Encadré par:
Charles BOUILLAGUET

Amine IDRES 21322043
Rania BLIBEK 21215298

Le 27/05/2024

Sommaire

- Cryptographie
- Problèmes de Cryptographie
- Crible algébrique - GNFS
- Fusion dans CADO-NFS
- Améliorations apportées et comparaison
- Conclusion

Cryptographie

La cryptographie est l'art de chiffrer les secrets, transformant les mots en énigmes que seuls les initiés peuvent déchiffrer.

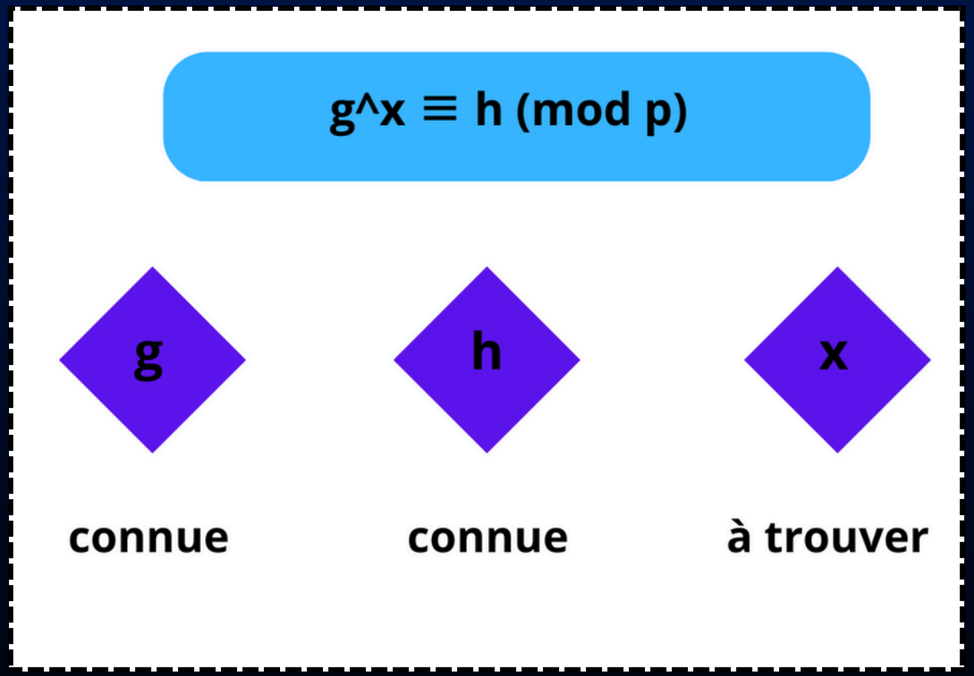
Factorisation

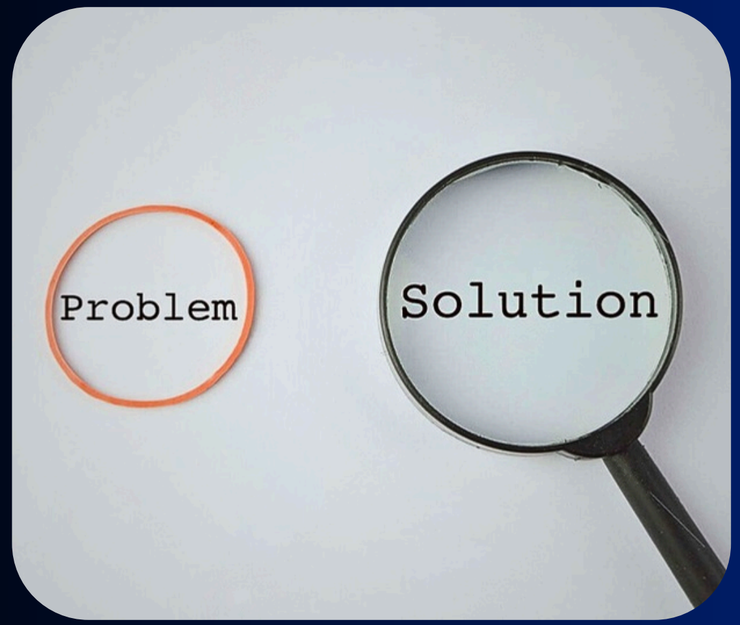
La factorisation est le processus de décomposer un nombre entier en un produit de nombres premiers.

Le problème de la factorisation est crucial pour la sécurité de l'algorithme RSA

Logarithme discret

Le logarithme discret est fondamental pour la sécurité de nombreux algorithmes cryptographiques.

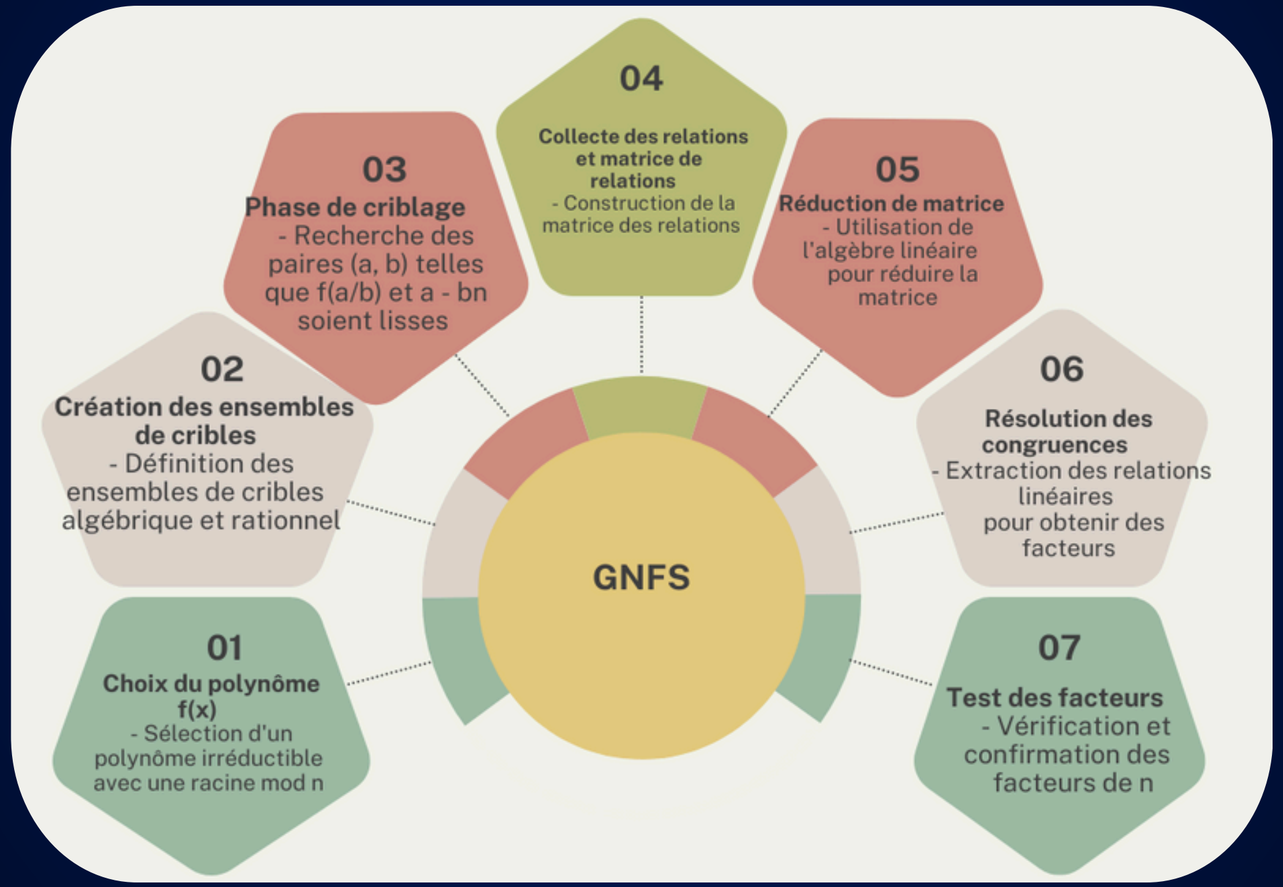




GNFS

la méthode la plus efficace connue pour factoriser de grands nombres entiers et calculer des logarithmes discrets.

Fonctionnement de GNFS



Records de factorisation

Number	Digits	Date	MIPS-years	Algorithm
C116	116	1990	275	MPQS
RSA-120	120	June, 1993	830	MPQS
RSA-129	129	April, 1994	5000	MPQS
RSA-130	130	April, 1996	1000	GNFS
RSA-140	140	February, 1999	2000	GNFS
RSA-155	155	August, 1999	8000	GNFS
RSA-576	174	December, 2003	13200	GNFS
C176	176	May, 2005	48.6 (Pentium 1 GHz CPU) years	GNFS
RSA-200	200	May, 2005	121 (Pentium 1 GHz CPU) years	GNFS

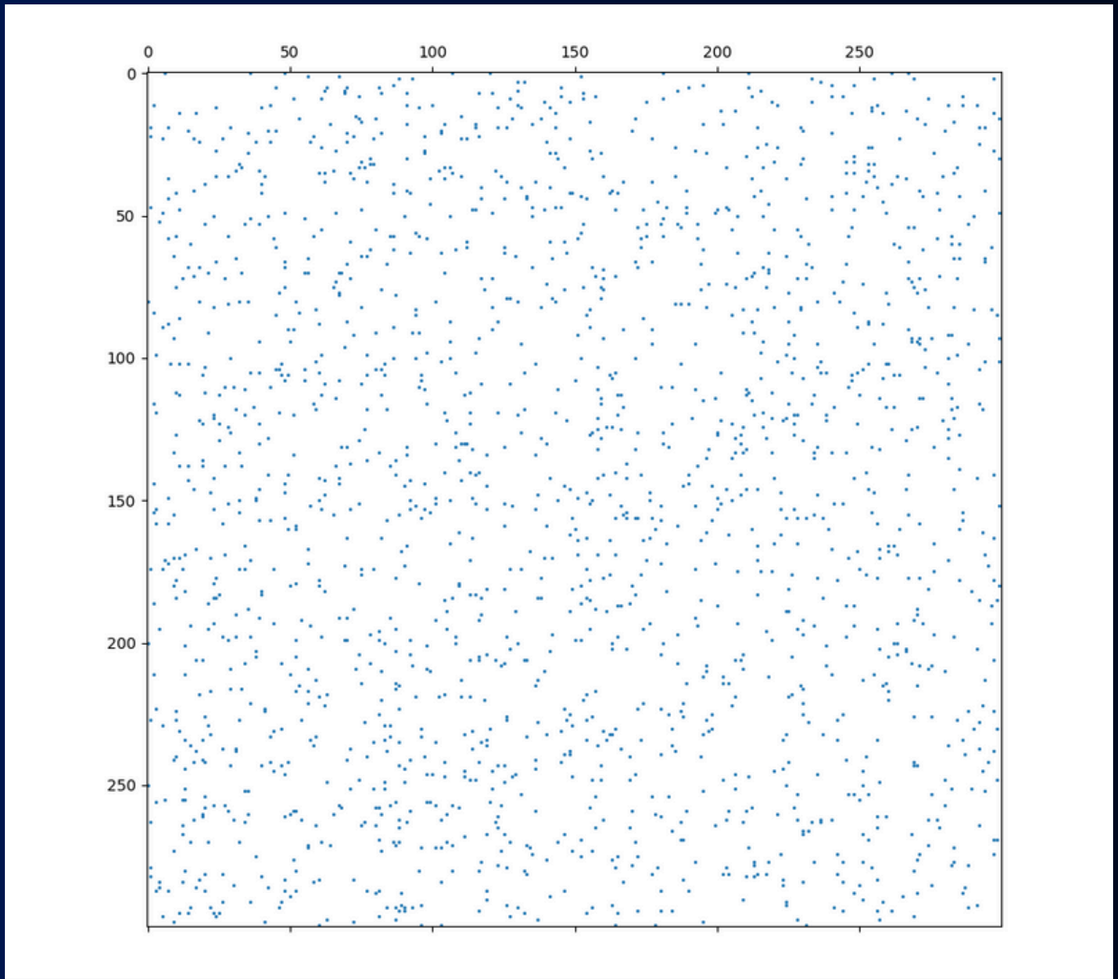
CADO-NFS

CADO-NFS est une implémentation optimisée de l'algorithme General Number Field Sieve (GNFS).
Il permet de résoudre des problèmes cryptographiques complexes avec une efficacité et une performance accrues.

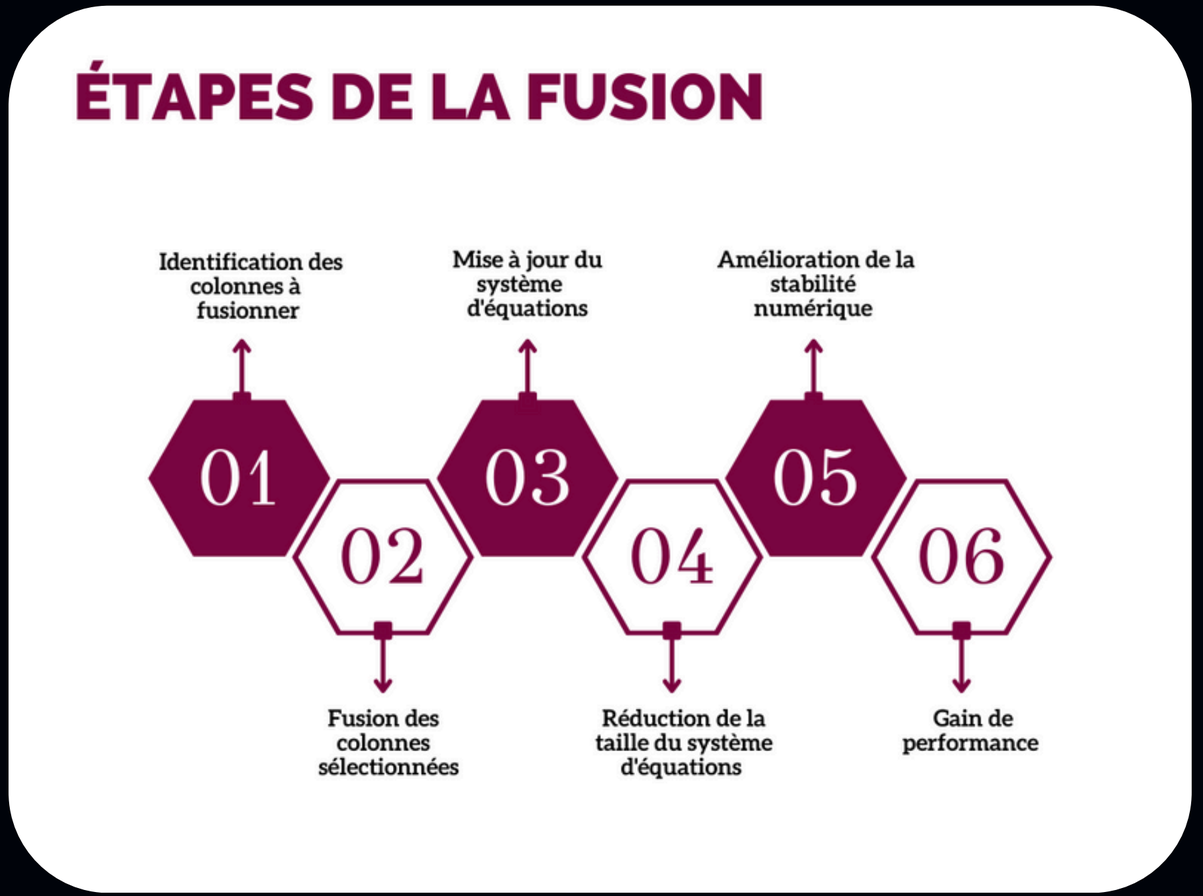
Input number	CADO-NFS 2.3.0
RSA-120	26 hours [1.9 hours]
RSA-130	107 hours [7.5 hours]
RSA-140	352 hours [23 hours]
RSA-155	83 days [5.3 days]


FUSIO
CADO
00:00:01:02

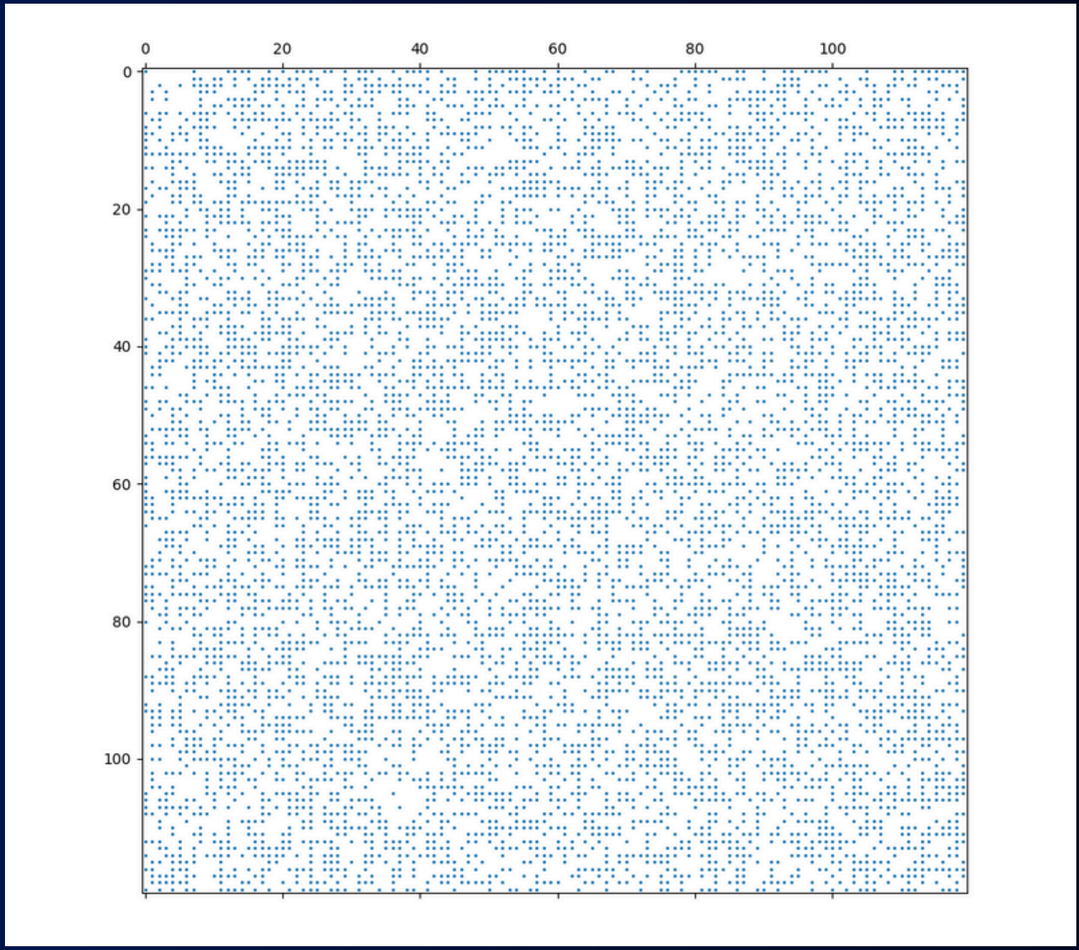
Exemple de matrice d’entrée (creuse)



Etapes de la fusion



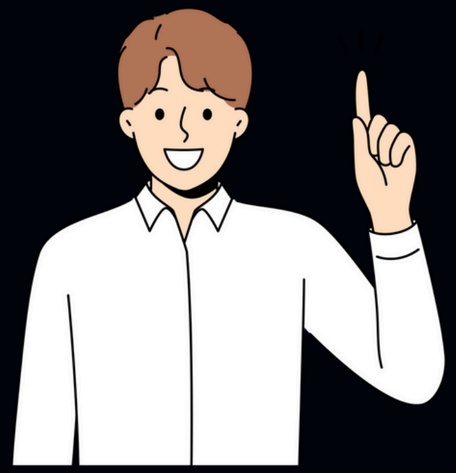
Exemple de matrice de sortie (dense)

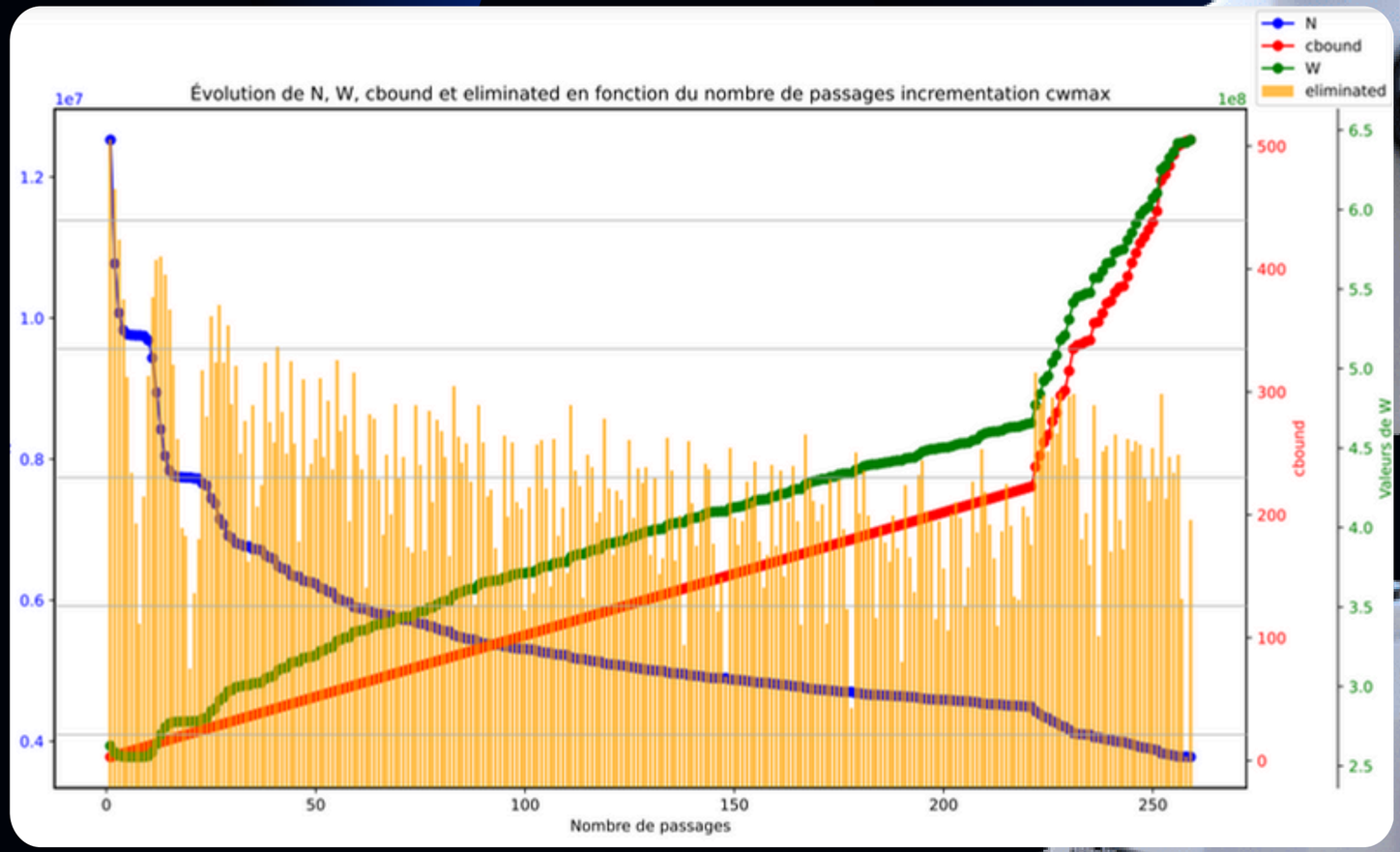


Améliorations apportées

Amélioration 1

Changement de la méthode d'incrémentation de cwmax

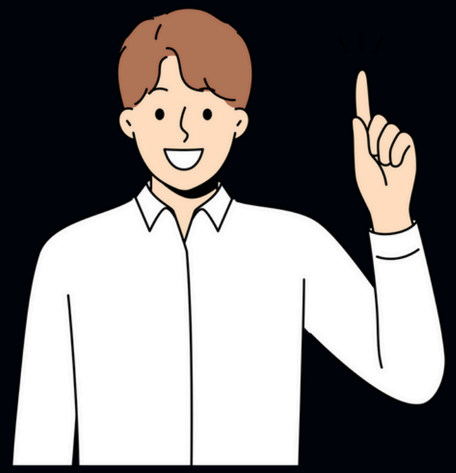


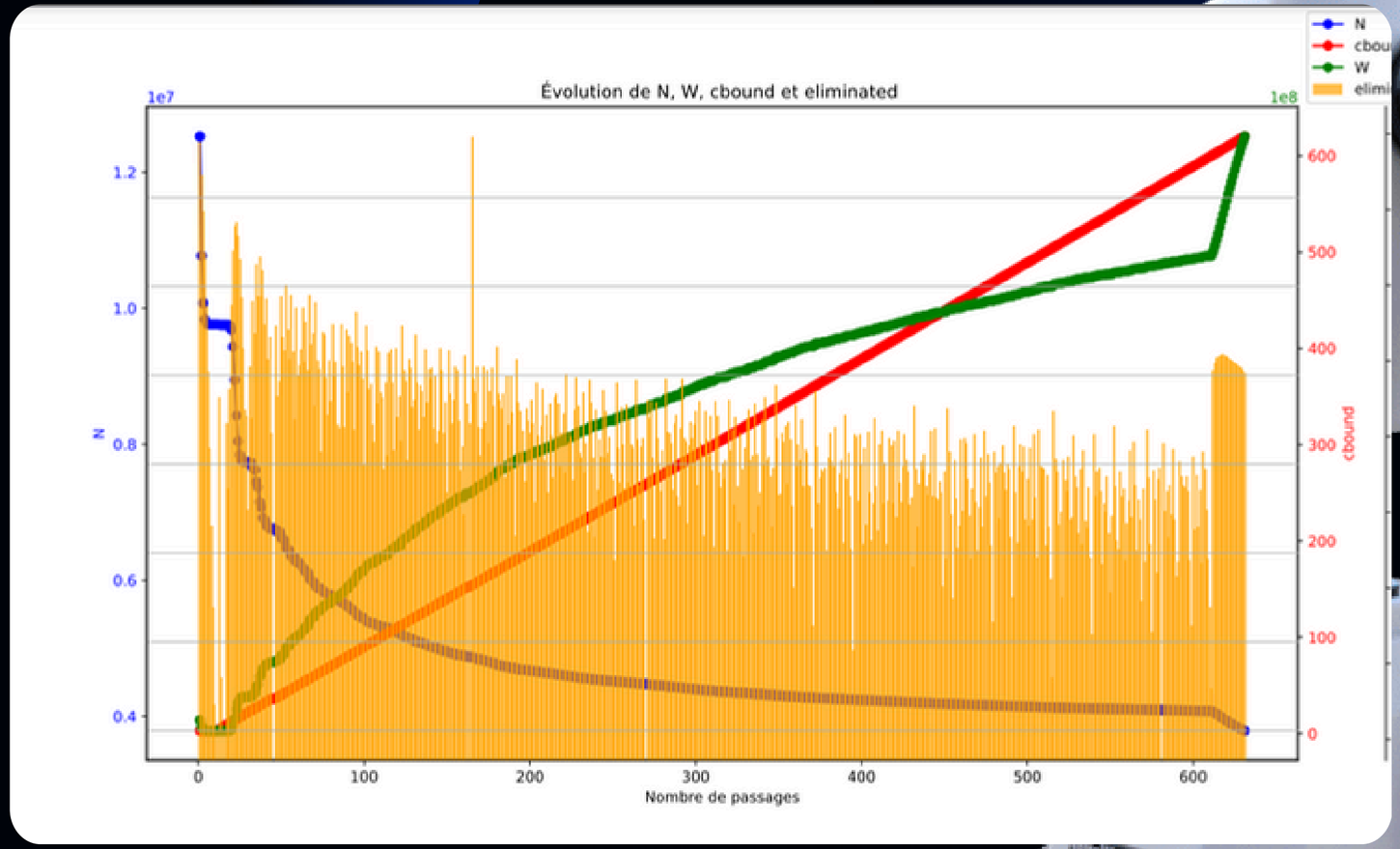


Améliorations apportées

Amélioration 2

attribution de la
valeur 1 à cbound

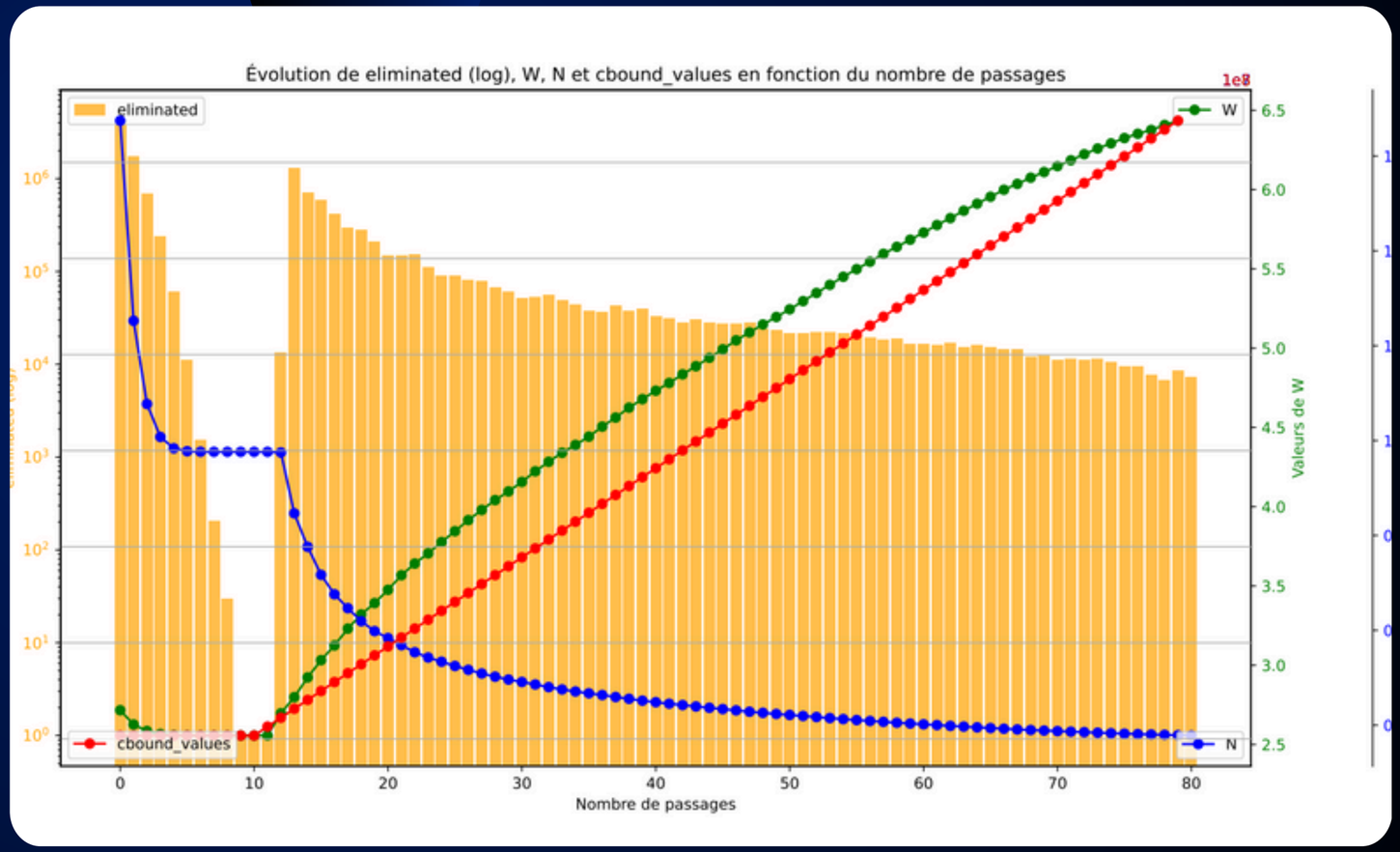




Comparaison

Version Original

L'amélioration 1 offre des avantages supérieurs par rapport à l'amélioration 2, laquelle elle-même représente une amélioration significative par rapport à la version originale



Autres tentatives

1

Augmentation de cwmax uniquement si plus de n fusions ont été effectuées.
(n arbitraire)

2

Ajustement de cwmax en l'augmentant si aucune fusion n'a été effectuée ou en le diminuant si moins de n fusions ont été effectuées .
(n arbitraire)

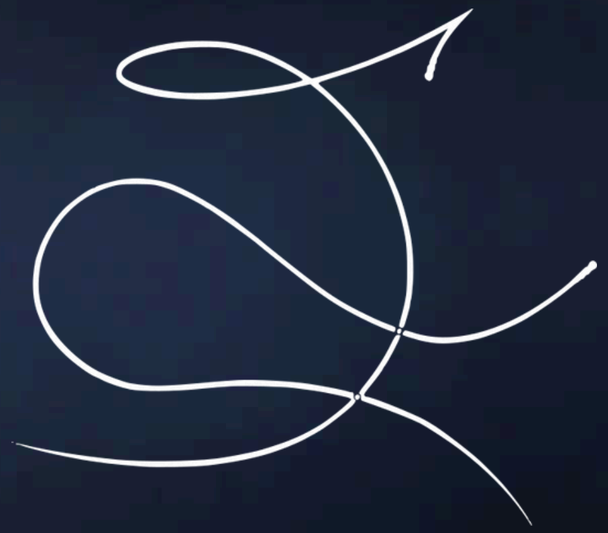
3

Réglage de cwmax à sa valeur maximale.

Conclusion

Le CADO -NFS est l'un des algorithmes les plus efficaces pour factoriser de grands nombres entiers, un problème fondamental en cryptographie.

Les améliorations apportées au CADO-NFS peuvent avoir un impact significatif sur la sécurité des systèmes cryptographiques basés sur la difficulté de la factorisation, comme RSA.



Merci pour votre attention

Des Questions