Le groupe des tresses et ses applications en cryptographie

Axel Benyamine

Numéro de Candidat : 29530

1 Introduction

1.1 Définition

On définit ainsi le groupe des tresses : B_n est le groupe engendré par les n-1 générateurs σ_i pour i $\in [\![1,n-1]\!]$.

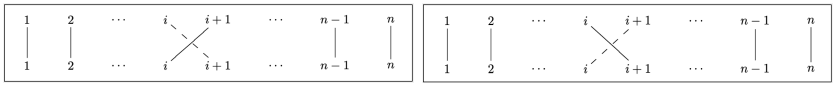

Figure 1: Représentation de σ_i (à gauche) et σ_i^{-1} (à droite)

Ces générateurs vérifient les relations suivantes : $\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i & si \ \mid i-j \mid \geq 2 \ (1) \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & si \ \mid i-j \mid = 1 \ (2) \end{cases}$

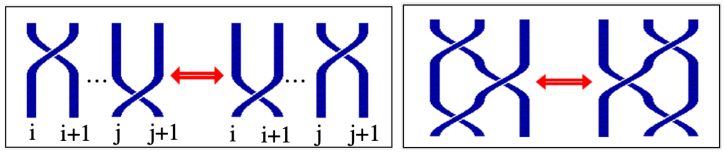

Figure 2: Illustration des relations (1) (à gauche) et (2) (à droite)

On adoptera pour la suite une écriture des tresses sous forme de mots sur l'alphabet des σ_i et des σ_i^{-1}. Le produit de tresses étant par conséquent la concaténation des deux mots.

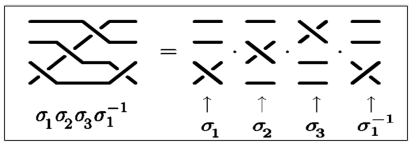

Figure 3: Un exemple de produit de tresses

2 Des propriétés algébriques

La structure algébrique, et en particulier non commutative, du groupe des tresses fait émerger trois problèmes qui, étant difficiles à résoudre, peuvent être exploités dans l'élaboration d'un système cryptographique.

2.1 Le problème de mots

On parle de problème de mot lorsque l'on se demande si deux mots donnés représentent la même tresse de B_n, c'est à dire si les deux mots proposés son équivalents.

2.2 Le problème de conjugaison

On parle de problème de conjugaison lorsque l'on se demande si deux mots x et y sont conjugués, c'est à dire s'il exite a tel que $y = a^{-1}xa$.

2.3 Le problème de recherche du conjuguant

On parle de problème de conjugaison lorsque l'on souhaite retrouver a à partir de x et $y = a^{-1}xa$.

3 Le retournement des mots

On cherche ici à représenter une tresse t sous la forme $N(t)D(t)^{-1}$, où $N(t)$ et $D(t)$ sont des tresses positives (engendrées par les générateurs, sans les inverses). On se munit de trois transformations :

- $a\sigma_i\sigma_i^{-1}b \to ab$
- $\mid i-j \mid = 1 \Longrightarrow a\sigma_i^{-1}\sigma_j b \to a\sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1}b$
- $\mid i-j \mid > 1 \Longrightarrow a\sigma_i^{-1}\sigma_j b \to a\sigma_j\sigma_i^{-1}b$

Théorème (Confluence) : Si un mot a se transforme en deux mots b et b', il existe un mot c tel que b et b' se transforment en c.

Théorème (Convergence) : Toute suite (t_n) telle que pout tout n entier naturel, t_n se transforme en t_{n+1} est stationnaire et sa limite est un quotient de tresses positives.

D'où l'existence et l'unicité du couple $(N(t), D(t))$.
De plus on dispose du théorème suivant qui permet de résoudre le problème de conjugaison:

Théorème : t est la tresse simple si et seulement si $D(t)^{-1}N(t)$ se transforme en ϵ (mot vide).

4 Implémentation du cryptosystème

4.1 Principe général

La cryptographie à base de tresses est fondée sur un système à clé publique et privée. Bob et Alice choisissent tous deux une tresse x dans un ensemble de tresses B_n.

Ensuite, Alice et Bob choisissent respectivement une clé privée a et b respectivement dans $B_{0,r}$ et dans $B_{r+1,n}$ ($B_{i,j}$ est le sous-groupe engendré par les tresses à n brins composées de générateurs dont les indices sont dans $[i, j-1]$). On a alors $ab = ba$.

Ils envoient alors respectivement à l'autre $p_A := a^{-1}xa$ et $p_B := b^{-1}xb$ sous forme retournée (l'envoie sous la forme de concaténation de mots permettrait de "lire" les clefs privées, ce que la forme retournée empêche a priori). Un hacker aura du mal à retrouver a et b à partir de ces deux-là du fait de la complexité du problème de conjugaison.

La clé privée partagée par les Alice et Bob est donc $K = a^{-1}p_Ba = b^{-1}p_Ab$.

4.2 Nécessité d'une fonction hachage

Pour crypter un message à l'aide de la tresse K préalablement calculée il est nécessaire de se munir d'une fonction $H : B_n \to \{0,1\}^N$ où N est fixé (taille en bits du message à transmettre).
Ensuite, Alice cryptera le message M en un message $M' = M \oplus H(K)$ où $\oplus$ est l'addition bit à bit modulo 2.
Ainsi, Bob pourra décrypter M' grâce à la relation $M' \oplus H(K) = M \oplus 2.H(K) = M$.

4.3 La représentation de *Burau*

4.3.1 Définition de la représentation de *Burau*

La représentation (non réduite) de *Burau* (non-réduite) est un homomorphisme de B_n vers $GL_n(\mathbb{Z}[t, t^{-1}])$. On le définit sur les tresses élémentaires σ_i de B_n comme :

$$\beta(\sigma_i) = Diag(I_{i-1}, \begin{pmatrix} 1-t & 1 \\ t & 0 \end{pmatrix}, I_{n-i-1})$$

Finalement, on retrouve bien :

$$\beta(\sigma_i)\beta(\sigma_j) = \beta(\sigma_j)\beta(\sigma_i) \ si \mid i-j \mid \geq 1$$
$$\beta(\sigma_i)\beta(\sigma_j)\beta(\sigma_i) = \beta(\sigma_j)\beta(\sigma_i)\beta(\sigma_j) \ si \mid i-j \mid = 1$$

Ce qui garantit bien l'unicité de l'image par β d'une classe d'isotopie.

4.3.2 Défaut d'injectivité

Pour n$\geq 5, \beta$ n'est pas injectif. Par exemple, en posant :

$$\psi_1 = \sigma_3^{-1}\sigma_2\sigma_1^2\sigma_2\sigma_4^3\sigma_3\sigma_2 \; et \; \psi_2 = \sigma_4^{-1}\sigma_3\sigma_2\sigma_1^{-2}\sigma_2\sigma_1^2\sigma_2^2\sigma_1\sigma_4^5$$

Puis

$$a = \psi_1^{-1}\sigma_4\sigma_1 \; et \; b = \psi_2^{-1}\sigma_4\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_4\psi_2$$

On obtient :

$$\beta(ab) = \beta(ba)$$

4.4 Construction de la fonction de hachage

On utilise la représentation de Burau avec t=10 (choix arbitraire). On dispose ainsi de $\beta : B_n \to GL_n(\mathbb{Q})$. On pose ensuite :

$$\gamma : \begin{cases} GL_n(\mathbb{Q}) & \to B_n \\ (\frac{a_{i,j}}{b_{i,j}})_{1\geq i,j\geq n} & \mapsto \overline{a_{1,1}b_{1,1}a_{2,1}...a_{n,n}b_{n,n}} \end{cases} \quad Où \; \forall (i,j) \in [\![1,n]\!]^2, \begin{cases} (a_{i,j}, b_{i,j}) \in \mathbb{Z} \times \mathbb{N}^* \\ a_{i,j} \wedge b_{i,j} = 1 \; si \; a_{i,j} \neq 0 \\ b_{i,j} = 1 \; si \; a_{i,j} = 0 \end{cases}$$

Et où $\overline{a}$ est l'écriture non signée en base 10.
On utilise ensuite l'algorithme $sha256 : Chaine \; de \; caractère \to \{0,1\}^{256}$.
Finalement,

$$H = sha256 \circ \gamma \circ \beta$$

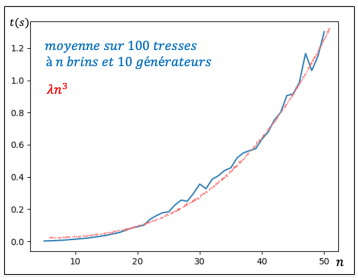

Figure 4: Temps d'éxécution de β (les temps d'éxécution de γ et $sha256$ sont négligeables devant ce dernier)

5 Craquage du sytème

5.1 Idée générale pour résoudre les problèmes de conjugaison et de recherche du conjuguant

Le but est de construire à partir de a un ensemble fini SSS(a) (nommé Super Summit Set de a), dépendant uniquement de la classe de conjugaison de a.
a et b sont alors conjugués si et seulement si SSS(a)=SSS(b).
De plus, en gardant en mémoire toutes les conjugaisons nécessaires pour passer de a aux éléments de SSS(a), on résout le problème de recherche du conjuguant

5.2 Forme normale

5.2.1 Présentation

La forme normale d'une tresse est une représentation particulière qui possède une propriété d'unicité.

5.2.2 Définitions

Diviseur à gauche : Pour deux tresses a et b, on dit que b divise a à gauche lorsqu'il existe c une tresse telle que a = bc.

Demi-tour de Garside : Il s'agit de la tresse correspondant à une permutation suivant le schéma i devient n-i. On le note Δ_n. Plusieurs écritures différentes existent, une étant $\Delta_n = (\sigma_1...\sigma_{n-1})(\sigma_1...\sigma_{n-2})...(\sigma_1)$. Ses diviseurs sont appelés les tresses simples et sont en bijection avec S_n.

5.2.3 Procédé

On s'intéresse d'abord aux tresses positives. Tout d'abord, on note r le plus grand entier tel que Δ_n^r divise la tresse, le reste étant noté b. Ensuite, on calcule $y_1 = b \wedge \Delta_n$, puis on itère ce procédé sur le reste jusqu'à ce qu'on obtienne le mot vide. La terminaison est assurée car les générateurs sont des tresses simples.

La forme normale de la tresse est unique et prend la forme $(r, y_1, ..., y_p)$.

5.2.4 Généralisation

Pour faire disparaitre les générateurs négatifs, il faut utiliser les propriétés suivantes :

- $\Delta_n \sigma_i = \sigma_{n-i} \Delta_n$
- $\Delta_n = (\sigma_1...\sigma_{n-1})...(\sigma_1...\sigma_{i+1})(\sigma_i...\sigma_1)...(\sigma_i...\sigma_{i-1})(\sigma_i)$

Ainsi, en faisant apparaitre $\Delta_n^{-1}\Delta_n$ devant le terme négatif, on peut le supprimer et déplacer le Δ_n^{-1} tout à gauche. On applique ensuite le procédé précédent pour déterminer la forme normale.

5.3 Le Super Summit Set

5.4 Définitions

Pour une tresse écrite sous forme normale : $a = \Delta_n^{-r} a_1...a_p$, on pose :

la longueur canonique de a : $\|a\| = p$

la classe de conjugaison de a : $C(a) = \{\sigma^{-1} a \sigma, \sigma \in B_n\}$

la grande longueur de a : $gl(a) = min\{\|x\|, x \in C(a)\}$

le Supper Summit Set de a : $SSS(a) = \{x \in C(a) : \|x\| = gl(a)\}$

l'automorphisme τ :

$$\tau : \begin{cases} B_n & \to B_n \\ x & \mapsto \Delta_n^{-1} x \Delta_n \end{cases}$$

le cyclage de a : $c(a) = \Delta_n^{-r} a_2...a_p \tau^r(a_1)$

le décyclage de a : $d(a) = \Delta_n^{-r} \tau^{-r}(a_p) a_1...a_{p-1}$

5.4.1 Construction de SSS(a)

Proposition : $c(a)$ et $d(a)$ sont conjugués à a.

Conséquences : On peut construire un élément de SSS(a) par cyclage successifs puis décyclage succesifs. Une fois cet élément obtenu, on peut construire facilement par conjugaison successive par des tresses simples, jusqu'à obtenir SSS(a).
La complexité théorique de la construction du SSS est en moyenne de $O(n!)$.

6 Conclusion

- Ce crypto-sytème permet l'élaboration d'un système relativement rapide (transmission et décodage durant entre 1sec et 1min).
- Le craquage du sytème est très lent voire impossible pour n suffisament grand.

n \ l	1	2	3	4	5	6	7	8	9
2	0,24	0,91	1,28	2,62	5,47	8,67	14,3	14,5	20,4
3	0,47	1,42	3,10	5,68	8,27	15,8	20,4	24,0	30,1
4	35,6	136	175	434	Erreur	Erreur	Erreur	Erreur	Erreur

Figure 5: temps de craquage (en s) pour n brins et l générateurs

- Limites : la transmission peut laisser entrevoir des informations sur les clefs privées et les compléxités sont difficilement maîtrisables (pour la transmission et le craquage).

7 Bibliographie

[1] Patrick Dehornoy : Braid-based cryptography : Contemporary Mathematics 360, (2004)

[2] Patrick Dehornoy : Le probleème d'isotopie des tresses : Leçons mathématiques de Bordeaux vol. 4, Cassini (2011), pages 259-300

[3] Daniel Gagnon : Cryptographie et Groupes de Tresses : Mémoire présenté comme exigence partielle à la maîtrise de mathématiques, (2007)

[4] Alaa Eddine Belfedhal : Etude et Implémentation des Fonctions de Hachage Cryptographiques Basées sur les Automates Cellulaires : Thèse, (2015)

[5] Joël Riou, Xavier Caruso : Groupe des tresses d'Artin : mémoire d'activités inter-magistères (2000)

[6] Jean Fromentin : Forme normale tournante des tresses : Thèse, (2009)

[7] Cédric Millet : Groupe de tresses et Cryptographie : Rapport de stage de magistère, (2003)

[8] David Garber : Braid Group Cryptography : World Scientific Review Volume (2009)

[9] Notes rédigées par Didier Trotoux d'une conférence de Patrick Dehornoy : Le calcul des tresses : journées APMEP (2005), Caen

[10] Patrick Dehornoy : Solutions des exercices du livre "Le calcul des tresses" : Calvage et Mounet, (2019)

29530 BENYAMINE Axel

Le groupe des tresses et ses applications en cryptographie

Les tresses, à première vue simple objet visuel, ont aujourd'hui de nombreuses applications dans les sciences modernes, comme la physique statistique et la mécanique quantique. Cependant, leur aspect géométrique renferme une structure de groupe, au moins tout aussi utile, notamment pour l'informatique théorique.
La structure de groupe des tresses permet un chiffrage sécurisé des données. Le piratage des données étant de plus en plus répandu, leur protection apparaît comme un enjeu sociétal majeur. Cet aspect motive donc un travail sur les propriétés algébriques des tresses afin de construire un crypto-système sûr et rapide.

Ce TIPE fait l'objet d'un travail de groupe.
Liste des membres du groupe :

- *COLLIN--LIZAN-ESQUERRÉTOU Jérôme*
- *FÉVRIER Guillaume*
- *LAMBERT Julien*

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique Théorique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Tresses	*Braids*
Cryptographie	*Cryptography*
Implémentation	*Implementation*
Piratage informatique	*Hacking*
Théorie des groupes	*Groupe theory*

Bibliographie commentée

Les tresses sont un arrangement de brins alignés réalisant un motif harmonieux pour une utilisation artistique ou pratique. A partir de la vision intuitive géométrique que nous nous faisons des tresses, il est possible d'introduire une structure algébrique de groupe [9]. Chaque tresse est engendrée par des générateurs, correspondant chacun à un échange de brins voisins. L'élément neutre correspond à des brins parallèles (la tresse neutre)[5].

Les premiers travaux sur le groupe des tresses remontent au mathématicien autrichien Emil Artin qui, en 1924, donna les relations de base définissant la construction du groupe des tresses [1] ainsi que ses premières propriétés et notations. De nombreuses avancées ont été réalisées ensuite,

notamment par Patrick Dehornoy [2] qui trouva de nouvelles formes de représentation du groupe des tresses et s'intéressa au problème d'isotopie des tresses, c'est-à-dire la construction de classes d'équivalences selon la relation : "représenter la même tresse". En effet, des enchaînements différents de générateurs peuvent en réalité renvoyer à la même tresse, et déterminer si c'est le cas soulève de réelles difficultés. C'est ici la base du problème de mots [1] et de la forme normale [6]: comment savoir si deux tresses sont égales. Une autre méthode poussée, appelée réduction des poignées, permet une implémentation rapide algorithmiquement parlant.

Ainsi, le groupe des tresses peut permettre le transport de données cryptées via un système à clés publiques et à clés privées [3], les clés étant des tresses. En effet, une attaque informatique sur une telle implémentation nécessite de résoudre le problème du conjugant, c'est-à-dire retrouver le conjugant de deux éléments conjugués. Mais sa résolution présente une complexité élevée, ce qui justifie l'intérêt des tresses en cryptographie. Ce système est basé sur un échange de la clé publique cryptant le message, qu'il faut ensuite décrypter à partir des clés privées que possèdent l'émetteur et le destinataire. La transmission des données, non étudiée en détail, peut se réaliser à l'aide de la forme normale qui a l'avantage d'être assez compacte. Pour réaliser notre implémentation, nous avons utilisé des matrices, dites de Burau [3], qui partagent des propriétés avec le groupe des tresses, et une fonction de hachage [4] qui permet de réduire les matrices de Burau en bits.

Nous nous sommes ensuite intéressés à une manière de casser notre système, passant par la construction d'un sous-groupe fini des classes de conjugaison [7] de plusieurs tresses intervenant dans la transmission du message. C'est ce cassage qui a nécessité la plupart des algorithmes les plus complexes.

Problématique retenue

Quelles sont les propriétés définissant le groupe des tresses ? Dans quelle mesure permet-il de réaliser un crypto-système performant et sûr ?

Objectifs du TIPE

-S'approprier la modélisation algébrique du groupe des tresses et ses propriétés, et relever sa cohérence vis à vis de la représentation géométrique des tresses.
-Se munir d'une représentation linéaire du groupe des tresses.
-Étudier la fidélité de cette représentation (injectivité de la fonction « représentation »).
-Établir une fonction « hachage » qui à toute tresse renvoie une suite de bits de taille prédéfinie.
-Employer les tresses et leur hachage dans le cadre d'un système de cryptographie à clef publique.

Références bibliographiques (ETAPE 1)

[1] PATRICK DEHORNOY : Braid-based cryptography : *Contemporary Mathematics 360, (2004)*
[2] PATRICK DEHORNOY : Le problème d'isotopie des tresses : *Leçons mathématiques de Bordeaux vol. 4, Cassini (2011), pages 259-300*

[3] Daniel Gagnon : Cryptographie et Groupes de Tresses : *Mémoire présenté comme exigence partielle à la maîtrise de mathématiques, (2007)*
[4] Alaa Eddine Belfedhal : Etude et Implémentation des Fonctions de Hachage Cryptographiques Basées sur les Automates Cellulaires : *Thèse, (2015)*
[5] Joël Riou, Xavier Caruso : Groupe des tresses d'Artin : *Mémoire d'activités inter-magistères (2000)*
[6] Jean Fromentin : Forme normale tournante des tresses : *Thèse, (2009)*
[7] Cédric Millet : Groupe de tresses et Cryptographie : *Rapport de stage de magistère, (2003)*
[8] David Garber : Braid Group Cryptography : *World Scientific Review Volume (2009)*
[9] Didier Trotoux : Le calcul des tresses : *Notes d'une conférence de Patrick Dehornoy : journées APMEP (2005), Caen*
[10] Patrick Dehornoy : Solutions des exercices du livre "Le calcul des tresses" : *Calvage et Mounet, (2019)*

DOT

[1] *En septembre-octobre, recherche d'un sujet et choix du groupe des tresses. Décision commune de travailler sur la représentation algébrique et non géométrique des tresses en raison des applications en cryptographie. Travail sur la théorie de ce groupe.*
[2] *En novembre-décembre, choix de l'implémentation et recherches sur les problèmes de mot et de conjugaison, en s'attardant en particulier sur la forme normale et la réduction des poignées. Début des recherches sur les matrices de Burau.*
[3] *En janvier-février, codage des différents algorithmes nécessaires au cryptosystème et fin des recherches sur les matrices de Burau.*
[4] *En février-mars, recherches sur les complexités des algorithmes existant, et analyse de la viabilité de notre système dans un cadre plus réaliste. Implémentation d'une méthode permettant de casser notre système et étude de ses limites.*