Sacs à dos orthogonaux et sacs à dos divisibles

Orthogonal and Divisible Knapsacks

Samy HARARI, Groupe d'Étude du Codage, Université de Toulon et du Var, BP 132, 83957 La Garde Cedex.

Résumé

Ce travail introduit deux nouvelles familles de sacs à dos décodables : les sacs à dos orthogonaux et les sacs à dos divisibles. Ils constituent une généralisation des sacs à dos de Graham Shamir [1]. Pour ces familles, la décodabilité est obtenue par une propriété de divisibilité sur les termes de la suite. Les algorithmes de décodage correspondants sont ensuite exposés ainsi qu'une nouvelle classe de transformations, définie pour chacune des deux familles, à valeurs dans la classe des sacs à dos généraux. Ces transformations rendent ces sacs à dos susceptibles d'être utilisés dans des applications cryptographiques. Deux protocoles de chiffrement à clé publique, utilisant les sacs à dos de chacune des familles sont présentés. Une étude de la cardinalité de la classe des sacs à dos orthogonaux est faite puis une généralisation des sacs à dos orthogonaux et des sacs à dos divisibles permettant d'obtenir de nouvelles classes est esquissée. La solidité cryptographique de chacune des classes est abordée à travers la notion d'amplitude qui est introduite et justifiée. Cette solidité est confirmée par le résultat d'expérimentations.

Mots clés

Chiffrement, sac à dos, algorithme de cryptographie.

Summary

In this work two new families of knapsacks are itroduced. They are orthogonal and divisible knapsacks. They are a generalization of Graham Shamir knapsacks. For those families the decodability is obtained through a divisibility property of each of the terms of the sequence defining them. The corresponding decoding algorithms are presented as well as a new class of transformations, defined on each of the families with values in the class of general knapsacks. These transformation make these knapsacks eligible for use in cryptographic applications. Two publics key cryptographic protocols are presented, one for each class. A study of the cardinality of each class is done, then a generalization to polynomials is sketched. The cryptographic strength of each class is studied through the notion of amplitude of a knapsack which is introduced evaluated and justified. This strength is confirmed through experimental results.

Key words

Enciphering, Knapsacks, Cryptographic algorithm.

1. Introduction

Dans ce travail, après un rappel de la notion de sac à dos décodable, sera introduite celle de cas à dos orthogonal et de sac à dos divisible. Ces sacs à dos sont une généralisation de ceux de Graham Shamir [1] et ont une propriété de divisibilité sur les termes de la suite les définissant qui les rend décodables par un algorithme de complexité linéaire. Une généralisation de la classe de transformations habituellement utilisée pour les sacs à dos est obtenue. Ces transformations s'appliquent, notamment, aux nouveaux sacs à dos introduits.

2. Les sacs à dos décodables

2.1. DÉFINITION

Un problème de sac à dos consiste en la donnée d'une suite (a_i) $1 \leqslant i \leqslant n$ d'entiers positifs et d'un entier c qui

s'écrit sous la forme : $c = \sum_{i=1}^{n} x_i \cdot a_i$ où les x_i valent 0 ou 1 et sont inconnus.

2.2. DÉFINITION

La solution du problème de sac à dos posé par c et (a_i) $1 \leq i \leq n$ est une suite binaire (x_i) $1 \leq i \leq n$ telle que $c = \sum_{i=1}^{n} x_i \cdot a_i$.

2.3. DÉFINITION

Un algorithme de résolution du problème de sac à dos posé par c et (a_i) $1 \leq i \leq n$ est un algorithme permettant de calculer la solution (x_i) $1 \leq i \leq n$ à partir des données du problème.

Si la suite (a_i) n'a pas de structure particulière, il n'existe pas d'algorithme polynomial en n pour résoudre le problème. Les problèmes de sacs à dos sont estimés être NP complets dans le cas général.

2.4. DÉFINITION

Une suite $a_1, \ldots, a_n$ est super croissante si les inégalités suivantes sont vérifiées :

$$a_i > \sum_{j<i} a_j \qquad i = 2, \ldots, n .$$

Si la suite (a_i) est super croissante, il existe un algorithme linéaire pour résoudre tout problème de sac à dos posé à l'aide de (a_i) [2].

3. Les sacs à dos orthogonaux

Soit p un entier premier. Une suite de n entiers $a_1, \ldots, a_n$ définit un sac à dos orthogonal si ses termes vérifient :

$$p^i \mid a_i \text{ et } p^{i+1} \nmid a_i \qquad i = 1, \ldots, n .$$

3.1. LEMME

Soit (a_i) $1 \leq i \leq n$ une suite définissant un sac à dos orthogonal, et $c = \sum_{i=1}^{n} x_i \cdot a_i$ un problème de sac à dos. Il existe un algorithme linéaire pour résoudre ce problème.

3.2. PREUVE

La démonstration utilise la propriété des entiers a_i : a_i est divisible par p^i, et a_i n'est pas divisible par p^{i+1}.

Soit $c = \sum_{i=1}^{n} x_i \cdot a_i$. L'algorithme pour déterminer les x_i est itératif et comporte n étapes.

Pour i allant de 1 à n faire :

1. Si c est divisible par p^i et non divisible par p^{i+1} alors $x_i = 1$ sinon $x_i = 0$.
2. Poser $c = c - x_i \cdot a_i$, et faire $i = i + 1$ itérer.

3.3. EXEMPLE

Soit $p = 11$ et $a_1 = 1288419, a_2 = 1610631, a_3 = 1289739, a_4 = 819896$ et $c = 2899050$. Le nombre c est divisible par 11 et n'est pas divisible par 121. On en déduit que $x_1 = 1$. On pose alors $c = 2899050 - 1288419 = 1610631$. On vérifie qu'il est divisible par 121 et non par 1331 pour en déduire que $x_2 = 1$ et que tous les autres x_i valent 0.

4. Transformations des sacs à dos

Il existe un groupe de transformations, défini sur la classe des sacs à dos décodables, à valeurs dans l'ensemble des sacs à dos sans structure.

Soit (a_i) une suite définissant un sac à dos orthogonal. Soit (k, w, m) un triplet d'entiers vérifiant :

1. PGCD $(w, m) = 1$.
2. $m > \sum_i (a_i + k)$.

La transformation $\Phi_{k,w,m}[(a_i)]$ de la suite (a_i) $1 \leq i \leq n$ est une suite (b_i) $1 \leq i \leq n$ définie par :

$$b_i = (a_i + k) \cdot w \bmod m \qquad i = 1, \ldots, n .$$

L'application inverse est de même nature. Soit w^{-1} l'inverse de $w \bmod m$. On vérifie que $\Phi_{-k \cdot w, w^{-1}, m}[(b_i)] = (a_i)$. Ceci provient des égalités :

$$a_i = (b_i - k \cdot w)\, w^{-1} \bmod m \qquad i = 1, \ldots, n .$$

5. Algorithme de chiffrement à clé publique utilisant des sacs à dos orthogonaux

Le système décrit un protocole entre un utilisateur A qui est destinataire des informations secrètes, détenteur du sac à dos orthogonal lui permettant de déchiffrer les informations, et un utilisateur B qui souhaite chiffrer des informations à l'intention de A à l'aide des données publiques.

5.1. DÉTERMINATION DES DONNÉES PUBLIQUES ET SECRÈTES

L'intervenant A choisit n le nombre de termes de la suite et un nombre premier $p > n$. Il choisit ensuite n entiers aléatoires de même taille $r_i, \ldots, r_n$ non divisibles par p. Il détermine un sac à dos orthogonal (a_i) $1 \leq i \leq n$ par les équations :

$$a_i = p^{n+1} \cdot r_i + p^i \qquad i = 1, \ldots, n .$$

Les entiers r_i sont détruits, les (a_i) sont gardés secrets. A choisit un entier arbitraire k, deux entiers w et m. Les entiers w, m et k sont soumis aux conditions :

1. m est tel que $m > \sum_i (a_i + k)$.

2. $w < m$ et PGCD $(w, m) = 1$.

A garde secret les entiers k, w, m et calcule la suite

$$b_i = (a_i + k) \,.\, w \bmod m \qquad i = 1, \ldots, n$$

qui constitue sa clé publique.

5.2. CHIFFREMENT DES DONNÉES

Lorsque qu'un utilisateur B a des données (x_i) $1 \leqslant i \leqslant n$ à transmettre secrètement à A, il calcule

$$c = \sum_{i=1}^{n} x_i \,.\, b_i$$

qu'il émet sur la ligne de communication.

5.3. DÉCHIFFREMENT DES DONNÉES

Le destinataire A calcule

$$d = w^{-1} \,.\, c \bmod m \,.$$

La quantité d satisfait à l'équation

$$d = \sum_{i=1}^{n} x_i \,.\, a_i + \text{poids } (x) \,.\, k \bmod m \,.$$

La quantité poids (x) qui est égale au nombre de coefficients (x_i) non nuls est inconnue de A. De plus elle satisfait aux inégalités

$$0 \leqslant \text{poids } (x) \leqslant n \,.$$

l'algorithme de décodage, utilise par A, comporte deux parties.

5.4. ALGORITHME POUR RETROUVER POIDS (x)

Il se sert du fait que $p > n$ et que PGCD $(k, p) = 1$. Pour tout entier μ avec $0 < \mu < n$, la quantité $d - \mu \,.\, k$ est divisible par p si et seulement si $\mu =$ poids (x). L'algorithme qui en découle est le suivant :

Tant que PGCD $(d, p) = 1$ *faire*
$d = d - k$
fin .

Cet algorithme comporte au plus n itérations et, en moyenne, trouve la bonne valeur de d en $n/2$ itérations.

Une fois déterminée la bonne valeur de d, A applique l'algorithme de décodage des sacs à dos orthogonaux décrit en 3.1 pour retrouver la suite (x_i) $1 < i \leqslant n$.

5.5. REMARQUE

Ces transformations s'appliquent aussi aux sacs à dos super croissants et permettent d'obtenir des sacs à dos non super croissants qui sont décodables.

5.6. ÉNUMÉRATION DES SACS A DOS ORTHOGONAUX

Parmi les méthodes d'énumération des sacs à dos en général, et des sacs à dos orthogonaux en particulier, on peut retenir celle qui consiste à compter les suites d'un certain type en fonction du nombre de ses éléments et d'un majorat de ses termes. Soit $S(n, r)$ resp. $O(n, r)$ resp. $C(n, r)$ la cardinalité de l'ensemble des suites à n termes majorés par 2^r définissant des sacs à dos resp. des sacs à dos orthogonaux resp. des sacs à dos super croissants.

La quantité $S(n, r)$ est majorée par la cardinalité de l'ensemble des n-uples d'éléments inférieurs à 2^r. On a donc

$$S(n, r) < 2^{r \cdot n} \,.$$

La quantité $O(n, r)$ peut être calculée de manière précise. En effet si (a_i) $1 \leqslant i \leqslant n$ est une suite définissant un sac à dos orthogonal, les $\log_2 p \,.\, n$ bits de poids faible du développement binaire de chacun des termes sont connus. Les bits restnats du développement binaire de chacun des termes peuvent être choisis arbitrairement. Ceci entraîne que

$$O(n, r) = 2^{n \cdot (r - \log_2 p \,.\, n)} \,.$$

Pour n fixé on a

$$O(n, r)/S(n, r) \to 2^{-n^2 \log_2 p} \,.$$

L'expression analytique de la cardinalité des sacs à dos super croissants est difficile à obtenir. Toutefois pour des valeurs particulières la valeur de $S(n, r)$ s'obtient à l'aide de programmes informatiques de comptage. Les valeurs calculées portent à croire que le nombre de sacs à dos super croissants est en $O(r^2)$ et donc, qu'asymptotiquement,

$$O(n, r)/S(n, r) \to 0 \,.$$

6. Les sacs à dos orthogonaux généralisés

Soit p un entier premier. Une suite de n entiers $a_1, \ldots, a_n$ définit un sac à dos orthogonal généralisé s'il existe deux entiers e et f, f vérifiant $f \geqslant \log_2 n$, tels que la suite $a'_1, \ldots, a'_n$ qui lui est associée par l'opération $a'_i = [a_i / p^e]$ $i = 1, \ldots, n$ vérifie :

$$p^{i+f} \mid a'_i \text{ et } p^{i+f+1} \nmid a'_i \qquad i = 1, \ldots, n \,.$$

6.1. CONSTRUCTION DE SAC A DOS ORTHOGONAUX GÉNÉRALISÉS

Soient $r_1, \ldots, r_n$ des entiers choisis aléatoirement et $l_1, \ldots, l_n$ des entiers également choisis aléatoirement, tous inférieurs à p^e. La suite (a_i) définie par

$$a_i = r_i \cdot p^{n+f+e} + p^{i+f+e} + l_i \quad 1 \leqslant i \leqslant n$$

est une suite définissant un sac à dos orthogonal généralisé.

6.2. EXEMPLE

Soit $p = 5$, $n = 4$, $f = 1$, $e = 3$. En prenant les r_i constants $r_i = 1$ $1 \leqslant i \leqslant n$ et les l_i aléatoires positifs et inférieurs à 125, on obtient la suite : 391267, 393779, 406348, 468861 qui est très faiblement croissante.

6.3. REMARQUE

Ceci est une généralisation de la méthode de construction des sacs à dos de Graham Shamir qui est obtenue avec $p = 2$.

6.4. DÉCODAGE DES SACS A DOS ORTHOGONAUX GÉNÉRALISÉS

Soit (a_i) une suite définissant un sac à dos orthogonal généralisé, et $c = \sum_{i=1}^{n} x_i \cdot a_i$ un problème de sac à dos. L'algorithme linéaire pour résoudre ce problème est dérivé de l'algorithme de décodage des sacs à dos orthogonaux. En effet il suffit de considérer la suite $a'_i = a_i/p^{e+f}$ $1 \leqslant i \leqslant n$ et $c' = c/p^{e+f}$. Les entiers a'_i forment un sac à dos orthogonal et jouissent donc de la propriété suivante : a'_i est divisible par p^i et a'_i n'est pas divisible par p^{i+1}. On a de même $c' = \sum_{i=1}^{n} x_i \cdot a'_i$. La solution x_i du problème de sac à dos orthogonal généralisé de départ est identique à celle du problème posé par c' et la suite (a'_i). Il suffit donc d'appliquer l'algorithme de résolution des sacs à dos orthogonaux à ce nouveau problème pour obtenir la solution (x_i) $1 \leqslant i \leqslant n$.

7. Les sacs à dos divisibles

7.1. DÉFINITION

Soient $q_1, \ldots, q_n$ n entiers tels que PGCD $(q_i, q_j) = 1$ pour $i \neq j$. Soit $P = \prod_{i=1}^{n} q_i$. La suite $a_i = P/q_i$ $i = 1, \ldots, n$ définit un sac à dos divisible.

7.2. LEMME

Soit (a_i) $1 \leqslant i \leqslant n$ une suite d'entiers définissant un sac à dos divisible, et $c = \sum_{i=1}^{n} x_i \cdot a_i$ un problème de sac à dos où les coefficients x_i ne sont pas tous égaux à 1. Il existe un algorithme linéaire pour résoudre ce problème.

7.3. PREUVE

La démonstration utilise le fait que, pour chaque indice i, l'entier c est divisible par q_i si et seulement si le coefficient $x_i = 0$.

L'algorithme pour déterminer les x_i est itératif et comporte n étapes.

Pour i allant de 1 à n faire :

Calculer $r = c$ modulo q_i. Si $r = 0$ alors $x_i = 0$ sinon $x_i = 1$ incrémenter i.

7.4. EXEMPLE

Prenant $n = 5$, et pour les q_i les entiers {29, 31, 37, 43, 47} on obtient la suite : {2318087, 2168533, 1816879, 1563361, 1430309 } qui définit un sac à dos divisible.

7.5. TRANSFORMATION DES SACS A DOS DIVISIBLES

Les transformations de la famille $\Phi(k, w, m)$ avec les conditions :

1. PGCD $(a_i + k, P) = 1$ $i = 1, \ldots, n$
2. $m > \sum_i (a_i + k)$
3. PGCD $(w, m) = 1$

appliquées aux sacs à dos divisibles ont pour résultat des sacs à dos décodables. En effet soit $b_i = (a_i + k) \cdot w \bmod m$ et $c = \sum_{i=1}^{n} x_i \cdot a_i$. Alors la quantité $d = c \cdot w^{-1} \bmod m$ satisfait à l'équation :

$$d \bmod m = \sum_{i=1}^{n} x_i (a_i + k) \bmod m =$$

$$= \sum_{i=1}^{n} x_i a_i + \text{poids } (x) \cdot k \bmod m$$

et dans ces conditions l'équation

$$d - \mu \cdot k = \sum_{i=1}^{n} x_i a_i \quad 0 \leqslant \mu \leqslant n$$

n'a de solution que si $\mu = \text{poids } (x)$.

7.6. CRYPTOGRAPHIE A CLÉ PUBLIQUE ET SACS A DOS DIVISIBLES

Le système décrit un protocole entre un utilisateur A qui est destinataire des informations secrètes, détenteur du sac

à dos divisible lui permettant de déchiffrer les informations, et un utilisateur B qui aura chiffré des informations à l'intention de A à l'aide des données publiques.

7.7. DÉTERMINATION DES DONNÉES PUBLIQUES ET SECRÈTES

A choisit n entiers premiers deux à deux $q_1, q_2, \ldots, q_n$ tels que $q_i > n$ $i = 1, \ldots, n$. Soit $P = \prod_{i=1}^{n} q_i$. Il détermine un sac à dos divisible (a_i) $1 \leqslant i \leqslant n$ par les équations :

$$a_i = P/q_i \quad i = 1, \ldots, n .$$

Les entiers (a_i) sont gardés secrets. A choisit trois entiers k, w, m satisfaisant aux conditions de **7.5**. A les garde secrets et calcule la suite

$$b_i = (a_i + k) . w \bmod m \quad i = 1, \ldots, n$$

qui cnstitue sa clé publique.

7.8. CHIFFREMENT DES DONNÉES

Lorsqu'un utilisateur B a des données (x_i) $i = 1, \ldots, n$ à transmettre secrètement à A, il calcule

$$c = \sum_{i=1}^{n} x_i . b_i$$

qu'il émet sur la ligne de communication.

7.9. DÉCHIFFREMENT DES DONNÉES

Le destinataire A calcule $d = w^{-1} . c \bmod m$. La quantité d satisfait à l'équation

$$d = \sum_{i=1}^{n} x_i . a_i + \text{poids } (x) . k .$$

L'entier poids (x) est inconnu de A et vérifie $0 \leqslant$ poids $(x) \leqslant n$. A doit d'abord déterminer cet entier, avant de pouvoir reconstituer la suite (x_i) en effectuant le décodage du sac à dos divisible. A cette fin A utilise l'algorithme ci-après, qui utilise les propriétés de divisibilité des termes de l'équation :

tant que PGCD $(d, P) = 1$
faire $d = d - k$
fin

Cet algorithme n'aboutit pas si tous les coefficients du sac à dos sont égaux à 1. Pour traiter cette éventualité il faut, au préalable, comparer d à $\sum_i a_i + n . k$. S'il y a égalité le déchiffrement est achevé puisque tous les coefficients x_i sont égaux à 1.

Une fois obtenue la bonne valeur de d, A applique l'algorithme de décodage des sacs à dos divisibles exposé en **7.3** pour retrouver les x_i $i = 1, \ldots, n$.

7.10. GÉNÉRALISATION AUX POLYNOMES

La définition des sacs à dos divisibles se généralise immédiatement aux polynômes à coefficients entiers. Dans ce cas les entiers sont remplacés par des polynômes, les propriétés de divisibilité et de calcul de PGCD étant appliquées aux polynômes à la place des entiers. Il en découle l'algorithme correspondant de chiffrement à clé publique.

8. Solidité cryptographique

Les sacs à dos orthogonaux et les sacs à dos divisibles présentés sont susceptibles d'être soumis à des méthodes de cryptanalyse. La plus universelle [4] consiste à associer à un problème de sac à dos un réseau. Les coefficients d'un vecteur particulier de norme courte de ce réseau constitue la solution au problème initial. Un algorithme de réduction de réseau (à savoir l'algorithme LLL noté encore L^3) est alors appliqué. La complexité de celui-ci est une fonction polynomiale du nombre d'éléments de la suite.

Soit (a_i) $1 \leqslant i \leqslant n$ une suite définissant un sac à dos, et c un problème de sac à dos posé à l'aide de cette suite. Considérons le réseau Λ de dimension $n + 1$ dans R^{n+1} ayant pour base les vecteurs $(\vec{e}_1, a_1), \ldots, (\vec{e}_i, a_i), \ldots, (\vec{e}_n, a_n), (\vec{0}, -c)$ où $\vec{e}_i$ désigne le i-ième vecteur de la base canonique de R^n. Ce réseau Λ admet pour vecteur court un vecteur $\vec{v}$, de norme voisine de $\sqrt{n}$ dont les coefficients sont la solution au problème posé.

L'algorithme de réduction convergera vers un vecteur qui n'est pas une solution au problème posé si, a priori, le réseau Λ comporte d'autres vecteurs de petite norme qui ne correspondent pas à une solution du problème. Cette situation se produit pour le réseau si la suite (a_i) $1 \leqslant i \leqslant n$ possède les propriétés suivantes :

1. L'ensemble des combinaisons linéaires à coefficient 0,1 de la suite (a_i) $1 \leqslant i \leqslant n$ est contenu dans un intervalle de petite longueur ;

Dans ce cas, si c' est un autre problème de sac à dos, $c' = \sum_{i=1}^{n} x'_i . a_i$, posé avec la même suite (a_i) $1 \leqslant i \leqslant n$, la quantité $c - c'$ est petite en valeur absolue et le vecteur $\vec{v} = \left(\sum_{i=1}^{n} (x_i - x'_i) . \vec{e}_i, c - c' \right)$, qui appartient au réseau, est alors de petite norme.

2. Il existe des combinaisons linéaires $\sum_{i=1}^{n} \lambda_i . a_i = 0$, avec les coefficients λ_i qui sont tous petits en valeur absolue. Ces combinaisons linéaires sont associées aux vecteurs $\vec{v} = \left(\sum_{i=1}^{n} \lambda_i . \vec{e}_i, 0 \right)$ du réseau qui sont aussi de petite norme.

L'algorithme de réduction converge vers un vecteur de petite norme. Si le réseau contient plusieurs vecteurs de ce

type, la probabilité de convergence de l'algorithme vers l'un d'entre eux est égale à l'inverse de leur nombre. Plus le nombre de vecteurs de norme petite ne correspondant pas au problème de sac à dos est élevé, plus faible sera la probabilité que l'algorithme L^3 converge vers un vecteur qui donne la solution désirée par le cryptanalyste. Ainsi tous les sacs à dos ne sont pas équivalents du point de vue de l'algorithme L^3 appliqué en cryptanalyse. Ceci conduit à définir l'amplitude d'un sac à dos pour caractériser de telles situations.

8.1. AMPLITUDE D'UN SAC A DOS

Soit (a_i) $1 \leqslant i \leqslant n$ une suite croissante définissant un sac à dos. L'amplitude $A[(a_i)]$ de cette suite est définie par

$$A[(a_i)] = \frac{\sum_{i=1}^{n} a_i - a_1}{a_1} = \frac{\sum_{1=2}^{n} a_i}{a_1}.$$

Plus l'amplitude d'une suite est faible, plus le réseau associé sera susceptible de contenir des vecteurs de norme courte, qui ne sont pas des solutions au problème posé par le cryptanalyste. La résistance d'un tel sac à dos à un algorithme de réduction dans les réseaux, tel l'algorithme L^3, utilisé en outil de cryptanalyse, sera donc plus forte.

Si la suite (a_i) est super croissante on sait d'après [3] que $a_i \geqslant 2^i$. Dans ce cas

$$A[(a_i)] \geqslant \sum_{i=2}^{n} 2^i = 2^{n+1}.$$

Soit $a_i = p^n + p^i$ $i = 1, \ldots, n$ une suite définissant un sac à dos orthogonal. Son amplitude vaut :

$$A[(a_i)] = \frac{\sum_{i=2}^{n} (p^n + p^i)}{p^n + p} = \frac{(n-1)\,p^n + \sum_{i=2}^{n} p^i}{p^n + p}.$$

On utilise les majorations suivantes :

$$\frac{(n-1)\,p^n}{p^n + p} \leqslant n - 1$$

et

$$\frac{\sum_{i=2}^{n} p^i}{p^n + p} = \frac{p}{p-1}\,\frac{p^n - p}{p^n + p} \leqslant 2$$

pour obtenir que :

$$A[(a_i)] \leqslant n + 1.$$

Si la suite ordonnée (a_i) définit un sac à dos divisible, on a, compte tenu des inégalités suivantes $q_1 \geqslant q_2 \ldots \geqslant q_n$:

$$A[(a_i)] = \frac{\sum_{i=2}^{n} P/q_i}{P/q_1} = q_1(1/q_2 + \cdots + 1/q_n) \leqslant$$

$$\leqslant q_1(1/q_n + \cdots + 1/q_n) = (n-1)\cdot\frac{q_1}{q_n}.$$

D'autre part, pour toute suite croissante (a_i) $1 \leqslant i \leqslant n$, on a $A[(a_i)] > n - 1$, on voit donc que les suites définissant des sacs à dos orthogonaux et des sacs à dos divisibles ont une très faible amplitude.

8.2. AMPLITUDE D'UN SAC A DOS TRANSFORMÉ

Il a été montré que l'amplitude des sacs à dos orthogonaux et des sacs à dos divisibles est plus faible que celle des sacs à dos super croissants de caractéristique comparable. Toutefois en vue d'utilisation cryptographique, il faut examiner l'amplitude des sacs à dos transformés pour chacune des classes. En effet, seuls les sacs à dos publics sont susceptibles d'être soumis à une éventuelle cryptanalyse.

Le tableau suivant donne les meilleures valeurs expérimentales de l'amplitude des sacs à dos transformés, pour diverses valeurs du nombre de termes n de la suite définissant le sac à dos, lorsque le multiplicateur w parcourt l'ensemble des valeurs possibles. Afin de pouvoir être exhaustif sur w, de petites valeurs de m ont été retenues. Il a été constaté expérimentalement que le choix du paramètre k influe peu sur les résultats.

Amplitude des sacs à dos :		
n	orthogonaux	divisibles
3	2,00	2,00
5	4,09	4,11
10	12,18	11,64
20	30,94	32,13
30	81,97	48,02
40	92,90	89,76

Les valeurs données dans le tableau sont les résultats d'expériences faites avec divers premiers et divers facteurs m. Ils confirment l'existence de sacs à dos difficiles à cryptanalyser par les méthodes de réduction de réseau, ce qui est confirmé par d'autres expériences.

9. Valeurs numériques

Dans [6] des expériences sur la résistance des sacs à dos obtenus à partir des sacs à dos orthogonaux et des sacs à dos divisibles à l'algorithme LLL ont été menées en dimension au plus 10.

Il en résulte que les sacs à dos orthogonaux ne sont pas plus résistants que les sacs à dos de Graham Shamir. Il faut toutefois noter que l'application de trois transformations de chiffrement à chaque sac à dos affaiblit notablement, pour chacune de ces deux familles, le taux de réussite de l'algorithme LL dès la dimension 7.

La résistance des sacs à dos obtenus à partir de sac à dos orthogonaux est très élevée. En dimension 10 l'algorithme LLL ne parvient pas à trouver de solution au problème posé, quelle que soit la version de l'algorithme qui est utilisée.

Il apparaît donc que l'utilisation de sacs à dos orthogonaux avec $n = 60$, la taille des entiers a_i étant de 200 chiffres décimaux est suffisante pour des applications cryptographiques.

10. Conclusion

Les nouvelles classes de sacs à dos introduites sont intéressantes car elles augmentent sensiblement le nombre de sacs à dos connus qui sont décodables. Elles ouvrent la voie vers l'examen de sacs à dos définis sur des anneaux de polynômes et sur des courbes algébriques.

D'autre part la cryptanalyse de ces sacs à dos par des méthodes de réduction dans les réseaux telles que l'algorithme de Lenstra Lenstra et Lovasz à une faible probabilité de réussite. Ceci contribuera à remettre en valeur une classe d'algorithmes de cryptographie injustement délaissée.

Manuscrit reçu le 7 juin 1991.

BIBLIOGRAPHIE

[1] A. Shamir and R. Zippel, *On the security of the Merkle Hellman cryptographic scheme IEEE Trans. on Info. Theory* Vol. IT-26(3), pp. 339-340, CA May 1980.

[2] R. C. Merkle and M. E. Hellman, « Hiding Information and signature in Trapdoor Knapsacks. » *IEEE Trans. on Info. Theory* Vol. IT-24(5), pp. 525-530, September 1978.

[3] M. Petit, « Étude mathématique de certains systèmes de chiffrement, les sacs à dos », *Thèse présentée à l'Université de Rennes,* septembre 1982.

[4] E. F. Brickell and A. M. Odlyzko, « Cryptanalysis : A survey of recent recent Results », *Preprint,* mars 1991.

[5] D. E. Denning, « Cryptography and data security », *Addison Wesley,* January 1983.

[6] L. Bournon, « Étude comparative de plusieurs familles de sacs à dos », *mémoire de D.E.A. Université d'Aix Marseille II,* septembre 1991.