

Compte-rendu hebdomadaire

Compte-rendu 7

Valentin Noyé

12 novembre 2025 - 14 novembre 2025

GitHub : <https://github.com/owilo/SecretSharing>

1 Résumé des tâches réalisées cette semaine

1. Avancée sur la section III.C de l'article sur la réduction de l'erreur sur l'image secrète introduite par des parts bruitées.
2. Présentations et activité dans le cadre de la journée des nouveaux entrants.
3. Section 2.1 – Analyse de l'annulation de l'erreur sur un cas concret en $GF(251)$. Vérification de l'exactitude des coefficients entre le polynôme d'origine et bruité.

2 Travail réalisé

2.1 Exemple d'annulation de l'erreur selon différentes configurations de bruit dans les parts

Dans un corps fini $GF(251)$, nous avons observé qu'introduire du bruit sur trois parts, par exemple $\{\varepsilon_a, \varepsilon_b, \varepsilon_c\} = \{-1, -1, 0\}$, permettait d'annuler l'erreur et de retrouver tout de même le secret en 0. Le problème a donc été posé pour le constater. Prenons 3 positions d'évaluation $\{x_a, x_b, x_c\} = \{1, 2, 3\}$, soit $k = 3$.

$$\begin{aligned}\varepsilon &= \sum_{i=1}^k \varepsilon_i \prod_{j=1, j \neq i}^k \frac{-x_j}{x_i - x_j} \\ &= \frac{x_b x_c}{(x_b - x_a)(x_c - x_a)} \varepsilon_a + \frac{x_a x_c}{(x_a - x_b)(x_c - x_b)} \varepsilon_b + \frac{x_a x_b}{(x_a - x_c)(x_b - x_c)} \varepsilon_c \\ &= -\frac{x_b x_c}{(x_b - x_a)(x_c - x_a)} - \frac{x_a x_c}{(x_a - x_b)(x_c - x_b)} \\ &= -\frac{6}{1 \cdot 2} - \frac{3}{-1 \cdot 1} \\ &= -3 + 3 \\ &= 0\end{aligned}\tag{1}$$

Ainsi, l'erreur totale s'évalue à 0 malgré la présence d'erreurs dans les parts. Nous voulons vérifier à présent si nous obtenons deux polynômes identiques avec et sans cette erreur.

Considérons des parts d'origine telles que $\{y_a, y_b, y_c\} = \{1, 1, 1\}$ et des parts bruitées $\{y'_a, y'_b, y'_c\} = \{0, 0, 1\}$. On a ainsi $\{\varepsilon_a, \varepsilon_b, \varepsilon_c\} = \{-1, -1, 0\}$ comme précédemment.

Nous constatons que le polynôme d'origine est $p(x) = 1$ tandis que le polynôme erroné est $p'(x) = 1 + 124x + 126x^2$. Il est clair qu'ici, $p(x) \neq p'(x)$, or nous avons $p(0) = p'(0) = 1$. Ainsi, même si l'erreur est nulle, nous obtenons des polynômes différents.

3 Travail à effectuer

1. Continuer l'article de Laura Bertojo sur l'analyse de l'erreur sur la reconstruction de l'image secrète avec des parts bruitées et essentiellement la section III.C.
2. Analyser en plus de détail l'impact de l'erreur δ sur les parts en ce qui concerne la qualité de la reconstruction ainsi qu'en sa capacité d'annulation de l'erreur.
3. Concrétiser l'application des codes correcteurs d'erreur de Reed-Solomon sur le partage d'images secrètes [1].

4 Activités

4.1 Réunions

Réunion de suivi (Mercredi 12/11/2025)

Lecture du compte-rendu précédent et clarification des points à intégrer dans l'article.

4.2 Journées

Journée des nouveaux entrants (Jeudi 13/11/2025)

Présentation des services du laboratoire en matinée et activité ludique escape game en après-midi.

Références

- [1] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Commun. ACM*, 24(9) :583–584, September 1981.