Compte-rendu hebdomadaire

Compte-rendu 5

Valentin Noyé

27 octobre 2025 - 31 octobre 2025

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

1 Résumé des tâches réalisées cette semaine

1. Lecture et compréhension de l'article IPTA de Laura Bertojo.
2. Section 2.1 – Mis en place d'un tableau de références dans le domaine du partage d'images secrètes.
3. Section 2.2 – Étude du choix de la position d'évaluation des polynômes sur la minimisation de l'erreur dans $GF(2^8)$. Étude du cas particulier où $k = 3$ selon une précédente observation et ouverture sur une éventuelle formulation générale.

2 Travail réalisé

2.1 Étude des méthodes en partage d'images secrètes

L'étude menée par Saha *et al.* [1] contient un grand nombre d'éléments nécessaires afin de comprendre le partage d'images secrètes (SIS). En l'occurrence, il met en valeur certains articles en SIS sur la base du partage de secrets de Shamir (PSIS) [2] qui peuvent tout à fait nous intéresser. Ainsi, de tels articles et d'autres non-référencés dans cette étude sont présent dans le tableau à l'adresse suivante : Lien du Google Sheets.

2.2 Étude du choix de la position d'évaluation des polynômes sur la minimisation de l'erreur dans $GF(2^8)$

2.2.1 Cas particulier : $k = 3$

Soit un ensemble $\{x_a, x_b, x_c\}$ de points d'évaluation d'un polynôme $p(x)$ de degré $k - 1 = 2$ encodant un secret S à partir de la méthode de partage de secrets de Shamir. Soit $y_i = p(x_i)$ pour $i \in \{1, \dots, k\}$. Selon l'interpolation de Lagrange, l'erreur totale ε est calculée par cumul des erreur $\varepsilon_i = y_i - y_i'$ où y_i' est la valeur de y_i érronnée ou non, et obtenue à la réception du message :

$$\varepsilon = \sum_i \varepsilon_i \ell_i(0) \tag{1}$$

et $\ell_i(0)$ est le polynôme de base de Lagrange d'indice i évalué en 0 :

$$\ell_i(0) = \prod_{i \neq j} \frac{x_j}{x_i - x_j} \tag{2}$$

Dans un précédent compte-rendu, nous avons noté qu'il existe des résultats de reconstruction optimaux pouvant être générés lorsque cette propriété est vraie :

$$x_a \oplus x_b \oplus x_c = 0, \tag{3}$$

où l'opération $\oplus$ représente un XOR.

En effet, le tableau 1 montre les meilleurs résultats obtenus lorsque cette propriété est vraie. Le PSNR moyen est de 37,2052 dB sur l'image de la grenouille et sur 500 configurations de x_i différentes.

PSNR (dB)	39,3816	39,2090	38,7489	38,7346	38,7215
$\{x_a, x_b, x_c\}$	$\{178, 143, 61\}$	$\{194, 239, 45\}$	$\{114, 11, 121\}$	$\{124, 1, 125\}$	$\{225, 182, 87\}$

TABLE 1 – Meilleurs résultats obtenus lorsque $x_a \oplus x_b \oplus x_c = 0$

En revanche, le tableau 2 montre que les meilleurs résultats obtenus sans cette propriété sont moins bons, avec un PSNR moyen de 19,2975 dB sur 500 configurations de x_i différentes. Or, certaines configurations réduisent tout de même l'erreur.

PSNR (dB)	34,5023	31,8235	30,5165	29,7341	28,7784
$\{x_a, x_b, x_c\}$	$\{168, 197, 78\}$	$\{131, 178, 48\}$	$\{4, 43, 162\}$	$\{211, 144, 175\}$	$\{127, 114, 254\}$

TABLE 2 – Meilleurs résultats obtenus lorsque $x_a \oplus x_b \oplus x_c \neq 0$

On explique alors cette observation. Tout d'abord, on en déduit que quelque soit $\ell_i(0)$, une valeur élevée amplifie l'erreur. Or $\ell_i(0) = 0$ est impossible car une multiplication de tout $j \neq i \neq 0$ dans le numérateur ne peut être 0. Dans ce cas, obtenir $L_i(0) = 1$ pour tout i serait donc optimal et minimiserait la valeur absolue.

Il en découle de l'équation (3) que dans $GF(2^8)$, cette propriété est similaire à :

$$\begin{aligned} x_a &= x_b - x_c \\ x_b &= x_a - x_c \\ x_c &= x_a - x_b \end{aligned} \tag{4}$$

Considérons alors $\ell_a(0)$, $\ell_b(0)$ et $\ell_c(0)$. En développant chacun des polynômes de base de l'équation (2), nous obtenons :

$$\ell_a(0) = \frac{bc}{(a-b)(a-c)}, \quad \ell_b(0) = \frac{ac}{(b-a)(b-c)}, \quad \ell_c(0) = \frac{ab}{(c-b)(c-a)} \tag{5}$$

Selon l'équation (4), on en conclue donc :

$$\ell_a(0) = \frac{(a-b)(a-c)}{(a-b)(a-c)} = 1, \quad \ell_b(0) = \frac{(b-a)(b-c)}{(b-a)(b-c)} = 1, \quad \ell_c(0) = \frac{(c-b)(c-a)}{(c-b)(c-a)} = 1 \tag{6}$$

Ainsi, en calculant l'erreur totale ε selon l'équation (1), on obtient :

$$\varepsilon = \sum_i \varepsilon_i \tag{7}$$

L'erreur finale ε est alors minimale.

2.2.2 Ouverture sur un possible cas général

Il est intéressant d'étudier l'observation précédente sur d'autres valeurs de k. L'idée est de trouver un moyen de générer une configuration optimale telle que tout $\ell_i(0)$ dans (1) soit évalué à 1. Le tableau 3 montre que certaines de ces configurations existent pour différents k.

k	Ensembles de x_i
3	$\{1, 2, 3\}$
5	$\{78, 110, 121, 129, 216\}$
7	$\{22, 23, 110, 173, 202, 230, 238\}$
9	$\{1, 16, 32, 102, 108, 131, 151, 203, 228\}$
11	$\{33, 41, 63, 93, 106, 151, 160, 194, 212, 220, 253\}$

TABLE 3 – Ensembles de x_i optimaux pour différentes valeurs de k

Or nous constatons que seuls des configurations optimales de x_i pour k impairs semblent exister. En effet, pour k pair, aucune configuration n'a été retrouvé par recherche exhaustive sur des x_i distincts générés aléatoirement tels que tout $\ell_i(0) = 1$.

Une méthode de génération d'un tel ensemble pourrait être intéressante à explorer. Potentiellement, elle ouvrirait également sur la possibilité de minimiser l'erreur quand nous ne pouvons pas garantir $\ell_i(0) = 1$ pour tout i.

Notons que par ailleurs, cette propriété s'avère vraie pour les ensembles du tableau 3 :

$$\bigoplus_i x_i = 0 \tag{8}$$

Cette observation pourrait être utile par la suite.

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 la capacité à reconstruire les coefficients du polynôme de Shamir selon différentes configurations d'erreur.
3. Concrétiser l'application des codes correcteurs d'erreur de Reed-Solomon sur le partage d'images secrètes [3].

4 Activités

4.1 Réunions

Point avec Pauline (Vendredi 31/10/2025)
Nous avons clarifié certains points dans l'article IPTA de Laura Bertojo, et avons discuté des points abordés ci-dessus dans le compte-rendu.

1. Mettre les dates des articles dans le tableau et potentiellement mettre de côté la capacité d'une méthode à être corrigeable.
2. Penser à la réécriture de certaines sections notamment selon des points précédemment abordés par mail.

Références

[1] Sanchita Saha, Arup Kumar Chattopadhyay, Anup Kumar Barman, Amitava Nag, and Sukumar Nandi. Secret image sharing schemes : A comprehensive survey. *IEEE Access*, 11 :98333–98361, 2023.

[2] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11) :612–613, November 1979.

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