Spécifications Mathématiques : Protocole Collatz-Trapdoor

Ce document détaille les fondements arithmétiques du système cryptographique basé sur la dynamique de Collatz compressée.

1. Définition de l'Opérateur de Base

Soit $\mathbb{I} = \{2n+1 \mid n \in \mathbb{N}\}$ l'ensemble des entiers impairs positifs. L'application de Collatz compressée $U : \mathbb{I} \to \mathbb{I}$ est définie par :

$$U(n) = \frac{3n+1}{2^{v_2(3n+1)}}$$

Où $v_2(x)$ est la **valuation 2-adique** de x (l'exposant de la plus grande puissance de 2 divisant x).

2. Construction de la Trajectoire (Clé Privée → Publique)

Soit $S \in \mathbb{I}$ la clé privée. On génère la clé publique en itérant k fois l'application U.

Formule Explicite de la Trajectoire

Après k étapes, le point d'arrivée $P = U^{(k)}(S)$ peut être exprimé par la relation linéaire :

$$2^{A_k} \cdot P = 3^k \cdot S + C_k$$

Où les paramètres structurels sont définis par :

1. **Somme des Valuations :** $A_k = \sum_{i=0}^{k-1} a_i$, avec $a_i = v_2(3 \cdot U^{(i)}(S) + 1)$.
2. **Terme Additif (Constante de Translation) :** $$ C_k = \sum_{j=0}^{k-1} 3^{k-1-j} \cdot 2^{A_j}

(avec la convention $A_0 = 0$).

Données de la Clé Publique

La clé publique est le triplet (P, k, M) où :

- P est le point d'arrivée.
- k est le nombre d'itérations.
- $M = 2^{A_k+k}$ est le **modulo de précision**.

3. Exemple Concret d'Application

A. Génération et Dérivation

Alice choisit $S = 7$ et $k = 2$. Comme calculé précédemment, sa clé publique est $(P = 17, k = 2, M = 16)$.

B. Chiffrement

Pour chiffrer un message m, Bob utilise un "sel" aléatoire r et calcule :

$$X = (m \cdot 2^{A_k+k}) + S_{virtuel}$$

Où $S_{virtuel}$ est un nombre qui suit la même trajectoire que S sur k pas.

C. Déchiffrement

Alice utilise S pour soustraire la structure de Collatz de X et retrouver m par division modulaire.

4. Protocole de Signature avec Nonce (Non-Répudiation)

L'utilisation d'un **Nonce** (N) garantit que chaque signature est unique. La signature $\sigma = f(S, H, N)$ lie le secret S au condensé du message H et au nombre à usage unique N.

5. Résistance Post-Quantique (Analyse Détaillée)

La résistance du protocole face à un ordinateur quantique repose sur deux piliers :

A. Échec de l'Algorithme de Shor (Non-Périodicité)

L'algorithme de Shor casse le RSA car il peut trouver la "période" (le cycle) d'une fonction d'exponentiation modulaire.

- **Dans Collatz :** La suite des valuations a_i est apériodique et chaotique. Il n'y a pas de structure répétitive prévisible sur laquelle un ordinateur quantique peut s'appuyer pour réduire la complexité.

B. Problème des Préimages dans un Graphe (Complexité de Grover)

L'algorithme de Grover permet de chercher un élément dans une base de données non triée avec une accélération quadratique ($\sqrt{N}$).

- **Le Labyrinthe Inverse :** Inverser $U^{(k)}(P)$ revient à remonter un arbre binaire dont le nombre de nœuds est proportionnel à 2^k.
- **Résistance :** Même avec l'accélération de Grover, le nombre d'opérations reste de l'ordre de $2^{k/2}$. Si $k = 512$, l'effort requis (2^{256}) reste totalement hors de portée des capacités de calcul de l'univers, qu'elles soient quantiques ou classiques.

C. Réduction au problème "Learning With Errors" (LWE)

Le terme additif C_k agit comme une erreur (un bruit) injectée à chaque pas. Retrouver S ressemble au problème de l'apprentissage avec erreurs, qui est l'une des bases les plus solides de la cryptographie post-quantique actuelle.

6. Performance et Sécurité

- **Compute :** Très efficace grâce aux opérations binaires (bit-shifts).
- **Exclusions :** Bannissement des nombres de Mersenne ($2^n - 1$) et des trajectoires trop courtes.

7. Recommandations Finales

- **Taille de S :** 2048 bits.
- **Horizon k :** 256 itérations minimum (512 pour une sécurité PQ maximale).