TP III – Codes de Tardos

Gaëtan Le Guelvouit

On laisse de côté le tatouage d'images pour cette session. L'objectif de ce dernier TP est d'implémenter des codes de Tardos, puis d'investiguer pour comprendre un algorithme de tatouage de livres. Les sources sont en C++, placées dans le répertoire `src` (un fichier `Makefile` comprend tous les paramètres de compilation).

`https://tinyurl.com/cswt2023`

1 Codes de Tardos

Le squelette du programme est donné dans le fichier `tardos.cpp`. En plus du cours, vous pouvez vous aider de l'article de vulgarisation de Teddy Furon, dont le lien de téléchargement est donné au début du fichier source.

1. Implémenter la fonction de génération du vecteur secret $\mathbf{p}$.
2. Coder la fonction de génération des vecteurs $\mathbf{x}_j$
3. Coder la fonction d'accusation $g()$.
4. Tester avec les paramètres par défaut. Que représentent les 20 derniers chiffres ?
5. Modifier le code pour comparer les scores à un seuil Z afin d'isoler les traitres. Fixer le seuil et la longueur du code pour $\epsilon < 10^{-3}$, puis tester.

2 Tatouage de livres

Plutôt que d'utiliser les DRM, environ un tiers de livres électroniques sont vendus avec un tatouage transactionnel. Dans le répertoire `data`, vous trouverez deux copies d'un même livre, achetées sous deux comptes utilisateur différents.

1. Quel est le véritable format des fichiers `.epub` ?
2. De quelle forme bien connue sont les fichiers qui constituent le livre ?
3. Quelles différences pouvez-vous identifier entre les deux copies ?
4. Que pensez-vous de la robustesse et de la sécurité de ce tatouage ?