are in use today. The first refers to RSA and other variants. The technique conjugates the polynomial-time root extraction of polynomials over finite fields with the intractability of factoring large numbers. Another famous technique combines the homomorphic properties of intractability of extracting discrete logarithms over finite groups.

However, very soon, a progressive emergence of a third class of trapdoor techniques occurred. Those techniques were firstly identified as trapdoor in the discrete logarithm, but they actually arise from the common algebraic setting of high degree residuosity classes. That need led Paillier to introduce in 1999 a new trapdoor mechanism. By contrast to prime residuosity, his technique is based on composite residuosity classes, *i.e.* of degree set to a hard-to-factor number $n = pq$, where p and q are large primes.

In this paper we describe thoroughly Paillier's technique. Starting with some notions such as one-wayness, we continue by discussing n-th residuosity mod n^2 in order to examine computing composite residuosity classes. We define the computational problem Composite Residuosity Class Problem (CRCP), whose intractability will be our main assumption. We, then, introduce the main probabilistic encryption scheme and later on its modification leading to smaller decryption complexity. Both schemes are proven additively homomorphic on the encryption function and semantically secure under appropriate intractability assumptions. Last, but not least, a trapdoor permutation is presented too. Our purpose is to approach the cryptosystem from the number theoretic viewpoint.

Chapter 1

Preliminaries

1.1 One-way functions

In cryptography, security is an essential matter. In order to enable it, we use a type of functions called one-way functions.

Definition 1.1. A function $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ is *strong one-way* or simply *one-way* iff:

(i) f is polynomial time computable

(ii) for any probabilistic polynomial time algorithm A, the probability that A successfully inverts $f(x)$, for random $x \in \{0,1\}^*$, is negligible.

Consider a communication channel. Two people who want to communicate through it should easily encrypt and decrypt, while for an intruder it must be computationally intractable to decrypt without the secret key. In order for this computational gap to exist, there must be a limit on the computational capabilities of the intruder which also applies on the original users. Thus there exists the assumption that any user can only perform probabilistic polynomial time computations. For the same reasons it is essential that such a function is hard to invert.

However, by being hard to invert, followingly decrypt, we do not mean impossible. Such an assumption would be unrealistic as there is a small, but, nevertheless, non-zero chance that if each time the intruder guesses the message, the guess might be correct. Instead, we want that, under the use of any probabilistic polynomial time algorithm, the probability the intruder decrypts ciphertext $c = E(m)$, m random message and E the encryption function, is negligible, even if he repeats the attacks a polynomial number of times.

Examples

Discrete Logarithm Problem (DLP)

Let p be prime, g a primitive root $\pmod p$. We define

$$\begin{aligned} dexp : (\mathbb{Z}_{p-1}, +) &\longrightarrow \mathbb{Z}_p^* \\ \bar{x} &\longmapsto \bar{g^x} \end{aligned}$$

which is well defined. Consider $\bar{x_1} = \bar{x_2}$, then

$$x_1 \equiv x_2 \pmod p \Leftrightarrow g^{x_1} \equiv g^{x_2} \pmod p.$$

The result depends on the class of x, not the representative. Whilst this output is easy to compute since exponentiation $\mod p$ can be performed in polynomial time, it is considered extremely hard to inversely compute x.

Factoring of the product of two large primes

Let p, q large primes randomly chosen. We define

$$\begin{aligned} mult : \mathbb{P} \times \mathbb{P} &\longrightarrow \mathbb{Z} \\ (p, q) &\longmapsto pq \end{aligned}$$

where $\mathbb{P}$ is the set of prime numbers . This one is believed to be hard to invert.

Discrete Root Extraction Problem (RSA encryption)

Let $n = pq$, where p, q large primes, $e \in \mathbb{Z}_n^*$ with $(e, \varphi(n)) = 1$ and $y \in \mathbb{Z}_n^*$ the message. We define

$$\begin{aligned} e_y : \mathbb{Z}_n^* &\longrightarrow \mathbb{Z}_n^* \\ y &\longmapsto y^e \end{aligned}$$

RSA encryption is thought to be a strong one-way function as it relies on the factoring of n in order to compute the message y using the Chinese Remainder Theorem.

Other examples are:
Quadratic residue problem
Subset sum problem

Trapdoor Functions

A trapdoor function f is a one-way function with an extra property; there exists a special information, called the "trapdoor", that allows inversion of the function when possessing it. It should be easy to compute f on any point, but infeasible to invert it on any point without knowledge of the trapdoor. Moreover, it should be easy to generate matched pairs of f and corresponding trapdoor. Once a matched pair is generated, the publication of f should not reveal anything about how to compute its inverse on any point. Trapdoor functions are widely used in cryptography, yet it is hard to find one.

1.2 Reductions

As we will define and refer to some algorithmic problems, we need to set a notion of algorithmic relation that will be used to connect two of them.

Definition 1.2. A computational problem A is *polynomial-time reducible* to a computational problem B if there exists an algorithm $\mathcal{A}$ for solving problem A that is allowed to make a polynomial (in the size of the input) number of calls to an algorithm $\mathcal{B}$ for problem B.

The relation $A \Leftarrow B$ will denote that the problem A is polynomial reducible to the problem B.

Definition 1.3. We will call two problems A and B *equivalent* if $A \Leftarrow B$ and $B \Leftarrow A$.

Random-Self-Reducibility

Definition 1.4. Suppose $f : A \longrightarrow B$ and $\mathcal{A}$ an algorithm that calculates f. We call f *random-self-reducible (RSR)* if there exists a probabilistic algorithm $G : A \longrightarrow A$ s.t. $\mathcal{A}(G(x)) = f(x)$ for an input x.

Random-self-reducibility can be used to show that a problem is as hard in the average, as it is in the worst case. Problems with this property, such as Factoring, DLP, RSA, are thought to be good candidates for one-way functions.

1.3 Carmichael's Lambda Function

Definition 1.5. Let n be a positive integer. We define as the *Carmichael's Lambda function*, $\lambda(n)$, the smallest positive integer m s.t.

$$\alpha^m \equiv 1 \pmod{n}, \quad \forall \alpha \in \{1, ..., n\}, \, (\alpha, n) = 1$$

Proposition 1.1. *We have that $\lambda(n)$ equals the exponent of the multiplicative group $\mathbb{Z}_n^*$, that is*

$$\lambda = \lambda(n) = \operatorname{lcm}\{\operatorname{ord}_n(\alpha) \, : \, (\alpha, n) = 1\}.$$

Proof. Suppose $\mathbb{Z}_n^* = \{a_1, a_2, \ldots, a_{\phi(n)}\}$ and we note

$$\operatorname{lcm} = \operatorname{lcm}(\operatorname{ord}(a_1), \operatorname{ord}(a_2), \ldots, \operatorname{ord}(a_{\phi(n)})).$$

We have that

$$\left.\begin{array}{lll} a_1^{\operatorname{ord}(a_1)} & \equiv 1 & \pmod{n} \\ a_2^{\operatorname{ord}(a_2)} & \equiv 1 & \pmod{n} \\ \vdots & & \vdots \\ a_{\phi(n)}^{\operatorname{ord}(a_{\phi(n)})} & \equiv 1 & \pmod{n} \end{array}\right\} \Rightarrow \begin{array}{lll} a_1^{\operatorname{lcm}} & \equiv 1 & \pmod{n} \\ a_2^{\operatorname{lcm}} & \equiv 1 & \pmod{n} \\ \vdots & & \vdots \\ a_{\phi(n)}^{\operatorname{lcm}} & \equiv 1 & \pmod{n} \end{array}$$

Consider there exists $r < \operatorname{lcm}$ s.t.

$$\begin{array}{lll} a_1^r & \equiv 1 & \pmod{n} \\ a_2^r & \equiv 1 & \pmod{n} \\ \vdots & & \vdots \\ a_{\phi(n)}^r & \equiv 1 & \pmod{n} \end{array}$$

Then

$$\left.\begin{array}{c} \operatorname{ord}(a_1) \mid r \\ \operatorname{ord}(a_2) \mid r \\ \vdots \\ \operatorname{ord}(a_{\phi(n)}) \mid r \end{array}\right\} \Rightarrow \operatorname{lcm} \mid r$$

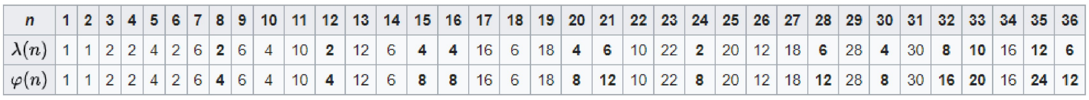
contradiction, so it must be lcm the minimum number m s.t.

$$\alpha^m \equiv 1 \pmod{n}, \quad \forall \alpha \in \mathbb{Z}_n^*.$$

It follows that $\lambda = \text{lcm}$

$\square$

Below they are compared the Carmichael function and Euler's totient function for some values of n.



n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\lambda(n)$	1	1	2	2	4	2	6	**2**	6	4	10	**2**	12	6	**4**	**4**	16	6	18	**4**	**6**	10	22	**2**	20	12	18	**6**	28	**4**	30	**8**	**10**	16	**12**	**6**
$\varphi(n)$	1	1	2	2	4	2	6	**4**	6	4	10	**4**	12	6	**8**	**8**	16	6	18	**8**	**12**	10	22	**8**	20	12	18	**12**	28	**8**	30	**16**	**20**	16	**24**	**12**

Figure 1.1: Comparison between Carmichael's function and Euler's totient function

Proposition 1.2. *For $\alpha, n \in \mathbb{N}$, $\alpha < n$, $(\alpha, n) = 1$ the following hold:*

(i) $ord_n(\alpha) \mid \lambda(n)$

(ii) *If* $\alpha^m \equiv 1 (mod\, n)\,,\ \forall \alpha$, *then* $\lambda(n) \mid m$

(iii) $\lambda(n) \mid \varphi(n)$

(iv) *If* $a \mid b$, *then* $\lambda(a) \mid \lambda(b)$

(v) $\lambda(\text{lcm}(a, b)) = \text{lcm}(\lambda(a), \lambda(b))$

(vi) $\lambda(2^k) \leq 2^{k-2}\,,\quad$ *for* $k \neq 3$

Proof. (i) We have shown that

$$\lambda(n) = \text{lcm}\{ord_n(\alpha) \;:\; (\alpha, n) = 1\}$$

so

$$ord_n(\alpha) \mid \lambda(n)\,, \quad \forall \alpha$$

(ii) Suppose that $m = \lambda(n)q + r\,,\ 0 \leq r < \lambda(n)$

$$\alpha^m \equiv 1 \pmod{n} \Rightarrow \alpha^{\lambda(n)q+r} \overset{def\lambda}{\Longrightarrow} \alpha^r \equiv 1 \pmod{n}\,, \quad \forall \alpha$$

By definition we have that λ is the smallest number m s.t.

$$\alpha^m \equiv 1 \pmod{n}\,, \forall \alpha$$

so the above contradicts with the minimality of $\lambda(n)$, unless $r = 0$.

(iii) From (ii) for $m = \varphi(n)$ we get

$$\lambda(n) \mid \varphi(n)$$

For the rest of the properties suppose $w \in \mathbb{N}$, $(w, \operatorname{lcm}(a, b)) = 1$.

(iv) If $a \mid b$, then $b = aq$, $q \in \mathbb{Z}$, $(a, q) = 1$.

$$w^{\lambda(b)} \equiv 1 \pmod b \Rightarrow w^{\lambda(b)} \equiv 1 \pmod a$$

But $\lambda(a)$ is the smallest number that satisfies the last congruence, so it must be $\lambda(a) \mid \lambda(b)$.

(v) On the one hand we have

$$w^{\lambda(\operatorname{lcm}(a,b))} \equiv 1 \pmod{\operatorname{lcm}(a, b)}$$

and also

$$\begin{gathered} a \mid \operatorname{lcm}(a, b) \Rightarrow \lambda(a) \mid \lambda(\operatorname{lcm}(a, b)) \\ b \mid \operatorname{lcm}(a, b) \Rightarrow \lambda(b) \mid \lambda(\operatorname{lcm}(a, b)) \end{gathered}$$

Which leads to

$$\operatorname{lcm}(\lambda(a), \lambda(b)) \mid \lambda(\operatorname{lcm}(a, b))$$

On the other hand,

$$\operatorname{lcm}(\lambda(a), \lambda(b)) = k\lambda(a)\,,\ k \in \mathbb{Z} \text{ or } \operatorname{lcm}(\lambda(a), \lambda(b)) = t\lambda(b)\,,\ t \in \mathbb{Z}$$

And so,

$$\begin{aligned} w^{\operatorname{lcm}(\lambda(a),\lambda(b))} &\equiv 1 \pmod a \Rightarrow w^{\operatorname{lcm}(\lambda(a),\lambda(b))} - 1 \equiv 0 \pmod a \\ w^{\operatorname{lcm}(\lambda(a),\lambda(b))} &\equiv 1 \pmod b \Rightarrow w^{\operatorname{lcm}(\lambda(a),\lambda(b))} - 1 \equiv 0 \pmod b \end{aligned}$$

From the above we have

$$\begin{gathered} w^{\operatorname{lcm}(\lambda(a),\lambda(b))} - 1 \equiv 0 \pmod{\operatorname{lcm}(a, b)} \Rightarrow \\ w^{\operatorname{lcm}(\lambda(a),\lambda(b))} \equiv 1 \pmod{\operatorname{lcm}(a, b)} \overset{(ii)}{\Longrightarrow} \\ \lambda(\operatorname{lcm}(a, b)) \mid \operatorname{lcm}(\lambda(a), \lambda(b)) \end{gathered}$$

The result follows.

(vi) An easy induction can show that for $r \geq 3$

$$\alpha^{2^{r-2}} \equiv 1 \pmod{2^r} \text{ , for every } \alpha \text{ odd.}$$

For $r = 3$ we get $\alpha^2 \equiv 1 \pmod 8$ which is true. Suppose it holds for r, that is $\alpha^{2^{r-2}} = 1 + k2^r$, for some $k \in \mathbb{Z}$. We square the equality and we get $\alpha^{2^{r-1}} = 1 + 2^{r+1}k + 2^{2r}k^2 \equiv 1 \pmod{2^{r+1}}$.
Now by (ii) we get $\lambda(2^r) \mid 2^{r-2}$.

□

Computing Carmichael's Lambda function

Proposition 1.3. *Let p prime. We have that,*

$$\lambda(p^r) = \begin{cases} \varphi(p^r) & \text{, if } p \geq 3 \text{ or } r \leq 2 \\ \frac{1}{2}\varphi(p^r) & \text{, if } p = 2 \text{ and } r \geq 3 \end{cases}$$

Proof. We start by examining the different cases.

- $p \geq 3$

Since p^r is an odd prime power, there exists a primitive root $g \pmod{p^r}$ s.t.

$$ord_{p^r}(g) = \varphi(p^r).$$

We have that

$$g^{\lambda(p^r)} \equiv 1 \pmod{p^r},$$

so it should be

$$ord_{p^r}(g) \mid \lambda(p^r) \Rightarrow \varphi(p^r) \mid \lambda(p^r).$$

But we know that $\lambda(p^r) \mid \varphi(p^r)$, so

$$\lambda(p^r) = \varphi(p^r).$$

- $p = 2$

For $r = 1, 2$ we can easily see that $\lambda(2^r) = \varphi(2^r)$.
For $r \geq 3$ we get from property (ii) that $\lambda(2^r) \mid 2^{r-2}$ and an easy induction shows that

$$5^{2^{r-3}} \equiv 1 + 2^{r-1} \pmod{2^r}.$$

This tells us that the order of 5 does not divide 2^{r-3}, but it is a power of 2, so it must be 2^{r-2}.
This shows that

$$\lambda(2^r) = 2^{r-2} = \frac{1}{2}\varphi(2^r).$$

□

Now let's consider the unique factorization of any $n > 1$ as $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, where $p_1 < p_2 < ... < p_k$ are primes and $r_1, r_2, ..., r_k$ are positive integers. Then,

$$\lambda(n) = \mathrm{lcm}(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}), ..., \lambda(p_k^{r_k})).$$

Proof. Now let $n = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, where $p_1 < p_2 < ... < p_k$ are primes and $r_1, r_2, ..., r_k$ are positive integers and $m = \mathrm{lcm}(\lambda(p_1^{r_1}), ..., \lambda(p_k^{r_k}))$.
For each p_i there exists a primitive root $g_i \pmod{p_i^{r_i}}$. We will use the Chinese Remainder Theorem. Consider a map

$$\begin{aligned} \theta \, : \, \mathbb{Z}_n^* &\cong \mathbb{Z}_{p_1^{r_1}}^* \otimes ... \otimes \mathbb{Z}_{p_k^{r_k}}^* \\ g &\longmapsto (g_1, ..., g_k) \end{aligned}$$

We have that,

$$\theta(g^m) = \theta(g)^m = (g_1, ..., g_k)^m = (g_1^m, ..., g_k^m) = (1, ..., 1) = \theta(1) \Rightarrow$$
$$g^m \equiv 1 (mod\, n) \Rightarrow ord(g) \mid m \, , \, \forall g \in \mathbb{Z}_n^* \xRightarrow{def\, \lambda} \lambda \mid m.$$

What is more, there exists $g \in \mathbb{Z}_n^*$ s.t. $ord(g) = \lambda(p_i^{r_i})$, $\forall p_i$. Then, by definition of λ, we have that

$$\lambda(p_i^{r_i}) \mid \lambda \, , \, \forall p_i \Rightarrow \mathrm{lcm}(\lambda(p_1^{r_1}), ..., \lambda(p_k^{r_k})) \mid \lambda \Rightarrow m \mid \lambda.$$

The result follows. □

1.4 Notations

From now on we set $n = pq$, where p and q are large primes s.t.

$$(p, q-1) = (p-1, q) = 1.$$

It follows that,

$$\varphi(n) = (p-1)(q-1) \qquad \text{and} \qquad \lambda(n) = \lambda = \operatorname{lcm}(p-1, q-1)$$

In particular,

$$(\lambda, n) = 1$$

as $(p, q-1) = (p-1, q) = 1$. Furthermore,

$$\begin{aligned}\lambda(n^2) &= \operatorname{lcm}(\lambda(p^2), \lambda(q^2)) = \operatorname{lcm}(p(p-1), q(q-1)) \\ &= n \operatorname{lcm}(p-1, q-1) = n\lambda\end{aligned}$$

We will work on $\mathbb{Z}^*_{n^2}$. It holds that

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

and that for any $w \in \mathbb{Z}^*_{n^2}$;

$$\begin{cases} w^{\lambda} & \equiv 1 \pmod{n} \\ w^{n\lambda} & \equiv 1 \pmod{n^2} \end{cases}$$

due to the Carmichael's Lambda function. More specifically, $w^{\lambda} \equiv 1 \pmod{n}$ from the definition of λ and $w^{n\lambda} \equiv w^{\lambda(n^2)} \equiv 1 \pmod{n^2}$.

Finally, we denote the following sets we will also work on:

$$\mathcal{Z}_n = \{0, 1, ..., n-1\}$$

and

$$\mathcal{Z}^*_n = \{y \in \mathbb{N} \mid \gcd(y, n) = 1,\ y < n\}$$

Chapter 2

Deciding Composite Residuosity

We note that from now on we will use the assumptions introduced in the previous section "Notations".

We begin by briefly introducing composite degree residues as a natural instance of higher degree residues and give some basic related facts. The originality of the setting resides in using a square number as modulus.

Definition 2.1. A number z is said to be a *n-th residue modulo n^2* if there exists a number $y \in \mathbb{Z}_{n^2}^*$ s.t.

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

Proposition 2.1. *For any $y \in \mathbb{Z}_{n^2}^*$ it holds that*

$$y^n \equiv 1 \pmod{n^2} \Rightarrow y \equiv 1 \pmod{n}.$$

Proof. If $y^n \equiv 1 \pmod{n^2}$, then $y^n \equiv 1 \pmod{n}$.
Furthermore we know that

$$y^\lambda \equiv 1 \pmod{n}$$

But $(\lambda, n) = 1$, so there exist $s, t \in \mathbb{Z}$ s.t. $1 = s\lambda + tn$, so

$$y \equiv y^{s\lambda + tn} \equiv y^{s\lambda} y^{tn} \equiv 1 \pmod{n}$$

□

Proposition 2.2. *The n-th roots of unity are the numbers of the form*

$$(1+n)^k \equiv 1+kn \pmod{n^2}, \quad 0 \le k \le n-1$$

Proof. We have

$$\begin{aligned} y^n \equiv 1 \pmod{n^2} &\Rightarrow y \equiv 1 \pmod{n}, \quad y \in \mathbb{Z}^*_{n^2} \\ &\Rightarrow y = 1+kn, \quad 0 \le k \le n-1 \end{aligned}$$

On the other side,

$$\begin{aligned} y^n &\equiv (1+kn)^n \equiv \sum_{i=0}^{n} \binom{n}{i} k^i n^i \\ &\equiv 1 + \binom{n}{1} kn + n^2 (\sum_{i=2}^{n} \binom{n}{i} k^i n^{i-2}) \\ &\equiv 1 \pmod{n^2} \end{aligned}$$

Furthermore

$$(1+n)^k \equiv \textstyle\sum_{j=0}^{k} n^j \equiv 1+kn \pmod{n^2}$$

The result follows. □

Proposition 2.3. *The set of n-th residues is a multiplicative subgroup of $\mathbb{Z}^*_{n^2}$ of order $\varphi(n)$.*

Proof. Suppose

$$z \equiv y^n \pmod{n^2}, \quad y \in \mathbb{Z}^*_{n^2}.$$

Now consider an homomorphism θ s.t.

$$\begin{aligned} \theta : \mathbb{Z}^*_{n^2} &\longrightarrow \mathbb{Z}^*_{n^2} \\ y &\longmapsto y^n \end{aligned}$$

The n-th residues are exactly the image of θ and $im(\theta) \subseteq \mathbb{Z}^*_{n^2}$, thus the set of n-th residues is a multiplicative subgroup of $\mathbb{Z}^*_{n^2}$.
Now, by the First Isomorphism Theorem, we get that

$$\mathrm{im}(\theta) \cong \frac{\mathbb{Z}^*_{n^2}}{\ker\theta} \Rightarrow \mid \mathrm{im}(\theta) \mid = \frac{\mid \mathbb{Z}^*_{n^2} \mid}{\mid \ker\theta \mid},$$

where

$$\ker\theta = \{y \in \mathbb{Z}^*_{n^2} \mid y^n \equiv 1 \pmod{n^2}\},$$

in other words, the n-th roots of unity modulo n^2.
We have already shown that they are numbers of the form

$$y \equiv 1 + kn \pmod{n^2}, \quad 0 \leq k \leq n-1$$

It remains to prove that for every value of k, we have a different result. Suppose $0 \leq i < j \leq n-1$ s.t.

$$1 + in \equiv 1 + jn \pmod{n^2}.$$

It follows that

$$i \equiv j \pmod{n},$$

that is

$$\mid \ker\theta \mid = n.$$

So,

$$\mid \mathrm{im}(\theta) \mid = \frac{n\varphi(n)}{n} = \varphi(n).$$

□

Proposition 2.4. *Each n-th residue z has exactly n n-th roots.*

Proof. We will use the previous homomorphism θ. We have that $\mathrm{im}\,\theta$ is all the n-th residues and we want to count all the y s.t. $\theta(y) = z$.
Let $y_0 \in \mathbb{Z}^*_{n^2}$ s.t.

$$\theta(y_0) = z.$$

We claim that

$$\theta^{-1}(z) = y_0 \ker(\theta)$$

If $y \in y_0 \ker(\theta)$, then

$$y = y_0 r \quad , \text{for some } r \in \ker(\theta)$$

and

$$\theta(y) = \theta(y_0 r) = \theta(y_0)\theta(r) = \theta(y_0) = z \Rightarrow y_0 \ker(\theta) \subseteq \theta^{-1}(z)$$

Now let $y \in \theta^{-1}(z)$, then

$$\theta(y) = z = \theta(y_0) \Rightarrow \theta(y)\theta^{-1}(y_0) = 1 \Rightarrow \theta(yy_0^{-1}) = 1 \Rightarrow yy_0^{-1} \in \ker(\theta)$$

$$\Rightarrow y = y_0 r \in y_0 \ker(\theta), \qquad \text{for some } r \in \ker(\theta)$$

$$\Rightarrow \theta^{-1}(z) \subseteq y_0 \ker(\theta)$$

Therefore,

$$\mid \theta^{-1}(z) \mid = \mid \ker(\theta) \mid = n$$

□

Definition 2.2. We note as $CR[n]$ the problem of deciding n-th residuosity, *i.e.* distinguishing n-th residues from the non-n-th residues.

$CR[n]$ is RSR that is, all of the instances are polynomially equivalent. Each case is thus an average one and the problem is either uniformly intractable or uniformly polynomial. However,

Conjecture. There exists no polynomial time distinguisher for n-th residues modulo n^2, *i.e.* *CR[n]* is intractable.

Definition 2.3. The hypothesis that $CR[n]$ is intractable will be noted as *Decisional Composite Residuosity Assumption (DCRA).*

Due to the RSR property its validity only depends on the choice of n.

Chapter 3

Computing Composite Residuosity Classes

We now proceed to describe the number-theoretic framework underlying the cryptosystems introduced later on.

Definition 3.1. Let g be some element of $\mathbb{Z}^*_{n^2}$. We denote by $\mathcal{E}_g$ the integer-valued function defined by

$$\begin{aligned} \mathcal{E}_g : \mathcal{Z}_n \times \mathcal{Z}^*_n &\longrightarrow \mathbb{Z}^*_{n^2} \\ (x, y) &\longmapsto g^x y^n \pmod{n^2} \end{aligned}$$

We denote by $\mathcal{B}_\alpha \subset \mathbb{Z}^*_{n^2}$ the set of elements of order $n\alpha$, $\alpha \in \{1, ..., \lambda\}$;

$$\mathcal{B}_\alpha = \{g \in \mathbb{Z}^*_{n^2} \mid ord(g) = n\alpha\}$$

and by $\mathcal{B}$ their disjoint union;

$$\mathcal{B} = \bigcup_{\alpha \in \{1,...,\lambda\}} \mathcal{B}_\alpha \quad .$$

Depending on g, $\mathcal{E}_g$ may feature some interesting properties.

Lemma 3.1. *If the order of g is a non-zero multiple of n, then $\mathcal{E}_g$ is bijective.*

Proof. We have to show that $\mathcal{E}_g$ is $1-1$ and onto.
As $\mid \mathcal{Z}_n \times \mathcal{Z}^*_n \mid = \mid \mathbb{Z}^*_{n^2} \mid = n\varphi(n)$, it suffices to show that $\mathcal{E}_g$ is $1-1$.
Let $g \in \mathcal{B}_\alpha$ and $(x_1, y_1), (x_2, y_2) \in \mathcal{Z}_n \times \mathcal{Z}^*_n$ be s.t.

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

We know that $y_1 \in \mathcal{Z}_n^*$, so its invertible exists, then we have,

$$g^{(x_2-x_1)}\left(\frac{y_2}{y_1}\right)^n \equiv 1 \pmod{n^2} \tag{3.1}$$

and

$$\begin{aligned} y_2, y_1^{-1} \in \mathcal{Z}_n^* &\Rightarrow y_2y_1^{-1} \in \mathcal{Z}_n^* \Rightarrow (y_2y_1^{-1}, n) = 1 \\ &\Rightarrow (y_2y_1^{-1}, n^2) = 1 \Rightarrow y_2y_1^{-1} \in \mathcal{Z}_{n^2}^* \end{aligned} \tag{3.2}$$

It is known that

$$\begin{cases} w^{\lambda} & \equiv 1 \pmod{n} \\ w^{n\lambda} & \equiv 1 \pmod{n^2} \end{cases}, \forall w \in \mathbb{Z}_{n^2}^* \tag{3.3}$$

So,

$$\begin{aligned} (3.1) \ &\Rightarrow g^{\lambda(x_1-x_2)}(y_2y_1^{-1})^{\lambda n} \equiv 1 \pmod{n^2} \\ &\xRightarrow[(3.2)]{(3.3)} g^{\lambda(x_1-x_2)} \equiv 1 \pmod{n^2} \\ &\Rightarrow ord(g) \mid \lambda(x_1-x_2) \Rightarrow n\alpha \mid \lambda(x_1-x_2) \\ &\xRightarrow{(\lambda,n)=1} n \mid x_1 - x_2 \Rightarrow x_1 - x_2 \equiv 0 \pmod{n} \end{aligned} \tag{3.4}$$

This leads to

$$g^{x_1-x_2} \equiv g^0 \equiv 1 \pmod{n^2}$$

It, then, follows that,

$$\begin{aligned} (3.1) \Rightarrow &\left(\frac{y_2}{y_1}\right)^n \equiv 1 \pmod{n^2} \\ \Rightarrow &\left(\frac{y_2}{y_1}\right)^n \equiv 1 \pmod{n} \\ \xRightarrow[Theorem]{Fermat's} &\left(\frac{y_2}{y_1}\right)^n \equiv \frac{y_2}{y_1} \equiv 1 \pmod{n} \end{aligned}$$

We conclude that $x_1 = x_2$ and $y_1 = y_2$, which means $\mathcal{E}_g$ is $1-1$, thus bijective. □

Having defined the function $\mathcal{E}_g$, we now introduce an important notion arising from $\mathcal{E}_g$.

Definition 3.2. Assume that $g \in \mathcal{B}$. For $w \in \mathbb{Z}^*_{n^2}$ we call *n-th residuosity class of w with respect to the g* the unique integer $x \in \mathcal{Z}_n$ for which there exists $y \in \mathcal{Z}^*_n$ s.t.

$$\mathcal{E}_g(x, y) = w.$$

The class of w is denoted $[\![w]\!]_g$.

It is worthwhile noticing the following property.

Lemma 3.2. *Let $w \in \mathbb{Z}^*_{n^2}$ and $g \in \mathcal{B}$. We have that*

$$[\![w]\!]_g = 0 \textit{ if and only if } w \textit{ is a n-th residue modulo } n^2.$$

What is more,

$$\forall w_1, w_2 \in \mathbb{Z}^*_{n^2}\ , \quad [\![w_1 w_2]\!]_g = [\![w_1]\!]_g + [\![w_2]\!]_g \pmod n \tag{3.1}$$

that is, the class function $w \longmapsto [\![w]\!]_g$ is a homomorphism from $(\mathbb{Z}^*_{n^2}, \times)$ to $(\mathbb{Z}_n, +)$, for any $g \in \mathcal{B}$.

Proof. Let $w \in \mathbb{Z}^*_{n^2}$ and $g \in \mathcal{B}$. As $\mathcal{E}_g$ is bijective, we have that

$$[\![w]\!]_g = 0 \Leftrightarrow \mathcal{E}_g(0, y) = w \Leftrightarrow g^0 y^n \equiv w\ (mod\, n^2) \Leftrightarrow w \equiv y^n\ (mod\, n^2)$$

for some $y \in \mathcal{Z}^*_n$.
Now we will prove that the function is an homomorphism.
Take $w_1, w_2 \in \mathbb{Z}^*_{n^2}$ and $x \in \mathcal{Z}_n$ s.t. $[\![w_1 w_2]\!] = x$. Then, for some $y \in \mathcal{Z}^*_n$ we have,

$$\mathcal{E}_g(x, y) = w_1 w_2 \Rightarrow g^x y^n = w_1 w_2 \pmod{n^2} \tag{3.2}$$

But

$$\begin{aligned} w_1 &= \mathcal{E}_g(x_1, y_1)\,, \quad for\ some\ (x_1, y_1) \in \mathcal{Z}_n \times \mathcal{Z}^*_n \\ w_2 &= \mathcal{E}_g(x_2, y_2)\,, \quad for\ some\ (x_2, y_2) \in \mathcal{Z}_n \times \mathcal{Z}^*_n \end{aligned}$$

Which means

$$w_1 = g^{x_1} y_1^n \pmod{n^2} \tag{3.3}$$
$$w_2 = g^{x_2} y_2^n \pmod{n^2} \tag{3.4}$$

Then,

$$\begin{aligned}
(3.2),(3.3),(3.4) &\Rightarrow g^x y^n = g^{x_1} y_1^n g^{x_2} y_2^n \equiv g^{x_1+x_2}(y_1y_2)^n \pmod{n^2} \\
&\Rightarrow g^{\lambda x} y^{\lambda n} \equiv g^{\lambda(x_1+x_2)}(y_1y_2)^{\lambda n} \pmod{n^2} \\
&\Rightarrow g^{\lambda x} \equiv g^{\lambda(x_1+x_2)} \pmod{n^2} \\
&\Rightarrow g^{\lambda x}(1 - g^{\lambda(x_1+x_2-x)}) \equiv 0 \pmod{n^2} \\
&\xRightarrow{g \in \mathbb{Z}^*_{n^2}} 1 - g^{\lambda(x_1+x_2-x)} \equiv 0 \pmod{n^2} \\
&\Rightarrow g^{\lambda(x_1+x_2-x)} \equiv 1 \pmod{n^2} \\
&\Rightarrow ord(g) \mid \lambda(x_1+x_2-x) \\
&\Rightarrow n\alpha \mid \lambda(x_1+x_2-x) \\
&\xRightarrow{(\lambda,n)=1} n \mid x_1+x_2-x \\
&\Rightarrow x \equiv x_1+x_2 \pmod{n} \\
&\Rightarrow [\![w_1w_2]\!]_g = [\![w_1]\!]_g + [\![w_2]\!]_g \pmod{n}
\end{aligned}$$

Thus, $w \longmapsto [\![w]\!]_g$ is a homomorphism.

□

Definition 3.3. We call the problem of computing the class function in base g as the *n-th Residuosity Class Problem of base g*, denoted $Class[n, g]$;

for a given $w \in \mathbb{Z}^*_{n^2}$, compute $[\![w]\!]_g$ from w.

We now state the following useful observations.

Lemma 3.3. *Class[n, g] is RSR over $w \in \mathbb{Z}^*_{n^2}$.*

Proof. We can easily transform any $w \in \mathbb{Z}^*_{n^2}$ into a random instance $w' \in \mathbb{Z}^*_{n^2}$ with uniform distribution.
Take uniformly random $(\alpha, \beta) \in \mathcal{Z}_n \times \mathcal{Z}^*_n$ and let

$$w' \equiv w g^\alpha \beta^n \pmod{n^2}.$$

After $[\![w']\!]_g$ has been computed, one can recover

$$[\![w]\!]_g = [\![w']\!]_g - \alpha \pmod{n}.$$

□

Lemma 3.4. *Class $[n, g]$ is RSR over $g \in \mathcal{B}$, i.e.*

$$Class[n, g_1] \equiv Class[n, g_2]\,, \quad \forall\, g_1, g_2 \in \mathcal{B}$$

Proof. Firstly we show that

$$\forall\, w \in \mathbb{Z}^*_{n^2}\,, \quad g_1, g_2 \in \mathcal{B}\ : \quad [\![w]\!]_{g_1} \equiv [\![w]\!]_{g_2}[\![g_2]\!]_{g_1} \pmod{n} \tag{3.1}$$

Suppose $[\![w]\!]_{g_1} = x_1$, $[\![w]\!]_{g_2} = x_2$ and $[\![g_2]\!]_{g_1} = x_{12}$, then,

$$\mathcal{E}_{g_1}(x_1, y_1) = w \ \Rightarrow\ w \equiv g_1^{x_1} y_1^n \pmod{n^2} \tag{3.2}$$

$$\mathcal{E}_{g_2}(x_2, y_2) = w \ \Rightarrow\ w \equiv g_2^{x_2} y_2^n \pmod{n^2} \tag{3.3}$$

$$\mathcal{E}_{g_1}(x_{12}, y_{12}) = g_2 \ \Rightarrow\ g_2 \equiv g_1^{x_{12}} y_{12}^n \pmod{n^2} \tag{3.4}$$

for some y_1, y_2, $y_{12} \in \mathcal{Z}^*_n$.

$$\begin{aligned}
(3.3), (3.4) &\Rightarrow w \equiv g_1^{x_{12}x_2} y_{12}^{x_2 n} y_2^n \pmod{n^2} \\
&\xRightarrow{(3.2)} g_1^{x_1} y_1^n \equiv g_1^{x_{12}x_2} y_{12}^{x_2 n} y_2^n \pmod{n^2} \\
&\Rightarrow g_1^{\lambda x_1} y_1^{\lambda n} \equiv g_1^{\lambda x_{12}x_2} y_{12}^{\lambda x_2 n} y_2^{\lambda n} \pmod{n^2} \\
&\Rightarrow g_1^{\lambda x_1} \equiv g_1^{\lambda x_{12}x_2} \pmod{n^2} \\
&\Rightarrow \lambda x_1 \equiv \lambda x_{12}x_2 \pmod{ord(g)} \\
&\Rightarrow \lambda x_1 \equiv \lambda x_{12}x_2 \pmod{n\alpha} \\
&\Rightarrow \lambda x_1 \equiv \lambda x_{12}x_2 \pmod{n} \\
&\xRightarrow{(\lambda,n)=1} x_1 \equiv x_{12}x_2 \pmod{n} \\
&\Rightarrow [\![w]\!]_{g_1} \equiv [\![g_2]\!]_{g_1}[\![w]\!]_{g_2} \pmod{n}
\end{aligned}$$

This yields to

$$[\![g_1]\!]_{g_2} \equiv [\![g_2]\!]_{g_1}^{-1} \pmod{n} \tag{3.5}$$

as

$$\begin{aligned}(3.1) &\Rightarrow [\![w]\!]_{g_1}[\![g_1]\!]_{g_2} \equiv [\![w]\!]_{g_2}[\![g_2]\!]_{g_1}[\![g_1]\!]_{g_2} \pmod{n}\\ &\Rightarrow [\![w]\!]_{g_2} \equiv [\![w]\!]_{g_2}[\![g_2]\!]_{g_1}[\![g_1]\!]_{g_2} \pmod{n}\\ &\Rightarrow [\![g_2]\!]_{g_1}[\![g_1]\!]_{g_2} \equiv 1 \pmod{n}\end{aligned}$$

Thus $[\![g_2]\!]_{g_1}$ is invertible $\mod n$.
Suppose that we are given an oracle for $Class[n, g_1]$. Feeding g_2 and w into the oracle respectively, gives $[\![g_2]\!]_{g_1}$ and $[\![w]\!]_{g_1}$ and by straightforward deduction :

$$[\![w]\!]_{g_2} \equiv [\![w]\!]_{g_1}[\![g_1]\!]_{g_2}^{-1} \pmod{n}$$

□

This Lemma essentially means that the complexity of $Class[n, g]$ is independant from g. This enables us to look upon it as a computational problem which purely relies on n.

Definition 3.4. We call *Composite Residuosity Class Problem (CRCP)* the computational problem Class[n] defined as follows:

$$\text{given } w \in \mathbb{Z}_{n^2}^* \text{ and } g \in \mathcal{B}, \text{ compute } [\![w]\!]_g.$$

We now proceed to find out which connections exist between the Composite Residuosity Class Problem and standard number-theoretic problems.

Observe that the set

$$\mathcal{S}_n = \{u < n^2 \mid u \equiv 1 \pmod{n}\}$$

is a multiplicative subgroup of modulo n^2. More specifically, $\mathcal{S}_n \subseteq \mathbb{Z}_{n^2}^*$. This set is exactly the n-th roots of unity which are a subgroup of the n-th residues modulo n^2 which are a multiplicative subgroup of $\mathbb{Z}_{n^2}^*$.

Over $\mathcal{S}_n$ the function L s.t.

$$\forall u \in \mathcal{S}_n,\ L(u) = \tfrac{u-1}{n}$$

is well-defined.
That is because:

(i) Let $u \in \mathcal{S}_n$, then $n \mid L(u)$

(ii) $\forall u \in \mathcal{S}_n \Rightarrow L(u) \in \mathbb{Z}_n$

Lemma 3.5. *For any* $w \in \mathbb{Z}^*_{n^2}$,

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

Proof. We have that $1+n \in \mathcal{B}$.

$$(1+n, n^2) = 1$$

Suppose that $\text{ord}(1+n) = r$, then $(1+n)^r \equiv 1 \pmod{n^2}$.
We have, though, that the n-th roots of unity are the numbers of the form

$$(1+n)^x \equiv 1 + nx \pmod{n^2}.$$

From the above we have that

$$nr \equiv 0 \pmod{n^2} \Rightarrow r = n\alpha, \quad \alpha \in \mathbb{Z}$$

We also have that

$$r \mid \varphi(n^2) \Rightarrow n\alpha \mid n\varphi(n) \Rightarrow \alpha \mid \varphi(n) = (p-1)(q-1) \Rightarrow \alpha \in \{1, ..., \lambda\}$$

So $1+n \in \mathcal{B}_\alpha \subseteq \mathcal{B}$.
As it follows, there exists a unique pair $(c,b) \in \mathcal{Z}_n \times \mathcal{Z}^*_n$ s.t.

$$w \equiv (1+n)^c b^n \pmod{n^2}$$

and $c = [\![w]\!]_{1+n}$ by definition. Then

$$w^\lambda \equiv (1+n)^{\lambda c} b^{\lambda n} \equiv 1 + n\lambda c \pmod{n^2}$$

which yields to

$$\begin{aligned} L(w^\lambda \mod n^2) &= L(1 + nc\lambda \mod n^2) = \frac{1 + nc\lambda - 1}{n} \\ &= \lambda c \equiv \lambda [\![w]\!]_{1+n} \pmod{n} \end{aligned}$$

□

Below they are presented two reductions related to our problem Class$[n]$.

Theorem 3.6. *Class*$[n] \Leftarrow$ *Fact*$[n]$

Proof. Let $g \in \mathbb{Z}^*_{n^2}$. By (3.5) we have that

$$[\![g]\!]_{1+n}^{-1} \equiv [\![1+n]\!]_g \pmod n$$

It applies that

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

From the above, we take that $L(g^\lambda \mod n^2)$ is also invertible $\mod n$. Factoring n leads to the knowledge of λ, therefore $\forall g \in \mathcal{B}$, $\forall w \in \mathbb{Z}_{n^2}^*$,

$$\frac{L(w^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} = \frac{\lambda [\![w]\!]_{1+n}}{\lambda [\![g]\!]_{1+n}} = \frac{[\![w]\!]_{1+n}}{[\![g]\!]_{1+n}} = [\![w]\!]_g \mod n \tag{3.1}$$

□

Theorem 3.7. *Class[n] ⇐ RSA[n,n].*

Proof. Since all the instances of $Class[n, g]$ are computationally equivalent for $g \in \mathcal{B}$ and $1 + n \in \mathcal{B}$, it suffices to show that

$$Class[n, 1+n] \Leftarrow RSA[n, n]$$

Supposing an oracle for $RSA[n, n]$. We know that

$$w \equiv (1+n)^x y^n \pmod{n^2} \quad \text{for some } (x, y) \in \mathcal{Z}_n \times \mathcal{Z}_n^*$$

Therefore we have

$$w \equiv y^n \pmod n$$

and we get y by giving $w \pmod n$ to the oracle.
From the above we get

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

which discloses $x = [\![w]\!]_{1+n}$ as announced.

□

Having set the computational approach of Class[n], we now proceed to the decisional one.

Definition 3.5. We define *D-Class*[n], the *decisional problem associated to* $Class[n]$,

i.e. given $w \in \mathbb{Z}_{n^2}^*, g \in \mathcal{B}$ and $x \in \mathcal{Z}_n$, decide whether $x = [\![w]\!]_g$ or not.

Theorem 3.8. *$CR[n] \equiv D\text{-}Class[n] \Leftarrow Class[n]$.*

Proof. As it is easier to verify a solution than to compute it, it applies that $D\text{-}Class[n] \Leftarrow Class[n]$.
Now, let's move to the left-side equivalence.
($\Rightarrow$) Suppose we want to solve D-Class[n] for $w \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$, $x \in \mathcal{Z}_n$.
Let an oracle solving CR[n], that is, given $z \in \mathbb{Z}^*_{n^2}$, decide whether z is a n-th residue or not. Now consider $wg^{-x} \mod n^2$ and submit it to the oracle.
In case of n-th residuosity we get from Lemma 3.2 that $[\![wg^{-x}]\!]_g = 0$, in other words,

$$wg^{-x} = \mathcal{E}_g(0, y), \text{ for some } y \in \mathcal{Z}^*_n.$$

Then,

$$wg^{-x} \equiv y^n \pmod{n^2} \Rightarrow w \equiv g^x y^n \pmod{n^2} \Rightarrow [\![w]\!]_g = x$$

and the answer to D-Class[n] is "Yes".
In the other case, the answer would be "No".
($\Leftarrow$) Suppose we want to check if $w \in \mathbb{Z}^*_{n^2}$ is a n-th residue.
Let an oracle solving D-Class[n], that is, given $w \in \mathbb{Z}^*_{n^2}$, $g \in \mathcal{B}$, $x \in \mathcal{Z}_n$, decides whether $[\![w]\!]_g = x$. We, then, choose an arbitrary $g \in \mathcal{B}$, ($1 + n$ will do) and submit the triple $(g, w, x = 0)$.
If the oracle responds "Yes", then we have $w \equiv g^0 y^n \equiv y^n \pmod{n^2}$ for some $y \in \mathcal{Z}^*_n$ and w is an n-th residue.
In the other case we get the opposite.

□

To conclude, the computational hierarchy we have been looking for is

$$CR[n] \equiv D\text{-}Class[n] \Leftarrow Class[n] \Leftarrow RSA[n, n] \Leftarrow Fact[n]$$

with serious doubts concerning a potential equivalence, expected possibly between *D-Class*[n] and *Class*[n].

Now, our second intractability hypothesis will be to assume the hardness of the CRCP by making the following conjecture.

Conjecture. There exists no probabilistic polynomial time algorithm that solves *CRCP i.e. Class*[n] is intractable.

Definition 3.6. The hypothesis that $Class[n]$ is intractable is called the *Computational Composite Residuosity Assumption (CCRA).*

As in the $DCRA$, the RSR implies that the validity of $CCRA$ is only conditioned by the choice of n.

Proposition 3.9. *If $DCRA$ is true, then $CCRA$ is true as well.*

Remark. However the converse still remains a challenging question.

Chapter 4

A New Probabilistic Encryption Scheme

Based on the $CRCP$, we now proceed to describe a public-key encryption scheme. The methodology is to employ the function $\mathcal{E}_g$ for encryption and the polynomial reduction $Class[n] \Leftarrow Fact[n]$ for decryption using the factorization as a trapdoor.

Firstly set $n = pq$ as usual and randomly select a base $g \in \mathcal{B}$. This can be done efficiently by employing the following proposition.

Proposition 4.1. *For $g \in \mathbb{Z}_{n^2}^*$, we have that $g \in \mathcal{B}$ if and only if*

$$\gcd\left(L(g^\lambda \mod n^2), n\right) = 1. \tag{4.1}$$

Proof. We know that an element g forms a base if and only if $\mathrm{ord}_{n^2}(g) = n\alpha$, $a \in \{1, \ldots, \lambda\}$. So we can paraphrase the proposition by

$$\mathrm{ord}_{n^2}(g) = n\alpha \Leftrightarrow \gcd\left(L(g^\lambda \mod n^2), n\right) = 1.$$

From now on we write $\gcd\left(L(g^\lambda \mod n^2), n\right)$ as gcd.
By definition of L, we have

$$L(g^\lambda \mod n^2) = \frac{[g^\lambda]_{n^2} - 1}{n}.$$

($\Rightarrow$) Take $n \mid \mathrm{ord}_{n^2}(g)$ and let gcd $= p$, then,

$$\begin{aligned}
&\frac{[g^\lambda]_{n^2} - 1}{n} = pk\,,\ k \in \mathbb{Z}\\
\Rightarrow & g^\lambda - 1 \equiv pkn \pmod{n^2}\\
\Rightarrow & g^\lambda \equiv 1 + pkn \pmod{n^2}\\
\Rightarrow & g^{q\lambda} \equiv (1+pkn)^q \equiv \sum_{j=0}^{q} \binom{q}{j} (pkn)^j\\
& \equiv 1 + \binom{q}{1} pkn + \sum_{j=2}^{q} \binom{q}{j} (pkn)^j\\
& \equiv 1 + pqkn + n^2 \sum_{j=2}^{q} \binom{q}{j} (pkn)^{j-2}\\
& \equiv 1 + kn^2\\
& \equiv 1 \pmod{n^2}
\end{aligned}$$

This shows that

$$\mathrm{ord}_{n^2}(g) \mid \lambda q$$

so

$$n \mid \lambda q \xRightarrow{(n,\lambda)=1} n \mid q, \text{ contradiction.}$$

Following the same procedure for gcd $= q$, we are lead to $n \mid p$, also a contradiction, that is gcd $= 1$.
($\Leftarrow$) Consider gcd $= 1$.
Set $\dfrac{[g^\lambda]_{n^2} - 1}{n} = k\,,\ k < n$ and let $d = \mathrm{ord}_{n^2}(g)$, we take

$$g^\lambda \equiv 1 + kn \pmod{n^2} \Rightarrow g^{p\lambda} \equiv (1+kn)^p \equiv 1 + pkn \pmod{n^2}.$$

It is $n^2 \nmid pkn$, as in different case it must be

$$n^2 \mid pkn \Rightarrow n \mid pk \Rightarrow k = tq,\ \ 0 < t < p.$$

But then it would be $L(g^\lambda \mod n^2) = tq$ which means gcd $= q$, contradiction to our hypothesis.
So that is

$$g^{\lambda p} \not\equiv 1 \pmod{n^2}.$$

Likewise we have

$$g^{\lambda q} \not\equiv 1 \pmod{n^2}.$$

We have previously shown that $g^{\lambda n} \equiv 1 \pmod{n^2}$, so

$$d \mid \lambda n \Rightarrow \lambda n = rd\,,\ r \in \mathbb{N} \Rightarrow \lambda pq = rd.$$

If $q \nmid d$, then $d \mid \lambda p$, which is not possible, as $g^{\lambda p} \not\equiv 1 \pmod{n^2}$, that is $q \mid d$.
Equally $p \mid d$.
It follows that $n \mid d$.

□

Now, consider

$$\begin{array}{lcl} (n, g) & \longrightarrow & \text{public key} \\ (p, q) & \longrightarrow & \text{private key} \end{array}$$

Remark. Using λ as a private key is equivalent to the pair (p, q) as its knowledge leads to calculation of both primes.

The cryptosystem is illustrated in the scheme below called *Scheme 1.*

$\boxed{\text{Encryption}}$

Step 1: Chose plaintext $m < n$

Step 2: Select random $r < n\,,\ (r, n) = 1$

Step 3: Calculate ciphertext $c \equiv g^m r^n \pmod{n^2}$

$\boxed{\text{Decryption}}$

Step 1: Receive ciphertext $c < n^2$

Step 2: Retrieve plaintext $m \equiv \dfrac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n$

Validation & Correctness of the Scheme The validity of the scheme is based on eq. (3.1) as

$$\frac{L(c^\lambda \mod n)}{L(g^\lambda \mod n)} \mod n \equiv [\![c]\!]_g \equiv m \pmod n,$$

which is the plaintext, by definition of $\mathcal{E}_g(c)$.

We can easily see that the encryption function is a trapdoor function with λ as the trapdoor secret. Knowledge of λ leads to knowledge of the factors of

n, that is use of the factorization as a trapdoor, as mentioned earlier. Oneyness lies on the computational problem discussed in the previous section. More specifically,

Theorem 4.2. *Scheme 1 is one-way iff the CCRA holds.*

Proof. Inverting the encryption function we get by definition the $CRCP$, thus if $Class[n]$ is intractable, the scheme is one-way.

□

We now introduce a notion of security that is extremely strong and refers to our cryptosystems. When it is met, there is no point for an adversary to eavesdrop the channel, regardless of what messages are being sent, of what he already knows about the message, and of what goal he is trying to accomplish.

Definition 4.1. Let m given message, $c \in \mathcal{C}$, where $\mathcal{C}$ a set of ciphertexts, and E the encryption function. We call a cryptosystem *semantically secure* if we cannot distinguish whether $c = E(m)$.

Specifically in our scheme, we have that, given message $m < n$, $g \in \mathcal{B}$ and $c \in \mathbb{Z}^*_{n^2}$, we cannot decide whether $c \equiv g^m r^n \pmod{n^2}$ for some $r < n$, $(r, n) = 1$.

Theorem 4.3. *Scheme 1 is semantically secure iff the DCRA holds.*

Proof. ($\Rightarrow$) Suppose the scheme is semantically secure but DCRA does not hold.
Let $m < n$ given message, $c \in \mathbb{Z}^*_{n^2}$ a ciphertext and $g \in \mathcal{B}$. Now consider an oracle solving DCRA that takes $n \in \mathbb{N}$ and $z \in \mathbb{Z}^*_{n^2}$ as input and decides if z is a n-th residue. We feed the oracle with $cg^{-m} \in \mathbb{Z}^*_{n^2}$.
If the oracle answers ”Yes”, then there exists $y \in \mathbb{Z}^*_{n^2}$ s.t.

$$cg^{-m} \equiv y^n \pmod{n^2} \Rightarrow c \equiv g^m y^n \pmod{n^2}$$

that is c is the ciphertext of m and the system is no longer semantically secure.
($\Leftarrow$) Suppose the scheme is not semantically secure, yet the DCRA holds.
Consider an oracle that given $c \in \mathbb{Z}^*_{n^2}$, $m < n$ and $g \in \mathcal{B}$ has as output ”Yes” if $c \equiv g^m y^n \pmod{n^2}$ for some $y \in \mathcal{Z}^*_n$ and ”No” in any other case. We now feed $zg^m \in \mathbb{Z}^*_{n^2}$ to the oracle. If we get ”Yes” as an answer, then we have

$$zg^m \equiv g^m y^n \pmod{n^2} \Rightarrow z \equiv y^n \pmod{n^2}$$

that is z is a n-th residue, contradiction to the assumption that DCRA holds.

□

Below we give a numerical example with small numbers in order to understand better the procedures of the scheme.

Example Take $p = 5$ and $q = 7$, suitable primes as

$$(p-1, q) = (4, 7) = 1$$

$$\text{and}$$

$$(q-1, p) = (6, 5) = 1$$

That is $n = 35$ with

$$\varphi(n) = 24 \text{ and } \lambda(n) = \operatorname{lcm}(4, 6) = 12.$$

We now need to find a base $g \in \mathcal{B}_\alpha$ for some $\alpha \in \{1, \ldots, 12\}$.
Take $g = 2$. This will form a base iff

$$\gcd(L(g^\lambda \mod n^2), n) = 1.$$

We have

$$2^{12} \equiv 421 \pmod{35^2}$$

so

$$L(2^{12} \mod 35^2) = L(421) = \frac{421-1}{35} \equiv 12 \pmod{35}$$

and

$$\gcd(12, 35) = 1.$$

Now let's consider $m = 14 < 35$ a message.

For the encryption, we randomly select $r = 3 < 35$, $(3, 35) = 1$.
The ciphertext would be

$$c \equiv g^m r^n \pmod{n^2} \Rightarrow c \equiv 2^{14} 3^{35} \equiv 538 \pmod{35^2}.$$

For the decryption, we calculate $L(c^\lambda \mod n^2)$ as above, where

$$538^{12} \equiv 981 \pmod{35^2}$$

and we have

$$L(981) = \frac{981-1}{35} \equiv 28 \pmod{35}.$$

To retrieve m we compute

$$\frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} = \frac{L(538^{12} \mod 35^2)}{L(2^{12} \mod 35^2)} = \frac{28}{12} \equiv 28 \cdot 12^{-1} \pmod{35}.$$

Let $k < 35$ s.t. $12k \equiv 1 \pmod{35}$. We get $k = 3$, thus

$$\frac{L(538^{12} \mod 35^2)}{L(2^{12} \mod 35^2)} \equiv 28 \cdot 12^{-1} \equiv 28 \cdot 3 \equiv 14 \pmod{35} \Rightarrow m = 14.$$

Decryption complexity

In order for our scheme to be effective, we need to take into consideration the computational time, principally that of decryption. The decryption function includes computations of L and an inversion $\mod (n)$. Its complexity, though, relies mainly on the calculation of the input of L which is of the form $a^m \pmod{n^2}$ for $a, m, n \in \mathbb{Z}$.

We will first show how to calculate that computational time. We write m in binary:

$$m = b_0 + 2b_1 + 2^2 b_2 + \cdots + 2^k b_k\,, \quad b_i \in \{0,1\}\,,\ i \in \{0,\dots,k\}$$

We then have

$$\bar{a}^m = \bar{a}^{b_0}\bar{a}^{2b_1}\dots\bar{a}^{2^k b_k} = \prod_{0\leq i\leq k}^{b_i=1} \bar{a}^{2^i}$$

The algorithm of doing so is:

```
$P \leftarrow 1$
$q \leftarrow \bar{a}$
while $m > 0$ do
    $b \leftarrow m \mod 2$
    $m \leftarrow m$ div 2
    if $b == 1$ then
        $P \leftarrow Pq$
    end if
    $q \leftarrow q^2$
end while
```

To compute its complexity we have to count the number of calculations and their cost. In every loop of `while`, there are at most 2 complex calculations; $P = Pq$ and/or $q = q^2$. The amount of loops is the length of m in bits, that is $\log m$. The cost of calculations in $\mathbb{Z}_n^*$ and $\mathbb{Z}_{n^2}^*$ is the following:

$$\begin{aligned} \mathbb{Z}_n^* \quad + &\longrightarrow \log n \\ \bullet &\longrightarrow \log^2 n \end{aligned}$$

$$\begin{aligned} \mathbb{Z}_{n^2}^* \quad + &\longrightarrow \log n^2 = 2\log n \\ \bullet &\longrightarrow \log^2 n^2 = 2\log^2 n \end{aligned}$$

Our complex calculations take place in $\mathbb{Z}_{n^2}^*$ and from the above we have that the total cost is

$$2\log m 2\log^2 n = 4\log m\log^2 n.$$

If m and n are the same length, *i.e.* $|m| = |n|$, then the cost becomes

$$4 \log^3 n,$$

that is

$$O(\log^3 n) = O(|n^3|).$$

The rest of calculations in Scheme 1 are negligible to the final result, so it follows that the scheme's complexity is $O(|n^3|)$ *i.e. cubic.*

Homomorphic Properties

Except for the composite residuosity, homomorphic properties is what also makes the cryptosystem special.

Proposition 4.4. *The encryption function is additively homomorphic on $\mathcal{Z}_n$.*

Proof. Let $m_1, m_2 \in \mathcal{Z}_n$ and $r_1, r_2 < n$, $(r_1, n) = (r_2, n) = 1$. We have

$$E(m_1, r_1) \equiv g^{m_1} r_1^n \pmod{n^2}$$

$$E(m_2, r_2) \equiv g^{m_2} r_2^n \pmod{n^2}$$

and now

$$\begin{aligned} E(m_1 + m_2, r_1 r_2) &\equiv g^{m_1+m_2}(r_1 r_2)^n \equiv g^{m_1} r_1^n g^{m_2} r_2^n \\ &\equiv E(m_1, r_1) E(m_2, r_2) \pmod{n^2} \end{aligned}$$

□

This property practically leads us to the following ones.

Proposition 4.5. $\forall m_1, m_2 \in \mathcal{Z}_n$, $r_1, r_2 < n$, $(r_1, n) = (r_2, n) = 1$ *chosen respectively and* $k \in \mathbb{N}$ *it holds:*

(i) $D(E(m_1)E(m_2) \mod n^2) \equiv m_1 + m_2 \pmod{n}$

(ii) $D(E(m)^k \mod n^2) \equiv km \pmod{n}$

(iii) $D(E(m_1)g^{m_2} \mod n^2) \equiv m_1 + m_2 \pmod{n}$

(iv) $\left.\begin{array}{ll} D(E(m_1)^{m_2} & \bmod n^2) \\ D(E(m_2)^{m_1} & \bmod n^2) \end{array}\right\} \equiv m_1 m_2 \pmod{n}$

Proof. Let

$$\begin{aligned} c \equiv E(m,r) &\equiv g^m r^n \pmod{n^2} \Rightarrow [\![c]\!]_g \equiv m \pmod{n} \\ c_1 \equiv E(m_1,r_1) &\equiv g^{m_1} r_1^n \pmod{n^2} \Rightarrow [\![c_1]\!]_g \equiv m_1 \pmod{n} \\ c_2 \equiv E(m_2,r_2) &\equiv g^{m_2} r_2^n \pmod{n^2} \Rightarrow [\![c_2]\!]_g \equiv m_2 \pmod{n} \end{aligned}$$

and we have

(i) $D(E(m_1,r_1)E(m_2,r_2)) \equiv D(E(m_1+m_2, r_1 r_2)) \equiv m_1 + m_2 \pmod{n}$

(ii) $c^k \equiv g^{km} r^{kn} \equiv g^{km}(r^k)^n \pmod{n^2}$

$D(E(m,r)^k) \equiv D(c^k) \equiv [\![c^k]\!]_g \equiv km \pmod{n}$

(iii) $c_1 g^{m_2} \equiv g^{(m_1+m_2)} r_1^n \pmod{n^2}$

$D(E(m_1,r_1)g^{m_2}) \equiv D(c_1 g^{m_2}) \equiv [\![c_1 g^{m_2}]\!]_g \equiv m_1 + m_2 \pmod{n}$

(iv) $c_1^{m_2} \equiv g^{m_1 m_2}(r_1^{m_2})^n \pmod{n^2}$

$D(E(m_1,r_1)^{m_2}) \equiv D(c_1^{m_2}) \equiv [\![c_1^{m_2}]\!]_g \equiv m_1 m_2 \pmod{n}$

We follow the same procedure for $D(E(m_2,r_2)^{m_1})$ as well.

□

Chapter 5

A New One-Way Trapdoor Permutation

One-way trapdoor permutations are very rare cryptographic objects. We proceed to show how to use the trapdoor technique introduced in the previous section to derive a permutation over $\mathbb{Z}^*_{n^2}$.

We have n as usual and g as chosen in eq. (4.1). Let $m_1 \in \mathcal{Z}_n$ and $m_2 \in \mathcal{Z}^*_n$. The permutation scheme is depicted below in Scheme 2 .

$\boxed{\text{Encryption}}$

Step 1: Choose plaintext $m < n^2$

Step 2: Split m as $m = m_1 + nm_2$, for some m_1, m_2 defined as above

Step 3: Apply $\mathcal{E}_g$ to calculate ciphertext $c \equiv g^{m_1} {m_2}^n \pmod{n^2}$

$\boxed{\text{Decryption}}$

Step 1: Receive ciphertext $c < n^2$

Step 2: Calculate $m_1 \equiv \dfrac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \pmod{n}$

Step 3: Calculate $c' \equiv cg^{-m_1} \pmod{n}$

Step 4: Calculate $m_2 \equiv c'^{\,n^{-1} \pmod{\lambda}} \pmod{n}$

Step 5: Retrieve plaintext $m = m_1 + nm_2$

Validation & Correctness of the Scheme Firstly there is:

$$\frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \equiv [\![c]\!]_g \equiv m_1 \pmod{n}.$$

Step 2 is a stepping stone for the process, necessary to recover $m_2^n \mod n$ as

$$c \equiv g^{m_1} m_2^n \pmod{n^2} \Rightarrow c g^{-m_1} \equiv m_2^n \pmod{n} \Rightarrow c' \equiv m_2^n \pmod{n}.$$

Now consider $\alpha \in \mathbb{Z}_n^*$ and let $r = ord_n(\alpha)$. We have $(\lambda, n) = 1$, so I can find $k \in \mathbb{Z}$ s.t.

$$kn \equiv 1 \pmod{\lambda}.$$

From the definition of λ we have $r \mid \lambda$ and then the last equivalence gives us:

$$kn \equiv 1 \pmod{r} \Rightarrow \alpha^{kn} \equiv \alpha \pmod{n}, \quad \forall \alpha \in \mathbb{Z}_n^*$$

Now we take

$$c'^{\,k} \equiv m_2^{kn} \equiv m_2 \pmod{n}$$

But

$$k \equiv n^{-1} \pmod{\lambda},$$

so it follows

$$m_2 \equiv c'^{n^{-1} \pmod{\lambda}} \pmod{n}.$$

We can perceive that step as an RSA decryption with public key exponent $e = n$. The final step recombines the original message m.

The fact that we apply the bijection

$$\begin{aligned} \mathcal{E}_g : \mathbb{Z}_{n^2}^* &\longrightarrow \mathbb{Z}_{n^2}^* \\ m &\longmapsto g^{m_1} m_2^n \end{aligned}$$

is what makes our scheme a permutation over $\mathbb{Z}_{n^2}^*$. Trapdoorness is based on the factorisation of n.

Remark. Note that, by definition of $\mathcal{E}_g$, the cryptosystem requires that $m_2 \in \mathcal{Z}_{n^2}^*$, just like the RSA setting . The case $m_2 \notin \mathcal{Z}_n^*$ either allows to factor n, as it follows that $(m_2, n) = p$ or q, or leads to ciphertext zero for all possible values of m_1. Another consequence of this fact is that our trapdoor permutation cannot be employed *ad hoc* to encrypt short messages *i.e.* messages smaller than n.

Theorem 5.1. *Scheme 2 is one-way if and only if $RSA[n, n]$ is hard.*

Proof. ($\Rightarrow$) Suppose it is one-way and assume $RSA[n,n]$ is easy. We have shown that $Class[n] \Leftarrow RSA[n,n]$, so we compute m_1 in $c \equiv g^{m_1} m_2^n \pmod{n^2}$. Retrieving m_2 requires one more root extraction; $c' \equiv m_2^n \pmod{n}$. Using one more time $RSA[n,n]$, which is considered easy, we get m_2 and with that we have managed to retrieve the message m and invert the Scheme, impossible as it is one-way.
($\Leftarrow$) Suppose $RSA[n,n]$ is hard and assume Scheme is invertible.
Let an oracle which inverts the Scheme, that is input $n, g \in \mathcal{B}, w \mod n^2$ and output $(x,y) \in \mathcal{Z}_n \times \mathcal{Z}_n^*$ s.t. $w \equiv g^x y^n \pmod{n^2}$. Then we can extract n-th roots $\mod n$.
We first query the oracle to give $(\alpha, b) \in \mathcal{Z}_n \times \mathcal{Z}_n^*$ s.t.

$$1 + n \equiv g^{\alpha} b^n \pmod{n^2} \tag{5.1}$$

If

$$w \equiv y_0^n \pmod{n}, \quad y_0 \in \mathcal{Z}_n^* \tag{5.2}$$

we ask the oracle to give $(x,y) \in (\mathcal{Z}_n, \mathcal{Z}_n^*)$ s.t.

$$w \equiv g^x y^n \pmod{n^2} \tag{5.3}$$

Since $1 + n \in \mathcal{B}$, there exists $x_0 \in \mathcal{Z}_n$ s.t.

$$w \equiv (1+n)^{x_0} y_0^n \pmod{n^2} \xRightarrow{(5.1)} w \equiv (g^{\alpha} b^n)^{x_0} y_0^n \equiv g^{\alpha x_0} b^{n x_0} y_0^n \tag{5.4}$$

Let $\alpha x_0 = kn + r$, for some $k, r \in \mathbb{Z}$, then

$$\begin{aligned}
(5.4) \Rightarrow w \equiv g^r g^{kn} b^{nx_0} y_0^n \equiv g^{\alpha x_0 \mod n} (g^k b^{x_0} y_0)^n \pmod{n^2} \\
\xRightarrow{(5.3)} \begin{cases} x \equiv \alpha x_0 \pmod{n} \\ y \equiv g^k b^{x_0} y_0 \pmod{n^2} \end{cases} \\
\Rightarrow \begin{cases} x_0 \equiv x\alpha^{-1} \pmod{n} \\ y_0 \equiv y g^{-k} b^{-x_0} \pmod{n} \end{cases}
\end{aligned}$$

So, by inverting the scheme we managed to compute y_0 which, according to (5.2), is the solution of $RSA[n,n]$, that is $RSA[n,n]$ is easy, contradiction.
□

Example We will use the same data as in the previous section; $p = 5$, $q = 7$, $n = 35$, $\varphi(35) = 24$, $\lambda(35) = 12$ and $g = 2$.
We also have $L(2^{12} \mod 35^2) = 12$ and $12^{-1} \equiv 3 \pmod{35}$.

For this scheme we use $m < n^2$,yet $m > n$, $m = 143$ will do.

For the encryption, we split m as below;

$$143 = 3 + 35 \cdot 4\,,$$

that is $m_1 = 3$ and $m_2 = 4$.

Now we calculate the ciphertext

$$c \equiv 2^3 4^{35} \equiv 142 \pmod{35^2}$$

For the decryption, we calculate

$$L(142^{12} \mod 35^2) = L(36) = \frac{36-1}{35} = 1$$

and then

$$m_1 = \frac{L(142^{12} \mod 35^2)}{L(2^{12} \mod 35^2)} = 1 \cdot 12^{-1} \equiv 3 \pmod{35^2}.$$

Now we set

$$c' \equiv 142 \cdot 2^{-3} \equiv 44 \pmod{35^2}$$

and before moving to m_2 we compute

$$35^{-1} \equiv -1 \pmod{12}.$$

From Step 4 we get that

$$m_2 \equiv 44^{-1} \equiv 4 \pmod{35}.$$

We have finally retrieve

$$m = 3 + 35 \cdot 4 = 143.$$

Decryption complexity

We follow the same procedure as in Scheme 1. The computational time of the decryption depends mainly on Step 2 and Step 4.

The first one will have the complexity computed previously, that is $4\log^3 n$. Now calculations of Step 4 take place in $\mathbb{Z}_n^*$, thus the cost of this operation would be $2\log^3 n$. The total cost is $4\log^3 n + 2\log^3 n = 6\log^3 n$ which leads again to cubic complexity $O(|n^3|)$.

Chapter 6

Almost Reaching Quadratic Complexity

The purpose of this scheme is to decrease the complexity of Scheme 1. This is accomplished by slightly modifying the first one.

Instead of working on $\mathbb{Z}_{n^2}^*$, we restrict ciphertext space to group $\langle g \rangle$ of smaller order by taking advantage of the following extension of eq. (3.1). Assume that $g \in \mathcal{B}_\alpha$ for some $1 \le \alpha \le \lambda$, then,

$$[\![w]\!]_g \equiv \frac{L(w^\alpha \mod n^2)}{L(g^\alpha \mod n^2)} \pmod n\,, \quad \forall w \in \langle g \rangle\,, \tag{6.1}$$

This expression is well-defined:

- *Both* $w^\alpha \mod n^2$ *and* $g^\alpha \mod n^2$ *belong to* S_n*.* Let $g \in \mathcal{B}$, then $\operatorname{ord}_{n^2}(g) = n\alpha$ for some $a \in \{1, \dots, \lambda\}$;

  $$g^{n\alpha} \equiv 1 \pmod{n^2} \Rightarrow g^{n\alpha} \equiv 1 \pmod n \Rightarrow g^\alpha \equiv 1 \pmod n.$$

  We have $w \in \langle g \rangle$, so $w = g^k$ for some $k \in \mathbb{N}_0$. Then

  $$g^\alpha \equiv 1 \pmod n \Rightarrow g^{k\alpha} \equiv 1 \pmod n \Rightarrow w^\alpha \equiv 1 \pmod n.$$

- *Calculating* L *and the fraction.* Now let $g \in \langle 1+n \rangle$ s.t. $g \in \mathcal{B}$. It is

  $$g = (1+n)^r\,, \quad \text{for some } r \in \mathbb{N}_0 \Rightarrow g^\alpha \equiv (1+n)^{r\alpha} \equiv 1 + nr\alpha \pmod{n^2}$$

  $$\Rightarrow L(g^\alpha \mod n^2) = \frac{1 + nr\alpha - 1}{n} = r\alpha \equiv \alpha[\![g]\!]_{1+n} \pmod n.$$

  and also

  $$w \equiv g^k \equiv (1+n)^{rk} \pmod{n^2} \Rightarrow w^\alpha \equiv (1+n)^{rk\alpha} \equiv 1 + nrk\alpha \pmod{n^2}$$

$$\Rightarrow L(w^{\alpha} \mod n^2) = \frac{1 + nrk\alpha - 1}{n} \equiv \alpha[\![w]\!]_{1+n}.$$

We finally have that

$$\frac{L(w^{\alpha} \mod n^2)}{L(g^{\alpha} \mod n^2)} = [\![w]\!]_{1+n}[\![g]\!]_{1+n}^{-1} \equiv [\![w]\!]_g \pmod{n}.$$

The new scheme which we call Scheme 3 , is presented below.

$\boxed{\text{Encryption}}$

$\underline{\text{Step 1}}$: Choose plaintext $m < n$

$\underline{\text{Step 2}}$: Select $r < n$

$\underline{\text{Step 3}}$: Compute ciphertext $c \equiv g^{m+nr} \pmod{n^2}$

$\boxed{\text{Decryption}}$

$\underline{\text{Step 1}}$: Receive ciphertext $c < n^2$

$\underline{\text{Step 2}}$: Retrieve plaintext $m \equiv \dfrac{L(c^{\alpha} \mod n^2)}{L(g^{\alpha} \mod n^2)} \pmod{n}$

Validation & Correctness of the scheme From (6.1) above we get

$$\frac{L(c^{\alpha} \mod n^2)}{L(g^{\alpha} \mod n^2)} \equiv [\![c]\!]_g \equiv m + nr \equiv m \pmod{n}$$

which is the plaintext. Since this time the ciphertext is known to be an element of $\langle g \rangle$, inverting the encryption function does not rely on the *CRCP*, but on a weaker instance. Note that the encryption function's trapdoorness relies on the knowledge of α instead of λ as secret key. More specifically we have the following definitions and theorems.

Definition 6.1. We call *Partial Discrete Logarithm Problem* ($PDL[n, g]$) the computational problem defined as

$$\text{given } w \in \langle g \rangle \text{ and } x \in \mathcal{Z}_n, \text{ compute } [\![w]\!]_g.$$

Theorem 6.1. *Scheme 3 is one-way if and only if $PDL[n,g]$ is hard.*

Proof. ($\Rightarrow$) Suppose Scheme 3 is one-way but PDL is easy.
We have

$$c \in \langle g \rangle \text{ and } c \equiv g^{m+nr} \pmod{n^2}.$$

Since PDL is easy, we can compute

$$[\![c]\!]_g = m + nr.$$

Calculate it $\mod n$ and we get,

$$m + nr \equiv m \pmod{n},$$

which is the plaintext. That contradicts the property of one-way.
($\Leftarrow$) Suppose PDL is hard and Scheme 3 invertible.
Being easy to invert means that given g^{m+nr} we are able to calculate $m + nr$, while g and n are known.
But $m + rn = [\![c]\!]_g$, which leads to the fact that PDL is easy, contradiction.
□

Now, we have shown that Scheme 1 is semantically secure, we want to examine that this property still stands for its modification.

According to the already given definition of semantic security, we will have particularly for this scheme that, given $m < n$, $c \in \mathbb{Z}^*_{n^2}$ a ciphertext, $g \in \mathcal{B}$, we cannot distinguish whether $c \equiv g^{m+nr} \pmod{n^2}$ for some $r < n$.

The fact that we work on the restricted group, occurs another decisional problem defined below, which we will use in our favour.

Definition 6.2. We call *Decisional Partial Discrete Logarithm Problem* ($D - PDL[n,g]$) the following decisional problem:

$$\text{given } w \in \langle g \rangle \text{ and } x \in \mathcal{Z}_n, \text{ decide whether } [\![w]\!]_g = x.$$

Theorem 6.2. *Scheme 3 is semantically secure if and only if $D - PDL[n,g]$ is hard.*

Proof. ($\Rightarrow$) Consider D-PDL$[n,g]$ is easy. Now let $c \in \langle g \rangle$ ciphertext and $x \equiv m \pmod{n} \Rightarrow x = m + nr$, $r \in \mathbb{Z}$, where m is the message.
Since D-PDL$[n,g]$ is easy, we can decide if $[\![c]\!]_g \equiv x \pmod{n}$, that is

$$c \equiv g^x \equiv g^{m+nr} \pmod{n^2}.$$

It follows that the scheme is not semantically secure, contradiction.
($\Leftarrow$) Suppose the scheme is not semantically secure, that is we can identify if $c \equiv g^{m+nr} \pmod{n^2}$, for given ciphertext $c \in \langle g \rangle$ and message $m \in \mathcal{Z}_n$.
Now let $x \in \mathcal{Z}_n$ and we want to check if $x \equiv [\![c]\!]_g \pmod{n}$.
If $x \equiv m \pmod{n}$, then $x = m + nr$, $r \in \mathbb{Z}$ and we have easily solved the D-PDL$[n, g]$, also a contradiction.

□

Proposition 6.3. *We have the following reductions:*

$$PDL[n, g] \Leftarrow Class[n] \text{ and } D - PDL[n, g] \Leftarrow CR[n].$$

Proof.

- $PDL[n, g] \Leftarrow Class[n]$
Suppose we can solve $Class[n]$, that is given $w \in \mathbb{Z}^*_{n^2}$ we can then compute $[\![w]\!]_g \in \mathcal{Z}_n$. But $\langle g \rangle \subseteq \mathbb{Z}^*_{n^2}$, so for $w \in \langle g \rangle$ we can also compute its class, thus $PDL[n, g]$ is solved.
- $D - PDL[n, g] \Leftarrow CR[n]$
Let $w \in \langle g \rangle$ and given $x \in \mathcal{Z}_n$. We want to show that $x \equiv [\![w]\!]_g \pmod{n}$. Consider the oracle that solves CR$[n]$ and takes as input w and x. We have $w \in \langle g \rangle \Rightarrow w \equiv g^r \pmod{n^2}$, $0 \leq r < \text{ord}_{n^2}(g)$ and we can write it as $w \equiv g^r 1^n \pmod{n^2}$, thus we can put it in the oracle.
If $x \equiv r \pmod{n}$, then the oracle's answer is "Yes" and we have also solved D-PDL$[n, g]$.

□

At this point, we introduce our third conjecture.

Conjecture: Under the conditions of Scheme 3, we conjecture that PDL$[n, g]$ and D-PDL$[n, g]$ are intractable.

Now, as in the Scheme 1, we present a numerical example, based on the previous data.

Example As before, we have

$$p = 5,\ q = 7, n = 35,\ \varphi(35) = 24 = 2 \cdot 3 \cdot 4,\ \lambda(35) = 12 \text{ and } g = 2.$$

We also have

$$L(2^{12} \mod 35^2) = 12 \text{ and } 12^{-1} \equiv 3 \pmod{35}.$$

This scheme, though, lies on the knowledge of α, thus we have to compute it. We first need to calculate $\text{ord}_{n^2}(g)$.
We have

$$\varphi(n^2) = n\varphi(n) \Rightarrow \varphi(35^2) = 35 \cdot \varphi(35) = 2^3 \cdot 3 \cdot 5 \cdot 7.$$

It is $\text{ord}_{n^2}(g) \mid \varphi(n^2)$, but we also know that the order should be of the form $n\alpha\,,\ \alpha \in \{1, \dots, \lambda\}$, that is, according to the primitive analysis of $\varphi(35^2)$ and the restrictions of α,

$$\text{ord}_{35^2}(2) = 35\alpha, \text{ where } \alpha \in \{1, 2, 3, 4, 6, 8, 12\}.$$

With calculations, we find that

$$\text{ord}_{35^2}(2) = 35 \cdot 12 = 420,$$

so $\alpha = 12$.
Now consider again $m = 14$ our plaintext and $r = 3$.
<u>*For the encryption*</u> we compute the ciphertext

$$c \equiv g^{m+nr} \pmod{n^2} \Rightarrow c \equiv 2^{14+3\cdot 35} \equiv 263 \pmod{35^2}.$$

<u>*For the decryption*</u> we compute $L(c^\alpha \mod n^2)$.

$$\begin{aligned} L(c^\alpha \mod n^2) &= L(263^{12} \mod 35^2) = L(981 \mod 35^2) \\ &= L(981) = \frac{981-1}{35} \equiv 28 \pmod{35} \end{aligned}$$

We retrieve m by

$$\frac{L(c^\alpha \mod n^2)}{L(g^\alpha \mod n^2)} = \frac{L(263^{12} \mod 35^2)}{L(2^{12} \mod 35^2)} = \frac{28}{12} \equiv 28 \cdot 12^{-1} \equiv 14 \pmod{35}.$$

Decryption complexity

As previously, the most computationally expensive operation is $c^a \mod n^2$ whose complexity is $O(|n^2||a|)$. If g is chosen in such a way that $|a| = \Omega(|n|^\epsilon)$, for some $\epsilon > 0$, then the decryption will only take $O(|n|^{2+\epsilon})$. Scheme 3 is the only public-key cryptosystem based on modular arithmetics whose decryption function features such a property.

Homomorphic Properties

Like in Scheme 1, we have the following propositions.

Proposition 6.4. *The encryption function is additively homomorphic on $\mathcal{Z}_n$.*

Proof. Let $m_1 m_2 \in \mathcal{Z}_n$ and $r_1, r_2 < n$. We have

$$E(m_1, r_1) \equiv g^{m_1+nr_1} \pmod{n^2}$$

$$E(m_2, r_2) \equiv g^{m_2+nr_2} \pmod{n^2}$$

and now

$$\begin{aligned} E(m_1+m_2, r_1+r_2) &\equiv g^{(m_1+m_2)+n(r_1+r_2)} \equiv g^{m_1+nr_1} g^{m_2+nr_2} \\ &\equiv E(m_1, r_1)E(m_2, r_2) \pmod{n^2} \end{aligned}$$

□

This property practically leads us to the following ones.

Proposition 6.5. *$\forall m_1, m_2 \in \mathcal{Z}_n$, $r_1, r_2 < n$ and $k \in \mathbb{N}$ it holds:*

(i) $D(E(m_1)E(m_2) \mod n^2) \equiv m_1 + m_2 \pmod n$

(ii) $D(E(m)^k \mod n^2) \equiv km \pmod n$

(iii) $D(E(m_1)g^{m_2} \mod n^2) \equiv m_1 + m_2 \pmod n$

(iv) $\left.\begin{array}{l} D(E(m_1)^{m_2} \mod n^2) \\ D(E(m_2)^{m_1} \mod n^2) \end{array}\right\} \equiv m_1 m_2 \pmod n$

Proof. Let

$$c \equiv E(m, r) \equiv g^{m+nr} \pmod{n^2} \Rightarrow [\![c]\!]_g \equiv m \pmod n$$

$$c_1 \equiv E(m_1, r_1) \equiv g^{m_1+nr_1} \pmod{n^2} \Rightarrow [\![c_1]\!]_g \equiv m_1 \pmod n$$

$$c_2 \equiv E(m_2, r_2) \equiv g^{m_2+nr_2} \pmod{n^2} \Rightarrow [\![c_2]\!]_g \equiv m_2 \pmod n$$

and we have

(i) $c_1c_2 \equiv g^{(m_1+m_2)+n(r_1+r_2)} \pmod{n^2}$

$D(E(m_1,r_1)E(m_2,r_2)) \equiv D(c_1c_2) \equiv [\![c_1c_2]\!]_g \equiv m_1 + m_2 \pmod{n}$

(ii) $c^k \equiv g^{km+knr} \pmod{n^2}$

$D(E(m,r)^k) \equiv D(c^k) \equiv [\![c^k]\!]_g \equiv km \pmod{n}$

(iii) $c_1g^{m_2} \equiv g^{(m_1+m_2)+nr_1} \pmod{n^2}$

$D(E(m_1)g^{m_2}) \equiv D(cg^{m_2}) \equiv [\![cg^{m_2}]\!]_g \equiv m_1 + m_2 \pmod{n}$

(iv) $c_1^{m_2} \equiv g^{m_1m_2+m_2nr_1} \pmod{n^2}$

$D(E(m_1)^{m_2}) \equiv D(c_1^{m_2}) \equiv [\![c_1^{m_2}]\!]_g \equiv m_1m_2 \pmod{n}$

We follow the same procedure for $D(E(m_2)^{m_1})$ as well.

□

Self-Blinding

Sometimes we would like to provide some information to someone without revealing the real input or the real output. This would be useful in order to prevent attacks. We are able to achieve that with the following interesting property that both Scheme 1 and Scheme 3 have.

Proposition 6.6. *Any ciphertext can be publicly changed into another one without affecting the plaintext:*

$$\forall m \in \mathcal{Z}_n \;\; \textit{and} \;\; r \in \mathbb{N}$$

$$D(E(m,r)r^n \mod n^2) \equiv m \pmod{n}$$

$$\textit{or}$$

$$D(E(m,r)g^{nr} \mod n^2) \equiv m \pmod{n},$$

for Scheme 1 and Scheme 3 respectively.

Proof. We have

- *Scheme 1*
  Let $E(m,r) = g^m r^n$, then

$$D(E(m,r)r^n \mod n^2) \equiv D(g^m(r^2)^n) \equiv m \pmod{n}.$$

- *Scheme 3*
  Let $E(m,r) = g^{m+nr}$, then

$$D(E(m,r)g^{nr} \mod n^2) \equiv D(g^{m+2nr}) \equiv m \pmod{n}.$$

□

Such a property has potential applications in a wide range of cryptographic settings.

Bibliography

[1] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity*, LNCS 1592, Proceedings of EUROCRYPT '99, Springer, pp. 223-238, 1999

[2] J. Talbot, D. Welsh, *Complexity and Cryptography: An introduction*, Cambridge, pp. 125-140, 2006

[3] E. W. Weisstein, *One-Way Function*, MathWorld - A Wolfram Web Resource, n.d.
https://mathworld.wolfram.com/One-WayFunction.html

[4] *One-Way Function*, CRYPTO-IT, 2020
http://www.crypto-it.net/eng/theory/one-way-function.html

[5] J. Patarin, L. Goubin, *Trapdoor One-Way Permutations and Multivariate Polynomials*, LNCS 1334, Proceedings of 7^{th} International Conference of Information and Communications Security, pp. 356-368, 2005

[6] S. Golwasser, M. Bellare, *Lecture Notes in Cryptography*, MIT, pp. 16-22, 2008

[7] *Data Compression and Encryption*, Mumbai University, 2014
https://www.ques10.com/p/7418/what-are-one-way-trap-functions-what-is-their-im-1/

[8] I. Wegener, *Complexity Theory, Exploring the Limits of Efficient Algorithms*, Springer, pp. 43-61, 2005

[9] J. Kleinberg, E. Tardos, *Algorithm Design*, Pearson, Addison-Wesley, pp. 452-454, 462, 2006

[10] D. Angluin, D. Lichtenstein, *Provable Security of Cryptosystems: a Survey*, Yale University, pp. 3-12, 1983

[11] J. Feigenbaum, L. Fortnow, *On the random-self-reducibility of complete sets*, IEEE, 1991

[12] M. Abadi, J. Feigenbaum, J. Kilian, *On Hiding Information from an Oracle*, Journal of Computer and Systems Sciences, vol. 39, no. 1, pp. 42-44, 1989

[13] *Carmichael's Lambda Function*, Brilliant.org, n.d. https://brilliant.org/wiki/carmichaels-lambda-function/

[14] *Carmichael Function*, Wikipedia, 2020 https://en.wikipedia.org/wiki/Carmichael_function

[15] N. Tzanakis, *Lecture Notes in Fundamental Number Theory*, University of Crete, 2019

[16] I. Antoniadis, A. Kontogeorgis, *Finite Fields and Cryptography*, Kallipos, 2015