ÉCOLE NATIONALE SUPÉRIEURE DE TECHNIQUES AVANCÉES

PROJET DE RECHERCHE

Etude du cryptosystème de Paillier

Auteur
Gustavo PACIANOTTO GOUVEIA
pacianotto@ensta.fr
Promotion 2013

Professeur Responsable
Françoise LEVY-DIT-VEHEL
levy@ensta.fr

Tuteur
Patrick CIARLET
ciarlet@ensta.fr

Stage éffectué du 14 mai 2012 au XX/XX/XXXX

ENSTA ParisTech | 32 Boulevard Victor, 75739 Paris
828 Boulevard des Maréchaux, 91762 Palaiseau

25 juin 2012

Résumé

il s'agit d'étudier un système de chiffrement à clef blabalbal

Abstract

The book is on the table balbalbala

Remerciements

Je remercie les pigeons rouges qui sont toujours assis dans ma fenêtre

Table des matières

Chapitre 1

Introduction au système

Le système de Paillier est basée sur les concepts de résiduosité modulo n^2 quand n a exactement deux facteurs premiers p et q, il utilise les particularités de l'anneau $\mathbb{Z}/n^2\mathbb{Z}^*$ pour combiner un message dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ et une valeur aléatoire dans $\mathbb{Z}/n\mathbb{Z}^*$ de tel forme que deux messages égales peuvent être chiffrées différemment, Paillier a aussi démontrée que le problème de déchiffrer les donnés peut être réduit en temps polynomial au problème *RSA* [1] qui est assumée intraitable pour la communauté scientifique. Premièrement on va introduire les fonctions de chiffrement et déchiffrement, nécessaires pour les conclusions sur les groupes cycliques liés, après on les reprendra en prouvant chaque propriété et en montrant la mathématique qui est a derrière.

1.1 La fonction de chiffrement

La fonction de chiffrement d'une mot m reçoit un valeur aléatoire r.

Définition 1. *On utilisera la notation $\mathcal{E}_g$ pour designer la fonction de chiffrement :*

$$\begin{array}{rccl} \mathcal{E}_g : & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}^* & \rightarrow & \mathbb{Z}/n^2\mathbb{Z}^* \\ & (m, r) & \mapsto & g^m r^n \mod n^2 \end{array} \tag{1.1}$$

Le système repose sur le fait que la clé publique est formée par la couple (n, g) et que le déchiffrement du message sans la connaissance de la factorisation de n est intraitable.

[1] trouver la clé privé de l'algorithme *RSA* a partir de la clé publique. c.f. : factoriser la multiplication $n = pq$.

1.2 La fonction de déchiffrement

Le déchiffrement se déroule en utilisant la fonction L_n juste après avoir élevé le mot chiffré a la valeur de la fonction de Carmichael en n, $\lambda(n)$:

$$\begin{array}{rccc} L_m : & \{x \in \mathbb{Z}/m^2\mathbb{Z}^*, x \equiv 1 \mod m\} & \rightarrow & \mathbb{Z}/m\mathbb{Z} \\ & x & \mapsto & \frac{x-1}{m} \end{array} \tag{1.2}$$

Définition 2. *On utilisera la notation D_n pour designer la fonction de dechiffrement :*

$$\begin{array}{rccc} D_n : & \mathbb{Z}/n^2\mathbb{Z}^* & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ & c & \mapsto & \frac{L_n(c^\lambda \mod n^2)}{L_n(g^\lambda \mod n^2)} \mod n \end{array} \tag{1.3}$$

Maintenant qu'on a déjà introduit les fonctions de chiffrement et déchiffrement, on va étudier avec plus de précision chaque aspect mathématique du système et autres simplifications et extensions proposées par des différents chercheurs.

Dans la section 2.2, on reprendra la fonction de déchiffrement en montrant pourquoi elle permet de retrouver le message clair.

Chapitre 2

Étude détaillé du système de Paillier

Dans ce chapitre on regardera plus en détail les hypothèses utilisées dans la analyse effectuée par Pascal Paillier[1] sur le cryptosystème de même nom.

2.1 Une faiblesse du système

Au cours de la familiarisation avec le système de Paillier, on a trouvé, par des méthodes expérimentales, des divergences entre la théorie introduite et le comportement réel des Groupes formés.

Dans la suite, on montrera comment le mauvais choix de p et q peut affaiblir le chiffrement des données.

Lemme 1. *Soient $b \in \mathbb{Z}/n^2\mathbb{Z}^*$ et $a \in \mathbb{Z}/n\mathbb{Z}^*$, si $b \equiv a \mod n$, alors $b^n \equiv a^n \mod n^2$.*

Démonstration. Si $b = a + kn$, $0 \leq k < n$, alors :

$$\begin{aligned} b^n &\equiv \sum_{i=0}^{n} \binom{n}{i} a^{n-i}(kn)^i \\ &\equiv a^n + n \cdot a^{n-1}kn + (kn)^2 \cdot A, A \in \mathbb{Z} \\ &\equiv a^n + n^2 A', A' \in \mathbb{Z} \\ &\equiv a^n \mod n^2 \end{aligned} \tag{2.1}$$

□

Définition 3. *On note $\mathbb{E}_n$ le sous groupe de $\mathbb{Z}/n\mathbb{Z}^*$ formée par :*

$$\mathbb{E}_n = \left\{ z, z^n \equiv 1 \mod n^2 \right\} \tag{2.2}$$

Lemme 2. *$\mathbb{E}_n$ est un sous groupe cyclique de $\mathbb{Z}/n\mathbb{Z}^*$.*

Démonstration. Soient a et b tels que $a, b \in \mathbb{E}_n$, grâce au Lemme 1 on prouve que leur produit $c \equiv ab \mod n$ appartient à $\mathbb{E}_n$ (fermeture) :

$$c^n \equiv (ab)^n \equiv a^n b^n \equiv 1 \cdot 1 \equiv 1 \mod n^2. \tag{2.3}$$

D'où $c \in \mathbb{E}_n$. L'associativité est héritée de $\mathbb{Z}/n\mathbb{Z}^*$, le élément 1 est élément neutre et il reste à prouver que l'inverse dans $\mathbb{Z}/n\mathbb{Z}^*$ fait partie aussi de $\mathbb{E}_n$:

Soient $a \in \mathbb{E}_n$ et d l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}^*$, on prouve que $d \in \mathbb{E}_n$:

$$(a \cdot d)^n = (1+nA)^n = 1 + n \cdot nA + (nA)^2 C \equiv 1 \mod n^2, (A, C) \in \mathbb{Z}^2 \tag{2.4}$$

Comme $(a \cdot d)^n = a^n d^n$ et $a^n \equiv 1 \mod n^2$:

$$d^n = 1 \mod n^2 \tag{2.5}$$

D'où $d \in \mathbb{E}_n$ □

On introduit λ, la fonction de Carmichael[2] :

Définition 4. *Soit p un nombre premier impair et p_i des nombres premiers distincts, $k \in \mathbb{N}^+$, $n = \prod p_i^{e_i}$ la factorisation canonique de n, où $e_i \in \mathbb{Z}$ et $\phi(n)$ la fonction indicatrice de Euler :*

$$\begin{array}{rccl} \lambda : & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & \begin{cases} \phi(n) & \text{si } n = 1, 2 \text{ ou } 4; \\ \frac{\phi(n)}{2} & \text{si } n = 2^k, k > 2; \\ \phi(n) & \text{si } n = p^k; \\ ppcm(\{\lambda(p_i^{e_i})\}) & sinon. \end{cases} \end{array} \tag{2.6}$$

Théorème 1. *$\forall a \in \mathbb{Z}/n\mathbb{Z}^*$, $\lambda(n)$ est le plus petit nombre positif tel que $a^{\lambda}(n) \equiv 1 \mod n$.*

Démonstration. On prouve cas par cas :

- Pour le premier cas ($n = 1$, 2 ou 4) : Les éléments des anneaux $\mathbb{Z}/n\mathbb{Z}^*$ sont $\{1\}$, $\{1\}$ et $\{1, 3\}$ respectivement et il est évident que 1, 1 et 2 sont les plus petits nombres qui conviennent.
- $n = 2^k$, avec $k > 2$: Tout élément a de $\mathbb{Z}/_{2^n}\mathbb{Z}^*$ est de la forme $4l \pm 1, l \in \mathbb{N}$ ($4l$ et $4l + 2$ sont paires), on prouve qu'il est valide pour $k = 3$, on continue par induction et finalement on prouve que $\exists a \in \mathbb{Z}/_{2^k}\mathbb{Z}^*, a^{2^{k-3}} \not\equiv 1 \mod n$:
  - $k = 3,\ \lambda(2^3) = \lambda(8) = 2$
    $\mathbb{Z}/_8\mathbb{Z}^* = \{1, 3, 5, 7\} = \{4l \pm 1\}$:

$$\begin{aligned} a^{\lambda(8)} &= (4l \pm 1)^2 = 16l^2 \pm 8l + 1 \\ &\equiv 1 \mod 8 \end{aligned}$$

– on suppose valide pour $k = m > 2$:

$$a^{2^{m-2}} = 1 + 2^m A, A \in \mathbb{Z} \tag{2.7}$$

– pour $k = m + 1$: en passant 2.7 au carré :

$$\begin{aligned}(a^{2^{m-2}})^2 &= 1 + 2 \cdot 2^m A + 2^{2m} A^2 \\ &\equiv 1 \mod 2^{m+1}\end{aligned} \tag{2.8}$$

2^{k-2} est le plus petit, parce que pour $a = 5$, $5^{2^{k-3}} \not\equiv 1 \mod 2^k$:

$$\begin{aligned}5^{2^{k-3}} &= (1 + 2^2)^{2^{k-3}} \\ &= 1 + 2^{k-1} + A \cdot 2^k k, A \in \mathbb{Z} \\ &\equiv 1 + 2^{k-1} \mod 2^k\end{aligned}$$

– $n = p^k$, p nombre premier impair : Les résultats de Gauss en 1798 permettent de montrer qu'il existent des éléments d'ordre $\phi(n)$ modulo p^k :

> If the greatest common divisor of the numbers t and $p^{n-1}(p-1)$ is e, the congruence $x^t \equiv 1 \mod p^n$ will have e different roots.
>
> *Carl Friedrich Gauss, DA art. 85[3]*

On utilise un raisonnement par contradiction assez simple pour ce cas. On suppose qu'il n'existent pas de nombres d'ordre $\phi(n)$, dans ce cas tout élément est dans $\mathbb{A}$ ou $\mathbb{B}$:

$$\mathbb{A} = \{y, y^{p^{k-1}} \equiv 1 \mod p^k\} \text{ et } \mathbb{B} = \{y, y^{p^{k-2}(p-1)} \equiv 1 \mod p^k\}$$

depuis Gauss, l'ordre de $\mathbb{A}$ et $\mathbb{B}$ est p^{k-1} et $p^{k-2}(p-1)$, par contre $\sharp(\mathbb{A}) + \sharp(\mathbb{B}) = p^{k-2}(2p-1)$ est moins grand que le nombre d'éléments $\phi(n) = p^{k-1}(p-1)$, alors il y a des éléments qui n'appartient pas à $\mathbb{A}$ ou $\mathbb{B}$.

□

Lemme 3. *Soient p et q nombres premiers*[1] *, l'ordre de $\mathbb{E}_{pq}$ est le* $\operatorname{pgcd}(\phi(pq), pq)$.

Démonstration. Soit d l'ordre de E_n, et $\lambda(n)$ la fonction de Carmichael, par définition tout élément de $\mathbb{E}_{pq}$ vaut 1 quand élevé a la n-ième puissance et tout élément de $\mathbb{Z}/n\mathbb{Z}^*$ vaut 1 quand élevé a la $\lambda(n)$-ième puissance :

$$d|n,\ d|\lambda(n) \Rightarrow d|\operatorname{pgcd}(n, \lambda(n)) \tag{2.9}$$

[1]Depuis cette Lemme, p et q sont réservés pour des nombres premières

Or $\lambda(n)$ et $\phi(n)$ ont les mêmes facteurs premiers, et $n = pq$, par conséquence :

$$\text{pgcd}(\lambda(n), n) = \text{pgcd}(\phi(n), n)$$

est vrai pour $n = pq$. On a aussi que :

$$\text{pgcd}(\phi(n), n) \in \{1, p, q, pq\}$$

or $\phi(n) < n$, alors le pgcd ne peut pas prendre la valeur pq. Maintenant, sans perte de généralité, on suppose[2] $q < p$, alors :

$$\text{pgcd}(\phi(n), n) = \text{pgcd}(\phi(pq), pq) = \text{pgcd}((p-1)(q-1), pq)$$

comme les facteurs de $\phi(n)$ sont plus petits que p, le pgcd peut prendre seulement les valeurs 1 et q :

$$\text{pgcd}(\phi(n), n) \in \{1, q\} \tag{2.10}$$

Étant donné que d divise le pgcd précèdent, donc d vaut q si $\mathbb{E}_n \neq \{1\}$, sinon $\mathbb{E}_n = \{1\}$ et d vaut 1. □

Lemme 4. $\text{pgcd}(\phi(pq), pq)) \neq 1$ *si et seulement si* $q|p-1$.

Démonstration. Grâce au résultat 2.10, on a que, soit q divise $\phi(pq)$, soit pq et $\phi(pq)$ n'ont pas de facteur en commun. On analyse les deux possibilités :

- $q \mid \phi(pq)$
$$q \mid (p-1)(q-1) \overset{q \text{ premier}}{\Rightarrow} q \mid p-1$$
- $q \nmid \phi(pq)$
$$q \nmid (p-1)(q-1) \Rightarrow q \nmid p-1$$

□

On introduit la notation $ord_m(a)$ l'ordre de l'élément a sur $\mathbb{Z}/m\mathbb{Z}^*$.

Lemme 5. *Une condition nécessaire à l'existence d'un élément* $a \neq 1, a \in E_n$ *est* $q \mid p-1$.

Démonstration. On suppose l'existence d'un $a \neq 1$ tel que $a^n \equiv 1 \mod n^2$, alors $a^n \equiv 1 \mod p$, ou plus précisément, $(a^p)^q \equiv 1 \mod p$. En appliquant le Petit Théorème de Fermat ($a^p \equiv a \mod p$) :

$$(a^p)^q \equiv a^q \equiv 1 \mod p \Rightarrow ord_p(a) \mid q$$

Étant donné que q est premier et $a \neq 1$:

$$q \mid p-1 \tag{2.11}$$

□

[2] cette supposition sera adopté dans le reste du chapitre.

On utilisera la notation C_m pour designer le groupe cyclique d'ordre m dans la suite.

Lemme 6. *Quand $p \equiv 1 \mod q$, il existe un seul Groupe Cyclique d'ordre q dans $\mathbb{Z}/pq\mathbb{Z}^*$.*

Démonstration. Depuis les résultats de [2, 4] (voir bibliographie), on sait qu'il existe un sous groupe cyclique d'ordre $\lambda(n)$ sur $\mathbb{Z}/pq\mathbb{Z}^*$.

On prouve que le seul sous groupe cyclique d'ordre q est le groupe contenu dans C_λ :

1. C_λ contient un sous groupe cyclique d'ordre q :
   Comme q est diviseur de λ et C_λ est un groupe cyclique, il y a un seul sous-groupe cyclique de C_λ d'ordre q.
2. Dans $\mathbb{Z}/pq\mathbb{Z}^* \setminus C_\lambda$ il n'existe pas de élément d'ordre q :
   Les ordres possibles pour les groupes sont diviseurs de :

$$\begin{aligned} \text{ordre possible } | \frac{\phi}{\lambda} &= \frac{(p-1)(q-1)}{\text{ppmc}(p-1, q-1)} \\ &= \text{pgcd}(p-1, q-1) < q \end{aligned} \tag{2.12}$$

Donc, comme l'ordre possible des autres groupes est limité à $q-1$, il y a un seul sous groupe cyclique d'ordre q dans $\mathbb{Z}/pq\mathbb{Z}^*$ □

Théorème 2. *Un élément a d'ordre q dans $\mathbb{Z}/n\mathbb{Z}^*$ appartient à $\mathbb{E}_n$.*

Démonstration. Premièrement on montre que $a^q \equiv 1 \mod n^2$:

On a $a^q \equiv 1 \mod n$, $a^q \equiv 1 \mod q$. Le Petit Théorème de Fermat donne $a \equiv 1 \mod q$, ou bien $a = qA + 1, A \in \mathbb{Z}$:

$$\begin{aligned} a^q &= \sum_{i=0}^{q} \left(\binom{q}{i} (qA)^i \right) \\ &= 1 + q \cdot (qA) + (qA)^2 C, C \in \mathbb{Z} \end{aligned}$$

d'où $a^q \equiv 1 \mod q^2$.

Maintenant, on montre que $p^2 | (a^n - 1)$, on part de l'hypothèse que $ord_n(a) = q$, ou bien $a^q - 1 = pqA, A \in \mathbb{Z}$:

$$a^{qp} = (pqA + 1)^p = 1 + (pqA)p + (pqA)^2 B, B \in \mathbb{Z}$$

d'où $a^n \equiv 1 \mod p^2$

Finalement, utilisant le Théorème du Reste Chinois, le système

$$\begin{cases} a^n \equiv 1 \mod q^2 \\ a^n \equiv 1 \mod p^2 \end{cases} \tag{2.13}$$

possède seulement une solution $\mod q^2 p^2$, la solution $a^n \equiv 1 \mod n^2$ vérifie le système. Alors, a appartient a $\mathbb{E}_n$. □

Ici, on utilisera la même définition énoncée dans l'article de Paillier :

Définition 5. *Un nombre z est appelé le n-ième résidu modulo n^2 si il existe un nombre y appartient à $\mathbb{Z}/n^2\mathbb{Z}^*$ tel que :*

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

Définition 6. *On gardera le symbole R_n pour le groupe formée par les n-ième résidus modulo n^2.*

Théorème 3. *R_n est un groupe multiplicatif.*

Démonstration. Soient a et b tels que $a, b \in \mathrm{R}_n$, soient a' et b' racines n-ièmes de a et b, on prouvera la fermeture du groupe multiplicatif :

$$c = a \cdot b \equiv (a')^n (b')^n \equiv (a' \cdot b')^n \mod n^2$$

alors, c possède au moins une racine n-ième, le produit $a'b'$.

L'associativité est hérité de $\mathbb{Z}/n^2\mathbb{Z}^*$, le élément 1 est élément neutre et il reste à prouver que l'inverse dans $\mathbb{Z}/n^2\mathbb{Z}^*$ fait partie aussi de R_n :

Soit $a \in \mathbb{Z}_n$, a' une racine n-ième de a et d l'inverse de a' dans $\mathbb{Z}/n^2\mathbb{Z}^*$. Comme $a' \cdot d \equiv 1 \mod n^2$, alors $(a'd)^n = 1 + n^2 C, C \in \mathbb{Z}$ et :

$$a \cdot d^n \equiv (a')^n d^n \equiv (a'd)^n \equiv 1 \mod n^2 \tag{2.14}$$

clairement d^n fait partie de R_n et est l'inverse de a dans ce groupe. □

En revanche, Paillier dit aussi que R_n est d'ordre $\phi(n)$, et si on regarde les résultats ici trouvés, on voit que l'ordre est plutôt $\phi(n)/Ker(\psi)$ où ψ est la fonction :

$$\begin{array}{rccc} \psi(y): & \mathbb{Z}/n\mathbb{Z}^* & \to & \mathbb{Z}/n\mathbb{Z}^* \\ & y & \mapsto & y^n \end{array} \tag{2.15}$$

Avant on a introduit $\mathbb{E}_n$, maintenant, on voit clairement que $\mathbb{E}_n$ est le $Ker(\psi)$ et alors, l'ordre de l'ensemble est $\phi(n)/q$ si et seulement si $p \equiv 1 \mod q$ (avec le Lemme 5, dans la page 7, on a prouvé que elle est nécessaire et avec le théorème 2, dans la page 8, on a prouvé que elle est suffisante). Ce qui préjudicie le isomorphisme de la fonction de chiffrement : plusieurs valeurs aléatoires de y peuvent chiffrer la même valeur x quand appliquées sur le même message.

Un exemple pratique peut montrer comment la choix de la paire (p, q) peut affaiblir le résultat :

$$\begin{aligned} q &= 53 \\ p &= 2 \times 53 + 1 = 107 \\ n &= pq = 5671 \\ n^2 &= 32160241. \end{aligned}$$

On calcule $\mathbb{E}_n$:

$$\begin{aligned}\mathbb{E}_n = \{&1, 160, 266, 319, 584, 637, 690, 743, 796, 849, 955,\\ &1114, 1326, 1432, 1538, 1644, 1697, 1856, 1909, 1962,\\ &2015, 2068, 2174, 2227, 2280, 2333, 2439, 2598, 2651,\\ &2704, 2863, 2916, 3075, 3128, 3340, 3393, 3499, 3764,\\ &4082, 4135, 4294, 4400, 4506, 4612, 4665, 4718, 4824,\\ &4877, 4983, 5354, 5407, 5460, 5513\}\end{aligned}$$

chaque valeur chiffrée correspond a cinquante-trois possibles valeurs de y, e.g. :

Pour $r \in \mathbb{E}_n$:

$$\mathcal{E}_g(1,1) = r^n = 1^n \equiv 160^n \equiv 266^n \equiv \cdots \equiv 1 \mod n^2$$

$$\mathcal{E}_g(x,1) = (g^x)r^n = (g^x)1^n \equiv (g^x)160^n \equiv (g^x)266^n \equiv \cdots \equiv (g^x) \mod n^2$$

On veut chiffrer le message 450, en utilisant $g = n + 1 = 5672$ comme clé publique et supposant qu'on a tiré au hasard 892 pour y :

$$\begin{aligned}\mathcal{E}_{5672}(450, 892) = 5672^{450}(\overbrace{892}^{y})^n &\equiv 5672^{450}(892 \cdot 160)^n \equiv 20893249\\ &\equiv 5672^{450}(892 \cdot 266)^n \equiv 20893249\\ &\equiv 5672^{450}(892 \cdot 319)^n \equiv 20893249\\ &\equiv 5672^{450}(892 \cdot 584)^n \equiv 20893249\\ &\equiv 5672^{450}(892 \cdot 637)^n \equiv 20893249\\ &\vdots\end{aligned}$$

2.1.1 Autres Particularités

Au cours de la caractérisation du groupe $\mathbb{E}_n$, on a trouvée d'autres particularités que restent sans application.

Théorème 4. *$p^i \equiv p \mod n, \forall i \in \mathbb{Z}^+, p \equiv 1 \mod q$, p^i est un point fixe sur le anneau $\mathbb{Z}/n\mathbb{Z}^*$.*

Démonstration.

$$\begin{cases} p^i \equiv 0 \mod p \\ p^i \equiv 1 \mod q \end{cases} \tag{2.16}$$

Du Théorème du Reste Chinois :

$$\begin{aligned} p^i &\equiv 0 \cdot q \cdot q^{p-2} + 1 \cdot p \cdot (p)_q^{-1} \\ &\equiv 0 + 1 \cdot p \cdot 1 \\ &\equiv p \mod n \end{aligned} \tag{2.17}$$

□

2.2 Le Mécanisme de déchiffrement

On déduira les propriétés mathématiques sur lesquelles le système de Paillier est basé.

Lemme 7. *Pour tout $w \in \mathbb{Z}/n^2\mathbb{Z}^*$, on a $w^{n\lambda(n)} \equiv 1 \mod n^2$.*

Démonstration. Soit $w_0 \equiv w \mod n$, comme $w_0^{-1} \equiv w^{-1} \mod n$ alors $w_0 \in \mathbb{Z}/n\mathbb{Z}^*$ et on peut appliquer le Théorème 1 : $w^{\lambda(n)} \equiv w_0^{\lambda(n)} \equiv 1 \mod n$, donc $w^{\lambda(n)}$ est de la forme $1 + nA, A \in \mathbb{Z}$ et on a :

$$w^{\lambda(n)n} = (1 + nA)^n = 1 + n \cdot An + (An)^2 \cdot C, C \in \mathbb{Z}$$

Ou encore $w^{\lambda(n)n} \equiv 1 \mod n^2$. □

TODO: [Rever o titulo do lemma, usar fixo nao fica legal. h eh uma raiz n esima dentro de ZnZ]

Lemme 8. *Pour tout $z \in \mathrm{R}_n$, les racines n-ièmes de z sont de la forme $(h + kn) \mod n^2$ avec h une racine n-ième dans $\mathbb{Z}/n\mathbb{Z}^*$ et $0 \leq k \leq n - 1$.*

Démonstration. On a vu dans le Lemme 1 que si h est une racine n-ième de z, $u \in \mathbb{E}_n$ et $h_u \equiv h \cdot u \mod n$ alors les nombres $(h_u + kn)^n$ sont aussi congrus à z modulo n^2. Ainsi chaque valeur $(h_u + kn)$ est une racine n-ième d'un même z. Alors le nombre de racines n-ièmes de ce type est $\sharp(\mathbb{E}_n) \cdot n = \mathrm{pgcd}(n) \cdot n$. Comme l'ordre de R_n est :

$$\frac{\phi(n)}{\mathrm{pgcd}(n, \phi(n))},$$

le nombre de racines est $\sharp(\mathbb{E}_n) \cdot n \cdot \frac{\phi(n)}{\mathrm{pgcd}(n,\phi(n))} = n\phi(n) = \sharp(\mathbb{Z}/n^2\mathbb{Z}^*)$ alors chaque z dans R_n possède seulement les racines $(h_u + kn)$. C'est-à-dire toutes les racines sont de la forme $(h_u + kn)$. □

On note $\mathcal{B}_\alpha$ l'ensemble d'éléments d'ordre (dans $\mathbb{Z}/n^2\mathbb{Z}^*$) $n\alpha$ et

$$\mathcal{B} = \bigsqcup_{1 \leq \alpha \leq \lambda} \mathcal{B}_\alpha$$

l'union disjointe.

Si $p \not\equiv 1 \mod q$ alors l'ordre de R_n est $\phi(n)$ et par conséquence le nombre de racines d'un $z \in \mathbb{Z}/n^2\mathbb{Z}^*$ dans $\mathbb{Z}/n\mathbb{Z}^*$ est 1. On se place maintenant dans cette situation, on reprendre la fonction de chiffrement et on prouve qu'elle est bijective :

Théorème 5. *Si $g \in \mathcal{B}_\alpha$, alors $\mathcal{E}_g$ est bijective.*

Démonstration. Le nombre de éléments dans $\mathbb{Z}/n^2\mathbb{Z}^*$ est $\phi(n^2) = n\phi(n)$, donc l'anneau a le même nombre d'éléments que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}^*$ et il reste juste à prouver que $\mathcal{E}_g$ est injective.

Soient (x_1, y_1) et (x_2, y_2) des paires dans l'anneau $\mathbb{Z}/n\mathbb{Z}^* \times \mathbb{Z}/n\mathbb{Z}$ tels que $\mathcal{E}_g(x_1, y_1) = \mathcal{E}_g(x_2, y_2)$, c'est-à-dire $g^{x_1} y_1^n \equiv g^{x_2} y_2^n \mod n^2$, comme y_1 et y_2 ont une seule n-ième racine dans $\mathbb{Z}/n\mathbb{Z}^*$, l'équivalence $\frac{y_1^n}{y_2^n} \equiv (\frac{y_1}{y_2} \mod n)^n$ est valide dans $\mathbb{Z}/n^2\mathbb{Z}^*$ et on a :

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

Si on élève les deux côtés à la λ-ième puissance en appliquant le Lemme 7 :

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

et comme $|x_1 - x_2| < n$, $x_1 = x_2$ (si l'ordre de g est n, alors la puissance $x_1 - x_2$ est 0) et $y_1 y_2^{-1} \equiv 1 \mod n^2$ ainsi $y_1 = y_2$. □

Depuis ce théorème on considère que g appartient à $\mathcal{B}$ et on note $[\![w]\!]_g$ l'unique élément x de $\mathbb{Z}/n\mathbb{Z}$ tel que $\exists y \in \mathbb{Z}/n\mathbb{Z}^*$, $\mathcal{E}_g(x, y) = w$. C'est-à-dire si un message a été chiffre avec g, $[\![w]\!]_g$ est ce message.

Lemme 9. *$[\![w]\!]_g = 0$ si, et seulement si, w est un n-résidu modulo n^2.*

Démonstration. Si $[\![w]\!]_g = 0$, alors $w = \mathcal{E}_g(0, y) = y^n$. Dans l'autre côté, si w est un n-résidu modulo n^2, il existe un y tel que $y^n \equiv w \mod n^2$ et comme $g \in \mathcal{B}$ (et l'ordre est multiple de n) le seul x tel que $g^x \equiv 1$ (et par conséquence $g^x y^n \equiv w$) est $x = 0$. □

Propriété 1. *Propriété multiplicative du système : $[\![w_1 w_2]\!]_g = [\![w_1]\!]_g + [\![w_2]\!]_g \mod n$.*

Démonstration. Si $x_1 = [\![w_1]\!]_g$ et $x_2 = [\![w_2]\!]_g$, on a :

$$w_1 w_2 = g^{[\![w_1]\!]} y_1^n \cdot g^{[\![w_2]\!]} y_2^n$$

Alors, avec le même chemin du Théorème 5, $y_1^n y_2^n = (y_1 y_2 \mod n)^n$ et :

$$w_1 w_2 \equiv g^{[\![w_1]\!] + [\![w_2]\!]} (y_1 y_2 \mod n)^n \equiv g^{[\![w_1]\!] + [\![w_2]\!]} (y)^n \mod n^2$$

ainsi il existe un $y = y_1 y_2$ tel que $[\![w_1 w_2]\!]_g = x_1 + x_2 = [\![w_1]\!]_g + [\![w_2]\!]_g$ □

Remarque 1. *Le théorème précédent peut être interprété comme "la fonction $w \mapsto [\![w]\!]_g$ est un morphisme du groupe multiplicatif $(\mathbb{Z}/n^2\mathbb{Z}^*, \times)$ dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$".*

Lemme 10. $[\![w]\!]_{g_1} = [\![w]\!]_{g_2} [\![g_2]\!]_{g_1} \mod n$

Démonstration. Soient r_a,r_b et $r_c \in \mathbb{Z}/n\mathbb{Z}^*$ tels que :

$$\begin{array}{lll} \mathcal{E}_{g_1}([\![w]\!]_{g_1}, r_a) & = g_1^{[\![w]\!]_{g_1}} r_a^n & = w \\ \mathcal{E}_{g_2}([\![w]\!]_{g_2}, r_b) & = g_2^{[\![w]\!]_{g_2}} r_b^n & = w \\ \mathcal{E}_{g_1}([\![g_2]\!]_{g_1}, r_c) & = g_1^{[\![g_2]\!]_{g_1}} r_c^n & = g_2 \end{array} \tag{2.18}$$

La première et la deuxième ont la même valeur w, alors on peut dire que :

$$\mathcal{E}_{g_1}([\![w]\!]_{g_1}, r_a) = \mathcal{E}_{g_2}([\![w]\!]_{g_2}, r_b) = g_2^{[\![w]\!]_{g_2}} r_b^n$$

En remplaçant g_2 par $\mathcal{E}_{g_1}([\![g_2]\!]_{g_1}, r_c)$:

$$\mathcal{E}_{g_1}([\![w]\!]_{g_1}, r_a) = \left(g_1^{[\![g_2]\!]_{g_1}} r_c^n\right)^{[\![w]\!]_{g_2}} r_b^n = \left(g_1^{[\![g_2]\!]_{g_1}[\![w]\!]_{g_2}}\right) \left(r_c^{[\![w]\!]_{g_2}} r_b\right)^n$$

Alors, comme $\mathcal{E}_{g_1}$ est un isomorphisme :

$$\mathcal{E}_{g_1}([\![w]\!]_{g_1}, r_a) = \mathcal{E}_{g_1}([\![g_2]\!]_{g_1}[\![w]\!]_{g_2}, r_c^{[\![w]\!]_{g_2}} r_b)$$

et $[\![w]\!]_{g_1} = [\![g_2]\!]_{g_1}[\![w]\!]_{g_2}$ et $r_a = r_c^{[\![w]\!]_{g_2}} r_b$.

□

On reprend la fonction L introduite dans la Section 1.2 :

Lemme 11. $\forall w \in \mathbb{Z}/n^2\mathbb{Z}^*, L(w^{\lambda(n)} \mod n^2) \equiv \lambda(n)[\![w]\!]_{1+n} \mod n.$

Démonstration. Soient r_a et r_b tels que :

$$\begin{array}{lll} \mathcal{E}_g([\![w]\!]_g, r_a) & = g^{[\![w]\!]_g} r_a^n & = w \\ \mathcal{E}_{n+1}([\![g]\!]_{n+1}, r_b) & = (n+1)^{[\![g]\!]_{n+1}} r_b^n & = g \end{array} \tag{2.19}$$

En remplaçant g par $(n+1)^{[\![g]\!]_{n+1}} r_b^n$ dans la première équation :

$$\mathcal{E}_g([\![w]\!]_g, r_a) = ((n+1)^{[\![g]\!]_{n+1}} r_b^n)^{[\![w]\!]_g} r_a^n = (n+1)^{[\![g]\!]_{n+1}[\![w]\!]_g} (r_b^{[\![w]\!]_g} r_a)^n$$

avec le Théorème 10, $[\![g]\!]_{n+1}[\![w]\!]_g = [\![w]\!]_{n+1}$ et :

$$\mathcal{E}_g([\![w]\!]_g, r_a) = (n+1)^{[\![w]\!]_{n+1}} (r_b^{[\![w]\!]_g} r_a)^n$$

alors, $w^{\lambda(n)}$ vaut :

$$\begin{aligned} w^{\lambda(n)} &= (n+1)^{[\![w]\!]_{n+1}\lambda(n)} (r_b^{[\![w]\!]_g} r_a)^{n\lambda(n)} \\ &= 1 + n \cdot [\![w]\!]_{n+1}\lambda(n) + n^2 \cdot A, A \in \mathbb{Z} \\ &\equiv 1 + n \cdot [\![w]\!]_{n+1}\lambda(n) \mod n^2 \end{aligned}$$

D'où $L\left(w^{\lambda(n)}\right)$ vaut :

$$L\left(w^{\lambda(n)}\right) = \frac{1 + n \cdot [\![w]\!]_{n+1}\lambda(n) - 1}{n} = [\![w]\!]_{n+1}\lambda(n)$$

□

Le lemme précédent est la dernière pièce nécessaire pour comprendre la fonction de déchiffrement. Avec un développement analogue, on peut calculer $L\left(g^{\lambda(n)}\right)$ et changer la valeur w à g.

$$L\left(g^{\lambda(n)}\right) = \frac{1 + n \cdot [\![g]\!]_{n+1}\lambda(n) - 1}{n} = [\![g]\!]_{n+1}\lambda(n)$$

La fonction de déchiffrement devient :

$$D(w) = \frac{L\left(w^{\lambda(n)}\right)}{L\left(g^{\lambda(n)}\right)} = \frac{[\![w]\!]_{n+1}\lambda(n)}{[\![g]\!]_{n+1}\lambda(n)} = \frac{[\![w]\!]_{n+1}}{[\![g]\!]_{n+1}} = [\![w]\!]_g \tag{2.20}$$

Alors, comme $[\![w]\!]_g$ est la valeur x solution de la fonction bijective

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

x est le message contenu dans le mot chiffrée.

2.3 Les clés RSA

Depuis 2009, le standard *FIPS 186-3* sert de référence pour les implantations des protocoles *RSA* et *DSA*. Dans la page 52 du document il sont définies les contraintes pour la génération d'une paire *RSA* (p, q) :

⋮

2. The primes p and q **shall** be selected with the following constraints :
   (a) $(p–1)$ and $(q–1)$ **shall** be relatively prime to the public exponent e.
   (b) The private prime factor p **shall** be selected randomly and **shall** satisfy $\sqrt{2}(2^{\frac{nlen}{2}-1}) \leq p \leq (2^{\frac{nlen}{2}}–1)$, where $nlen$ is the appropriate length for the desired $security\_strength$.
   (c) The private prime factor q **shall** be selected randomly and **shall** satisfy $\sqrt{2}(2^{\frac{nlen}{2}-1}) \leq q \leq (2^{\frac{nlen}{2}}–1)$, where $nlen$ is the appropriate length for the desired $security\_strength$.
   (d) $|p–q| > 2^{\frac{nlen}{2}}–100$.

⋮

National Institute of Standards and Technology.[5]

Les items 2.b et 2.c permettent affirmer que $|p| = |q|$ en bits. Même si le choix entre p et q n'a pas été exprimé dans la description du système, il est dit que le choix doit respecter les recommandations usuelles, celles qui garantissent la relation $p \not\equiv 1 \mod q$, et alors, le cardinal de $\mathbb{E}_n$ est 1 et on a l'isomorphisme désiré.

Théorème 6. *Si p et q ont la même taille en bits, alors, $p \not\equiv 1 \mod q$.*

Démonstration. On suppose que $p \equiv 1 \mod q$:

$$\begin{aligned} p &\equiv 1 \mod q \\ &= 1 + qA, A \in \mathbb{Z} \end{aligned}$$

Comme p et q ont la même taille, A doit être moins grand que 2 ($A = 1$) :

$$p = 1 + q$$

On sait que, sauf 2 et 3, il n'existent pas deux premiers consécutifs. Alors, par absurde, si p et q ont la même taille en bits, $p \not\equiv 1 \mod q$ □

Chapitre 3

Sécurité

Paillier a prouvé que le problème de déchiffrer un message sans la connaissance de la factorisation du nombre n est réductible au problème *RSA,* qui est accepté comme difficile par la communauté scientifique.

Sont définis trois classes de problèmes (le tableau rétrospectif 3.1 est disponible dans la page 17) :

Problème 1. ***CR[n] :*** *décider si un entier est un n-résidu modulo n^2.*

Entrées :

· $x \in \mathbb{Z}/n^2\mathbb{Z}$: l'entier à être vérifié.

Sortie : $vrai$ si $x \in \mathcal{R}_n$ et $faux$ si $x \notin \mathcal{R}_n$.

Problème 2. ***Class[n,g] :*** *trouver $[\![w]\!]_g$ avec $w \in \mathbb{Z}/n\mathbb{Z}$.*

Entrées :

· w : le message à être déchiffre.

Sortie : x la seule valeur dans $\mathbb{Z}/n\mathbb{Z}$ tel que $\exists y \in \mathbb{Z}/n\mathbb{Z}^*$ et $\mathcal{E}_g(x, y) = w$.

Remarque 2. *Dans la section 3.1 il sera introduit la terminologie "auto réductibilité" et il sera prouvé dans le lemme 13 que la difficulté d'un problème de la classe Class[n,g] ne dépend pas directement de g et alors la classe peut être considère Class[n].*

Problème 3. ***D-Class[n] :*** *décider si un entier donné x dans $\mathbb{Z}/n\mathbb{Z}$ vérifie $w = \mathcal{E}_g(x, y)$ avec $y \in \mathbb{Z}/n\mathbb{Z}^*$. C'est-à-dire : Décider si $\exists y \in \mathbb{Z}/n\mathbb{Z}^*$ tel que $w = \mathcal{E}_g(x, y)$.*

Entrées :

· w : le message à être déchiffre.

· x : le message d'origine.

Sortie : $vrai$ si il existe un y comme décrit et $faux$ si il n'existe pas.

Dans les preuves on comparera les problèmes énoncés et les problèmes *RSA[n,n]* et *Fact[n].* Premièrement on les définit :

Problème 4. ***RSA[n,n] :*** *Trouver le seul m qui vérifie $c = m^e \mod n$ avec n le produit de deux premiers de grand taille, $m \in \mathbb{Z}/n\mathbb{Z}$ et e tel que $\text{pgcd}(e, \phi(n)) = 1$.*

Entrées :

· (n, e) : la clé publique formée par n semi premier et $e \in \mathbb{Z}/\phi(n)\mathbb{Z}^*$

· c : le message à être déchiffré.

Sortie : m la racine e-ième de l'entier c dans $\mathbb{Z}/n\mathbb{Z}$.

Problème 5. ***Fact[n] :*** *Factoriser n, la multiplication de deux grands entiers.*

Entrées : Le nombre n suffit pour caractériser le problème.

Sortie : p ou q positifs différents de n et 1 tel que $n = pq$.

TAB. 3.1 – Table des classes de problèmes

Classe	Type[1]	Relations	Cible	Données
CR[n]	D		si $x \in \mathrm{R}_n$	x
Class[n,g]	C	$w = g^m r^n [n^2]$	$[\![w]\!]_g$	w
Class[n]	C	$w = g^m r^n [n^2]$	$[\![w]\!]_g$	w et g
D-Class[n]	D	$w = g^m r^n [n^2]$	si $x = [\![w]\!]_g$	x, w et g
RSA[n,n]	C	$c = m^e [n]$	m	e et c
Fact[n]	C	$n = pq$	p ou q	

Définition 7. *(Réduction des problèmes [6]) Un problème A est dit réductible à un problème B si, pour chaque instance I_a du problème A, il est possible de trouver des instances du problème B auxquelles les résultats permettent de trouver la solution de I_a.*

Par exemple : résoudre une équation de degré 1 (on dit $2x + 1 = 0$) est réductible a résoudre une équation de degré 2 ($(2x + 1)^2 = 0$). La transition d'un problème dans un autre sera notée "transformation", la transformation est faite par une fonction qui implante un tel algorithme, ils sont appelés **fonction de réduction** et **algorithme de réduction** respectivement.

Si il existe une fonction qui permet la transformation d'une instance de A dans une instance de B et une fonction qui permet la traduction des résultats, et les deux fonctions sont calculables en temps polynomial, on dit que le problème est **réductible en temps polynomial**.

3.1 Auto Réductibilité

L'auto réductibilité est une propriété des classes de problèmes. Étant donné une instance d'un problème, si il est possible de la réduire en temps polynomial dans une autre instance aléatoire du même problème, alors la

[1] D pour Problème Décisionnel et C pour Problème de Calcul.

classe est appelé **auto réductible**. Cette propriété garantie que le temps pour la résolution d'une instance dite difficile n'est plus distant que d'un facteur polynomial du temps de solution d'une instance moyenne.

> A random-self reduction maps an arbitrary, worst-case instance x in the domain of f to a set of random instances $y_1, \ldots, y_k$ ...Thus the average-case complexity of f, where the average is taken with respect to the induced distribution on instances y_i, is the same, up to polynomial factors, as the worst-case randomized complexity of f.
>
> *Joan Feigenbaum et Lance Fortnow[7]*

Lemme 12. Class[n,g] *est aléatoirement auto réductible sur* $w \in \mathbb{Z}/n^2\mathbb{Z}^*$.

Démonstration. On pose $w' = wg^{\alpha}\beta^n \mod n^2$, en faisant le choix de α et β uniforme sur le espace $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}^*$, comme $\mathcal{E}_g$ est une bijection (c.f. Théorème 5), w' est distribué uniformément dans $\mathbb{Z}/n^2\mathbb{Z}^*$, finalement $[\![w]\!]_g$ est égal à $[\![w']\!]_g - \alpha$ et alors chaque instance peut être modifié dans n'importe quel autre instance de façon aléatoire et la solution de la première peut être trouve à partir de la deuxième. □

Lemme 13. Class[n,g] *est aléatoirement auto réductible sur* $g \in \mathcal{B}$ *:*

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

Démonstration. Du Théorème 10 on a :

$$[\![w]\!]_{g_1} = [\![w]\!]_{g_2}[\![g_2]\!]_{g_1} \mod n$$

En remplaçant w par g_1, on a :

$$[\![g_1]\!]_{g_1} = [\![g_1]\!]_{g_2}[\![g_2]\!]_{g_1} \mod n$$

Comme $\mathcal{E}_{g_1}(1,1) = g_1$, alors $[\![g_1]\!]_{g_1} = 1$ et $[\![g_1]\!]_{g_2} = [\![g_2]\!]_{g_1}^{-1} \mod n$. Ainsi :

$$[\![w]\!]_{g_1} = [\![w]\!]_{g_2}[\![g_1]\!]_{g_2}^{-1} \mod n$$

et on peut calculer $[\![w]\!]_{g_2}$, le déchiffrement de w sur g_2 avec le calcul de $[\![w]\!]_{g_2}$ et $[\![g_1]\!]_{g_2}$ les déchiffrements de w et g_1 sur g_2, alors il est possible de réduire le problème sur g_1 en ayant lui résolu sur g_2. □

Avec ces deux théorèmes on peut conclure que la difficulté pour chaque instance du système est comparable, et si une solution polynomiale est trouvée pour une instance, on peut trouver des solutions aussi polynomiales pour d'autres instances aléatoires.

3.2 Réductibilité à *RSA[x]*

Théorème 7. Class[n,g] *est réductible à* Fact[n].

Démonstration. Étant donné que la fonction 2.20 permet le déchiffrement avec la valeur de $\lambda(n)$ (en faisant la puissance modulaire, l'algorithme est polynomial), et cette valeur est facilement calculée avec la factorisation de n, un problème de la classe *Class[n,g]* peut être réduit à un autre de la classe *Fact[n]*. □

Théorème 8. Class[n,g] *est réductible à* Fact[n].

Démonstration. On suppose l'existence d'un oracle pour la classe *RSA[n]*, et qu'on a un message m chiffré avec $\mathcal{E}_g$.

Grâce à la bijection on sait que il existent x et y tel que $\mathcal{E}_{n+1}(x, y) = m$, alors on utilise la particularité de la base $n + 1$:

$$w \equiv (1+n)^x y^n \equiv y^n \mod n$$

et on calcule y (avec le oracle *RSA*) tel que $y^n \equiv w \mod n$. On divise w par y^n modulo n^2 et on trouve :

$$R_1 = \frac{w}{y^n} \equiv (1+n)^x \equiv 1 + nx \mod n^2$$

On fait le même raisonnement tel que g était le mot chiffré ($y_2^n \equiv g \mod n$) :

$$R_2 \equiv \frac{g}{y_2^n} \equiv 1 + n[\![g]\!]_{n+1} \mod n^2$$

En appliquant la fonction L sur les deux résultats :

$$\frac{L(R_1)}{L(R_2)} = \frac{[\![w]\!]_{n+1}}{[\![g]\!]_{n+1}} \equiv [\![x]\!]_g \mod n^2$$

on a le déchiffrement de w sur la base g. □

3.3 Moralité

Théorème 9. CR[n] ≡ D-Class[n].

Démonstration. On prouve chaque réductibilité.

- *CR[n]* est réductible à *D-Class[n]* :
  Soit CR_x l'instance (x) du problème *CR*[n], on décrit un algorithme polynomial de réduction de CR_x dans une instance de *D-Class*[n] :
  1. **Transformation de l'instance** : Soit $g \in_R \mathcal{B}$, l'instance $(0, x, g)$ de *D-Class*[n] est : "décider si $\exists y \in \mathbb{Z}/n\mathbb{Z}^*$ tel que $x \equiv g^0 y^n \equiv y^n \mod n^2$".

2. **Solution du problème *D-Class*[n]** : Retourne $vrai$ si il existe y et $faux$ sinon.
3. **Traduction de la solution** : La réponse est directe du pas 2. Le argument est la équivalence entre $g^0 y^n$ et y^n.

– *D-Class[n]* est réductible à *CR[n]* :
Soit $DC_{x,w,g}$ l'instance (x, w, g) du problème *D-Class*[n], on décrit un algorithme polynomial de réduction de $DC_{x,w,g}$ dans une instance de *CR*[n] :

1. **Transformation de l'instance** : Soit $x' \equiv g^{-x} w \mod n^2$, l'instance (x') de *CR*[n] est : "décider si $\exists y \in \mathbb{Z}/n\mathbb{Z}^*$ tel que $x' \equiv y^n \mod n^2$".
2. **Solution du problème *CR*[n]** : Retourne $vrai$ si il existe y et $faux$ sinon.
3. **Traduction de la solution** : La réponse est directe du pas 2. Le argument est que $x = [\![w]\!]_g$ si et seulement si il existe $r \in \mathbb{Z}/n\mathbb{Z}^*$ tel que $w \equiv g^x r^n$, et alors $x' \equiv g^x r^n g^{-x} \equiv r^n \mod n$.

Ainsi les deux classes sont réductibles entre elles, étant équivalentes. □

Depuis les théorèmes 7, 8 et 9 et le fait que *D-Class[n]* est évidemment réductible[1] a *Class[n]*, une hiérarchie peut être écrite en utilisant le symbole "⇐" pour la phrase "est réductible à" :

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

[1] On calcule $[\![w]\!]_g$ et compare avec x.

Chapitre 4

Signature Numérique

Comme les systèmes habituels à clé publique, la signature de Paillier se passe en calculant la valeur hachée h du message m et en "déchiffrant" cette valeur. Pour que ça soit possible le isomorphisme, de la fonction de chiffrement, doit être utilisé complètement, c'est-à-dire la fonction de déchiffrement a une image d'ordre $n\phi(n)$ et la signature doit contenir le "message déchiffré" $[\![h]\!]_g$ et la valeur aléatoire r utilisé pour le chiffrement pour apporter toute l'information nécessaire à calculer h.

Le premier problème posé est la récupération de r. La solution est assez naturel et s'utilise du fait que l'entité qui signe possède λ et peut retrouver la racine n-ième facilement étant donné le résidu.

Comme on sait que il existe r tel que :

$$h \equiv g^{[\![h]\!]_g} r^n \mod n^2$$

En multipliant h par $g^{-[\![h]\!]_g}$, on trouve r^n modulo n^2, comme l'ordre de r divise λ :

$$(r^n)^{(n^{-1} \mod \lambda)} \equiv r^{k\lambda+1} \equiv r \mod n^2, k \in \mathbb{Z}$$

Remarque 3. *La possibilité de trouver $[\![h]\!]_g$ et r existe grâce à la connaissance de la valeur de λ. Il n'existent pas des méthodes efficaces connus pour calculer $[\![h]\!]_g$ et r avec la clé publique (c.f. Chapitre 3 à la page 16).*

Chapitre 5

Implantation

Chapitre 6

Extensions de Damgård–Jurik

TODO: [revisar o francês]

Ivan B. Damgård et Mads J. Jurik ont proposé en 2001 une extension[8] au système de Paillier. Cette extension mettre l'accent sur les systèmes de votation numériques en reposant sur la propriété 1, ils ont proposé aussi l'utilisation des anneaux $\mathbb{Z}/n^{s+1}\mathbb{Z}^*$ où s est plus grand ou égal au 1 présent dans l'original. Sauf la limitation de s moins grand que les nombres premiers p et q, ils ont prouvé que l'ordre de l'élément $n+1$ est n^s, cette propriété ouvre la possibilité de introduire des informations dans $\mathbb{Z}/n^s\mathbb{Z}$ en gardant l'isomorphisme de la fonction $\mathcal{E}$ et la propriété multiplicative déjà présents dans le système de Paillier. Ainsi augmentant le taux d'information dans un message chiffré. Dans Paillier, malgré l'interférence de la valeur aléatoire, la taille des mots chiffrés est deux fois plus grand en octets que l'information transférée. Le système proposé accède à une taux d'information de $1 - 1/s$, clairement, si $s \to \infty$, le taux vaut 1.

L'utilisation de la base $1 + n$ permet aussi le calcul du logarithme modulaire avec complexité $O(s^2)$, l'algorithme utilisé par Damgård et Jurik est décrit en bas.

De manière itérative sur j il récupère le message modulo n^j : Soit m_j le message modulo n^j et t un entière strictement positif, l'égalité $\binom{m_j}{t+1}n^t \equiv \binom{m_{j-1}}{t+1}n^t + n^j \cdot k$ est vrai pour un entière k et permet d'engendrer un algorithme linéaire pour calculer la différence entre m_j e m_{j-1}. L'égalité est facilement prouvé en utilisant le fait que $\binom{m_j}{t+1}$ et $\binom{m_{j-1}}{t+1}$ sont congrus modulo n^j sauf pour un facteur de n^{j-1}, alors, en multipliant les deux côtés par n^t :

$$\binom{m_j}{t+1}n^t \equiv \binom{m_{j-1}}{t+1}n^t + n^{j-1} \cdot k \cdot n^t \equiv \binom{m_{j-1}}{t+1}n^t \mod n^j \tag{6.1}$$

On note $\mathcal{L}$ la fonction :

$$\mathcal{L}(m_{j-1}, j) = \sum_{k=1}^{j} \binom{m_{j-1}}{k} n^{k-1} \mod n^j$$

et on prouve que la différence $L((1+n)^m \mod n^{j+1}) - \mathcal{L}(m_{j-1}, j)$ vaut $m_j - m_{j-1}$

Lemme 14. $L((1+n)^m \mod n^{j+1}) - \mathcal{L}(m_{j-1}, j) \equiv m_i - m_{j-1} \mod n^j$:

Démonstration.

$$\begin{aligned} L &= L((1+n)^m \mod n^{j+1}) \\ &= \frac{1 + \binom{m_{j+1}}{1} n + \cdots + \binom{m_{j+1}}{j} n^j - 1 \mod n^{j+1}}{n} \\ &\equiv \binom{m_j}{1} + \cdots + \binom{m_j}{j} n^{j-1} \mod n^j \\ &\equiv \sum_{k=1}^{j} \binom{m_j}{k} n^{k-1} \mod n^j \end{aligned}$$

Si on soustrait $\mathcal{L}(m_{j-1}, j)$:

$$L - \mathcal{L}(m_{j-1}, j) = \sum_{k=1}^{j} \binom{m_j}{k} n^{k-1} - \sum_{k=1}^{j} \binom{m_{j-1}}{k} n^{k-1} \mod n^j$$

Depuis l'équation 6.1, on peut combiner les sommatoires et annuler les valeurs quand $k > 1$:

$$L - \mathcal{L}(m_{j-1}, j) \equiv \sum_{k=1}^{j} \left(\binom{m_j}{k} n^{k-1} - \binom{m_{j-1}}{k} n^{k-1} \right) \equiv m_j - m_{j-1} \mod n^j$$

□

Maintenant, on sait résoudre le problème de trouver l'exposant quand la base est $n+1$, par contre, la valeur aléatoire qui multiplie la puissance existe encore dans cette schéma et on doit la tenir en compte. On efface r^{n^s} de la même façon qu'on a fait pour Paillier. Comme $\lambda(n^{s+1}) = n^s \lambda(n)$, il faut juste élever le message chiffré à une valeur multiple de λ, Damgård et Jurik ont trouvé une façon créative de utiliser le Lemme 14 même quand on a élevé le message chiffré à λd.

Comme le méthode vu permet de trouver $m \mod n^s$, il faut juste que $\lambda d \equiv 1 \mod n^s$ et on peut s'en servir :

$$\left((1+n)^m r^{n^s}\right)^{\lambda d} \equiv (1+n)^{m\lambda d} \equiv (1+n)^{m \mod n^s} \mod n^{s+1}$$

Algorithme 1 Procédures de logarithme modulaire

function INIT_VALUES($maxS, n$)
  $Cn_0 = 1$
  for $j \leftarrow 1$ to $maxS$ **do**
    $Cn_j = Cn_{j-1} \cdot n$
    $FE_{0,j} = 1$
    for $k \leftarrow 1$ to j **do**
      $FE_{k,j} = FE_{k-1,j} \cdot n \cdot k^{-1} \% Cn_j$
function FIND_NEXT_M(m, c, j)
  $l \leftarrow ((c \% Cn_{j+1}) - 1)/n$
  $b \leftarrow 1$
  for $k \leftarrow 1$ to j **do**
    $b \leftarrow b \cdot (m - k + 1) \% Cn_j$
    $l \leftarrow (l - b \cdot FE_{k,j}) \% Cn_j$
  return l
function LOGARITHM_MOD(c, s)
  $m \leftarrow 0$
  for $j \leftarrow 1$ to s **do**
    $m =$ find_next_m(m, c, j)
  return m

6.1 Votation Numérique

6.1.1 Protocoles Répartis

TODO: [validacao do log de u e v, ver o paper do jurik, pg 23 : Brics-jurik.pdf.Protocol for equality of discrete logs]
TODO: [introduzir a ideia de exponenciacao usando interpolacao de lagrange]
TODO: [falar de Fiat-Shamir]
TODO: [protocolo de prova de escolha "1-out-of-2"]
TODO: [protocolo de multiplicacao mod n^s]

Chapitre 7

Implantation Generique

Bibliographie

[1] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *EUROCRYPT*, pp. 223–238, 1999.

[2] R. Carmichael, *The theory of numbers*. Mathematical monographs, J. Wiley & Sons, inc., 1914.

[3] C. Gauss, *Disquisitiones arithmeticae*. Yale paperbound, Yale University Press, 1966.

[4] E. W. Weisstein, "Modulo multiplication group. From MathWorld–A Wolfram Web Resource." Last visited on 31/05/2012.

[5] P. Gallagher, D. D. Foreword, and C. F. Director, "Fips pub 186-3 federal information processing standards publication digital signature standard (dss)," 2009.

[6] C. Stein, T. Cormen, R. Rivest, and C. Leiserson, *Introduction To Algorithms*. MIT Press, 2001.

[7] J. Feigenbaum and L. Fortnow, "On the random-self-reducibility of complete sets," *SIAM Journal on Computing*, vol. 22, pp. 994–1005, 1991.

[8] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography : Public Key Cryptography*, PKC '01, (London, UK, UK), pp. 119–136, Springer-Verlag, 2001.