TD introduction à la cryptographie post-quantique

Jean-Christophe Deneuville
jean-christophe.deneuville@enac.fr

8 décembre 2020

Intanciation pédagogique de McEliece

Le but de cet exercice de manipuler une instance du schéma de chiffrement de McEliece [1] afin de mieux en comprendre son fonctionnement.

1 Échauffement : décodage d'un mot bruité

Soit $\mathcal{C}$ le code linéaire généré par la matrice

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 7}$$

1. Quelle est la longueur du code ? Sa dimension ?
2. Combien de mots ce code possède-t-il ?
3. Quelle est sa distance minimale ?
4. Combien d'erreur(s) peut-il détecter ? Corriger ?

Nous venons de recevoir le mot $\mathbf{c} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$. Il existe une multitude d'algorithmes de décodage, plus ou moins efficaces. Nous allons en étudier deux : par maximum de vraissemblance, et par syndrome.

5. Quel est le mot de code le plus probable correspondant au mot reçu ?

Nous allons maintenant déterminer une matrice de parité $\mathbf{H}$ de $\mathcal{C}$.

6. Quelles sont les dimensions de cette matrice $\mathbf{H}$?
7. Quelle relation entre matrices génératrice et de parité faut-il exploiter pour construire cette matrice ?
8. Déterminez $\mathbf{H}$.
9. Calculez $\mathbf{s} = \mathbf{H}\mathbf{c}^\top$.
10. Expliquez pourquoi $\mathbf{s}$ correspond au syndrome de l'erreur.
11. Retrouvez l'erreur et donc le message envoyé.

Il n'est souvent pas raisonnable d'énumérer l'ensemble des mots du code, ce qui rend (entre autre) non praticable le décodage par maximum de vraissemblance.

2 McEliece : Génération des clés

Rappel : Dans le cryptosystème de McEliece, le code $\mathcal{C}$ (représenté par sa matrice génératrice $\mathbf{G}$) est rendu public dans une version dégradée/masquée. Pour ce faire, on publie la matrice $\tilde{\mathbf{G}} = \mathbf{SGP}$ où :

— $\mathbf{S}$ est une matrice $k \times k$ aléatoire inversible dans $\mathbb{F}_2$, et

— $\mathbf{P}$ est la matrice $n \times n$ d'une permutation aléatoire.

La clé publique est $\mathsf{pk} = \left(\tilde{\mathbf{G}}, t\right)$ où t est la capacité de correction du code (vous l'avez obtenue à la question 4 du premier exercice). On considère les matrices suivantes :

$$\mathbf{S} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \mathbf{P} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

1. Montrez que $\mathbf{S}$ est inversible.
2. Expliquez pourquoi $\mathbf{P}$ est bien une matrice de permutation.
3. Montrez que

$$\mathsf{pk} = \tilde{\mathbf{G}} = \mathbf{SGP} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

3 McEliece : Chiffrement

On souhaite chiffrer le message $\mathbf{m} = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}$. Soit l'erreur $\mathbf{e} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$ générée de manière aléatoire.

1. Calculez l'encodage $\mathbf{x}$ du message $\mathbf{m}$ par la matrice $\tilde{\mathbf{G}}$.
2. En déduire le chiffré $\mathbf{c}$ de ce message.

4 McEliece : Déchiffrement

Soit $\mathbf{c}$ le chiffré obtenu à la question 2 de l'exercice précédent.

1. Rappelez la procédure de déchiffrement.
2. Calculez $\mathbf{S}^{-1}$ (si vous ne l'aviez pas fait à la question 1 de l'exercice 2).
3. Calculez $\mathbf{P}^{-1}$ (vous pouvez vous aider d'une propriété bien connue des matrices de permutation).
4. Montrez que $\mathbf{y} = \mathbf{c}\mathbf{P}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$.
5. Exprimez $\mathbf{y}$ en fonction du message et de la clé secrète.
6. Décodez $\mathbf{y}$ en un message $\tilde{\mathbf{m}}$ (vous pouvez vous aider de la matrice de parité $\mathbf{H}$ trouvée à la question 8 de l'exercice 1).
7. Finissez le déchiffrement, et vérifiez que vous retrouvez bien le message $\mathbf{m}$ envoyé.

Références

[1] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.