# Compte-rendu hebdomadaire

**Compte-rendu 6**

Valentin Noyé

3 novembre 2025 - 7 novembre 2025

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

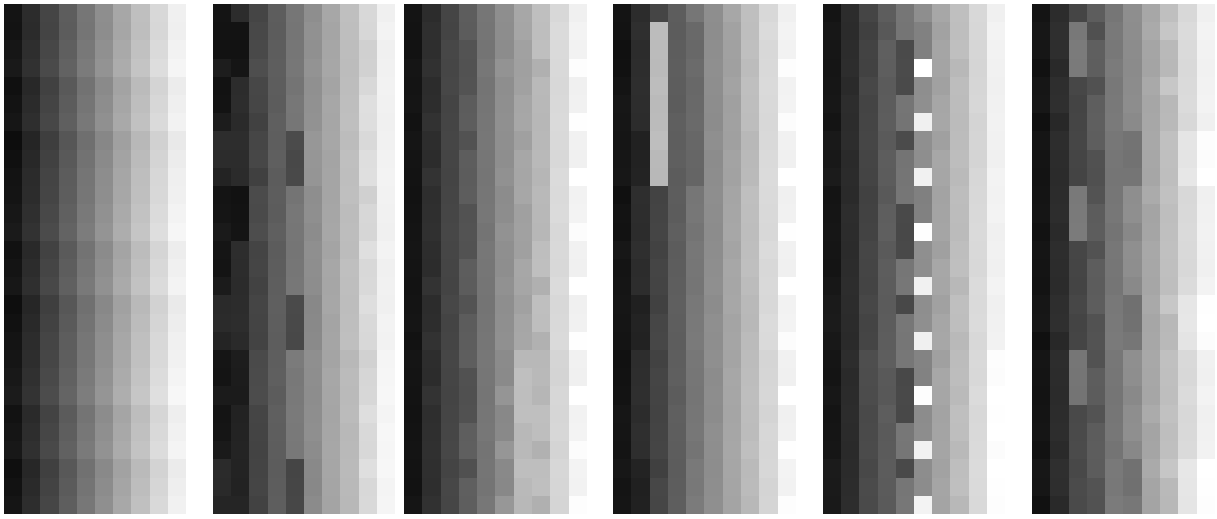
## 1 Résumé des tâches réalisées cette semaine

1. Légère avancée sur l'état de l'art de l'article sur l'analyse de l'erreur sur la reconstruction de l'image secrète avec parts bruitées.
2. Section 2.1 – Étude de l'erreur dans $GF(251)$ et $GF(2^8)$ pour différentes configurations de bruit contenu dans $\{-1, 0, 1\}$.
3. Section 2.2 – Analyse de la condition sur $k$ et $GF(p^m)$ garantissant un ensemble optimal de points d'évaluations. Étude des propriétés et des pistes quant à l'approfondissement de la recherche dans la réduction de l'erreur sur $GF(2^8)$.

## 2 Travail réalisé

### 2.1 Étude de l'erreur selon différentes configurations de bruit

Dans cette étude, nous appliquons le partage de secret de Shamir sur 10 valeurs de pixels différentes que nous reconstruisons avec $n = k = 3$ parts bruitées par l'ajout d'un $\delta = \{-1, 0, 1\}$. Dans la figure 1, la première ligne représente le pixel d'origine et les 27 autres lignes représentent les reconstructions par combinaison de parts bruitées avec différentes valeurs de $\delta$.



(a) $GF(251)$ (b) $GF(2^8)$ v1 (c) $GF(2^8)$ v2 (d) $GF(2^8)$ v3 (e) $GF(2^8)$ v4 (f) $GF(2^8)$ v5

FIGURE 1 – Reconstructions des pixels de la première ligne selons les différentes configurations de bruit (1 ligne = 1 configuration)

Nous constatons que dans $GF(251)$ l'erreur est minime tandis que $GF(2^8)$ pose tendance à l'amplifier puisque l'addition n'est pas analogue dans le domaine des entiers, et se traduit plus immédiatement par un XOR bit-à-bit. Nous voyons également que l'introduction d'aléa dans les parts donne des résultats différents uniquement pour $GF(2^8)$. Finalement, nous voyons qu'il existe pas de résultat de reconstruction exact et que chacune des lignes est distincte dans $GF(2^8)$. En revanche, dans $GF(251)$, certaines configurations d'erreur $\{\delta_1, \delta_2, \delta_3\}$ sur les parts confèrent soit un résultat exact ($\{-1,-1,0\}$, $\{0,0,0\}$ et $\{1,1,0\}$), c'est à dire des valeurs de pixel $\{20, 44, 69, \ldots\}$, soit avec un $\varepsilon = \pm 1$ de différence. Par exemple, $\{19, 43, 68, \ldots\}$ est généré par les parts $\{-1,-1,-1\}$, $\{0,0,-1\}$ et $\{1,1,-1\}$ tandis que $\{21, 45, 70, \ldots\}$ par les parts $\{-1,-1,1\}$, $\{0,0,1\}$ et $\{1,1,1\}$, ce qui forme une symétrie. En effet, l'erreur de certaines parts

## 2.2 Étude du choix de la position d'évaluation des polynômes sur la minimisation de l'erreur.

Rappelons l'interpolation de Lagrange de l'erreur $\varepsilon$ obtenue sur le secret à partir des erreurs sur les parts $\varepsilon_i$ et des polynômes de base de Lagrange $\ell_i$ évalués à partir de tout point $x_i$.

$$\varepsilon = \sum_i \varepsilon_i \ell_i(0), \quad \ell_i(0) = \prod_{i \neq j} \frac{x_j}{x_i - x_j} \tag{1}$$

Dans le précédent compte-rendu, nous avons prouvé l'existence d'ensembles de points d'évaluation $\{x_1, \ldots, x_k\}$ tels que tous les $\ell_i(0) = 1$ uniquement lorsque $k$ est impair, ce qui réduit l'erreur $\varepsilon_i$ indépendamment des autres. Dans ce compte-rendu, on démontre la condition nécessaire dans $GF(p^m)$ pour qu'un tel ensemble existe. Partons de la propriété de l'interpolation de Lagrange suivante :

$$\sum_{i=1}^{k} \ell_i(x) = 1$$

Tous les $\ell_i(x)$ partitionnent l'unité. Le secret étant évalué en $x = 0$, cela revient à calculer :

$$\sum_{i=1}^{k} \ell_i(0) = 1$$

Considérons $\ell_i(0) = \lambda$ où $\lambda$ est une constante.

$$\sum_{i=1}^{k} \ell_i(0) = \sum_{i=1}^{k} \lambda = \lambda k = 1$$

Fixons $\lambda = 1$. Pour tout $k$, on a alors la condition $k = 1$ en tant qu'élément de $GF(p^m)$. Cela revient alors à poser :

$$\begin{aligned} & k \equiv 1 \bmod p \\ \Leftrightarrow\ & k - 1 \equiv 0 \bmod p \\ \Leftrightarrow\ & p \mid (k-1) \end{aligned}$$

En $GF(2^8)$, il est donc clair qu'un tel ensemble existe si 2 divise $k-1$, donc si $k$ est impair.

Dans le cas où $k$ est pair, une idée pourrait être de partager une clé pour chaque participant encodant une $k+1$-ème part secrète afin d'effectuer le partage de secret à l'aide d'un seuil $k+1$ impair.

Par ailleurs, certaines propriétés semblent avoir lieu de manière générale dans $GF(2^m)$ mais n'ont pas été démontrées avec succès. Par exemple, s'il existe un tel ensemble, alors :

1. l'ensemble des $x_i$ somme à 0 dans le corps fini.

2. il existe au moins un ensemble contient l'élement $x_1 = 1$.

D'autres essais ont été menés, par exemple en essayant de comprendre la relation entre les entiers et les corps finis pour calculer une distance, ce qui rendait également difficile de concevoir une raison pour laquelle certains ensembles ne respectant pas la propriété 1 ci-dessus, possédaient des PSNR très différents (par exemple 34 dB versus 16 dB) lorsque $k = 3$.

# 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.
2. Analyser en détail l'impact de l'erreur $\delta$ 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 ICAR** (Mardi 04/11/2025)
« Conception d'un algorithme léger pour la détection temps réel de la mégafaune marine par drone aérien » – Martin Simonoviez

# Références

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