Compte-rendu hebdomadaire

Compte-rendu 1

Valentin Noyé

1 octobre 2025 - 3 octobre 2025

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

1 Résumé des tâches réalisées cette semaine

1. Introduction aux enjeux et attendus du doctorat : correction de parts bruitées pour la reconstruction d'images secrètes partagées.
2. Section 2.1 – Étude sommaire des corps de Galois (GF) appliqués à la cryptographie (AES, partage de secrets de Shamir [1]).
3. Section 2.2 – Premières recherches sur le partage de secrets de Shamir [1] et sur son application sur des images dans les corps de Galois $GF(251)$ [2, 3] et $GF(2^8)$ [3, 4] à partir de la méthode de Shamir appliquée sur chaque pixel, et à partir de la méthode de Thien & Lin [2].

2 Travail réalisé

2.1 Étude des corps de Galois (corps finis)

Quand on s'intéresse à des opérations entières avec des polynômes en cryptographie, la majorité des recherches à ce sujet emploient les corps de Galois (corps finis), et notamment les corps premiers $GF(p)$ où p est un nombre premier, pour leurs propriétés en arithmétique modulaire. En particulier, les propriétés suivantes sont particulièrement intéressantes :

1. Tout corps premier d'ordre p est muni d'entiers $a < p$, ce qui facilite la manipulation en mémoire.
2. Tout élément a d'un corps premier d'ordre p possède un unique inverse a^{-1} dans ce corps. Cet inverse peut être déterminé par plusieurs méthodes dont la méthode d'Euclide étendue ou selon la propriété $a^{-1} \equiv a^{p-2} \bmod p$, correspondant au petit théorème de Fermat.
3. La division $\frac{\cdot}{a}$ est simplifiée car elle correspond seulement à une multiplication par a^{-1}.

En effet, certaines de ces propriétés nous évitent tout simplement de travailler sur des nombres réels, ce qui rendrait la méthode de partage de secrets de Shamir plus vulnérable [1]. De plus, cela nous permet de recourir à des solutions plus simples et élégantes qu'avec des modulos non-premiers.

Par ailleurs, nous retrouvons plus souvent des extensions des corps premiers $GF(p^m)$ avec p premier, tels que sur la base de corps binaires $GF(2^m)$ où les opérations se réduisent généralement à des opérations arithmétiques binaires puisqu'elle conserve la relation isomorphique suivante :

$$GF(2^8) \cong \frac{GF(2)[x]}{f(x)}$$

où $f(x)$ est un polynôme irréductible de degré ≤ 7. Par exemple, le standard cryptographique AES emploie des opérations dans le corps $GF(2^8)$ à partir d'un polynôme irréductible $f(x) = x^8 + x^4 + x^3 + x + 1$ que nous utiliserons. Par ailleurs, $GF(2^8)[x]$ représente un polynôme sur 8 bits où chaque coefficient $a_i \in \{0, 1\}$. Ainsi, dans un tel cas, les opérations se simplifient de la sorte :

1. Le polynôme irréductible est simplement représenté par le code binaire `0x1B`.
2. L'addition de deux nombres $a, b \in GF(2^8)$ correspond à un XOR $c = a \oplus b$.
3. La multiplication de deux nombres $a, b \in GF(2^8)$ est effectuée suivant la méthode égyptienne suivie d'une reduction ($\oplus$) par $f(x)$.
4. L'inversion peut être effectuée de manière efficace selon le petit théorème de Fermat, car l'exponentiation en base 2 correspond à un simple décalage de bits.

2.2 Partage d'images secrètes

2.2.1 Partage de secrets de Shamir

Le partage d'images secrètes repose sur la méthode des polynômes de Shamir [1]. Supposons une donnée secrète D, nous souhaitons la partager en n parts telles que k parts sont suffisantes pour la reconstruire, et $k - 1$ parts ne permettraient pas de retrouver la donnée d'entrée. Dans son article, Shamir stipule qu'un secret peut être dissimulé dans la constante d'une fonction interpolable, telle qu'un polynôme de degré $k - 1$ de la forme $q(x) = D + a_0 x + a_1 x^2 + \ldots + a_{k-1} x^{k-1} \bmod p$ où p est un nombre premier et a_i sont des coefficients tirés aléatoirement depuis une distribution uniforme.

Puisque k points sont suffisant pour retrouver les coefficients du polynôme et donc la donnée cachée D, n parts du secret sont attribuées à divers détenteurs sous la forme de points $(x_i, y_i) = (x_i, q(x_i))$ du polynôme $q(x)$ avec $1 \leq i \leq n$, parmi lesquels k d'entre eux permettent de reconstruire cette donnée.

Le processus de reconstruction le plus courant est mené par la méthode de Lagrange. Soit k parts $(x_1, y_1), \ldots, (x_k, y_k)$, le polynôme $q(x)$ peut être retrouvé à partir de la formule suivante :

$$q(x) = \sum_{i=1}^{k} y_k \prod_{j=1, i \neq j}^{k} \frac{x - x_j}{x_i - x_j} \bmod p. \tag{1}$$

En particulier, dans $GF(p)$, la division se traduit par une multiplication par l'inverse que l'on peut déterminer par les méthodes décrits dans la section 2.1 :

$$q(x) = \sum_{i=1}^{k} y_k \prod_{j=1, i \neq j}^{k} (x - x_j)(x_i - x_j)^{-1} \bmod p. \tag{2}$$

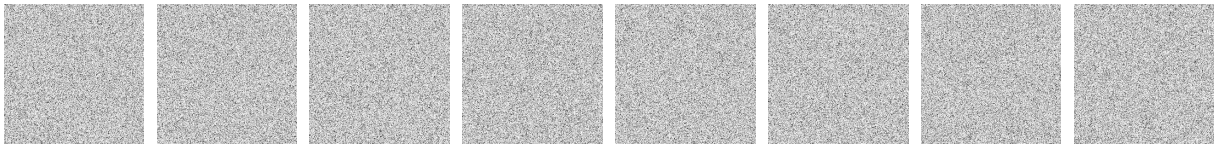
Car le secret D est la constante de $q(x)$, nous évaluons alors $q(0)$. Le secret est finalement reconstruit de la sorte :

$$D = q(0) = \sum_{i=1}^{k} y_k \prod_{j=1, i \neq j}^{k} -x_j (x_i - x_j)^{-1} \bmod p. \tag{3}$$

2.2.2 Partage d'images secrètes selon Shamir

Tout d'abord, nous nous intéressons à l'application du partage de secrets de Shamir sur les pixels individuels de l'image. Shamir opère dans un groupe Galois d'ordre p, Thien & Lin [2] ainsi que Qin *et al.* [3] emploient ainsi $p = 251$ qui est la valeur première de 8 bits la plus proche de 255, ce qui signifie que nous sommes en mesure de travailler dans $GF(251)$ mais également

d'être constraints d'encoder 250 valeurs de pixels. Pour ce faire, la méthode que ces chercheurs utilisaient consiste à réduire les pixels de valeurs $[251, 255]$ à 250, ce qui représente une faible perte de nuances à valeurs elevées. Dans la figure 1, nous décomposons une image en $n = 8$ parts avec un seuil $k = 4$.



$x_1 = 1$ $x_2 = 2$ $x_3 = 3$ $x_4 = 4$ $x_5 = 5$ $x_6 = 6$ $x_7 = 7$ $x_8 = 8$

FIGURE 1 – Les $n = 8$ parts de N pixels permettant la reconstruction de l'image

Cette image peut alors être reconstruite avec $k = 4$ parts, comme nous le constatons dans la figure 2. Avec $k - 1$ parts, nous ne sommes pas en mesure de reconstruire l'image. Puisque la reconstruction est avec perte, le PSNR évalué entre l'image d'origine et sa reconstruction est de 37,1616 dB.

(a) Image originale (b) $x_i = \{1, 2, 3, 4\}$ (c) $x_i = \{2, 5, 6, 7\}$ (d) $x_i = \{2, 6, 7\}$

FIGURE 2 – Reconstruction d'une image de N pixels dans $GF(251)$ avec $k = 4$ et $n = 8$

En revanche, si nous travaillons dans un groupe Galois $GF(2^8)$ tel que dans Qin *et al.* [3] et Yang *et al.* [4] suivant un procédé similaire mais en considérant les opérations indiquées dans la section 2.1, nous éliminons la perte de nuances dans l'image. Ainsi, l'image reconstruite est totalement identique à l'image d'entrée, tel que dans la figure 3.

(a) Image originale (b) $x_i = \{1, 2, 3, 4\}$ (c) $x_i = \{2, 5, 6, 7\}$ (d) $x_i = \{2, 6, 7\}$

FIGURE 3 – Reconstruction d'une image de N pixels dans $GF(2^8)$ avec $k = 4$ et $n = 8$

2.2.3 Partage d'images secrètes selon Thien et Lin

Le partage d'images secrètes telle qu'implementée par Thien & Lin [2] se base sur le partage de secret de Shamir mais fournit une observation supplémentaire. En effet, tandis que Shamir utilise la constante du polynôme secret afin de masquer la donnée secrète (le pixel), Thien & Lin

considèrent l'ensemble des coefficients $a_i \in [0, 251[$ du polynôme $r(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$ comme détenteurs de plusieurs secrets, soit un groupe de k pixels où chacun est encodé dans un coefficient a_i. En effet, cette méthode permet de réduire la quantité d'information dans chacune des parts à $\lceil \frac{N}{k} \rceil$ pixels pour une image d'entrée de N pixels en encodant plusieurs pixels dans une unique part qui, lorsque complétée avec les $k-1$ autres parts, reconstruit cet ensemble de pixels. Ainsi, l'ensemble des coefficients peut être simplement déterminé en redéfinissant $r(x)$ par interpolation de Lagrange telle que décrite dans l'équation (2).

La figure 4 montre $n = 8$ parts avec $k = 4$ appliquées sur une image. L'avantage que nous avons ici concerne la quantité d'information contenue dans chacune des parts qui est alors réduite à $\lceil \frac{N}{4} \rceil$ pixels. Nous voyons que la part avec l'indice le plus faible ($x_1 = 1$) fait légèrement paraître le contenu de l'image. Pour cette raison, Thien & Lin ont introduit une étape optionnelle de permutation des pixels pour éviter que l'information soit découverte de la sorte.

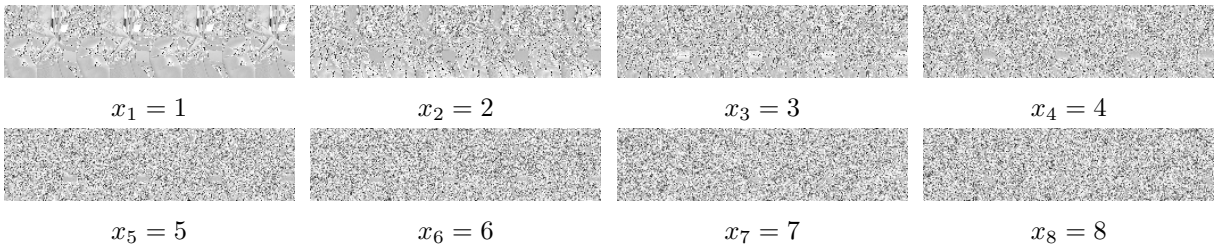


FIGURE 4 – Les $n = 8$ parts de $\lceil \frac{N}{4} \rceil$ pixels ($k = 4$) permettant la reconstruction de l'image par la méthode de Thien & Lin [2]

Dans la figure 5, nous reconstruisons l'information avec k différentes parts. Dans $GF(251)$, nous constatons la même perte que précédemment, avec un PSNR de 37,1616 dB. Il n'est pas possible de reconstruire une image avec $k-1$ parts car il n'y a pas suffisamment d'information dans chacune des parts du à la réduction du nombre de pixels dans celles-ci.

(a) Image originale (b) $x_i = \{1, 2, 3, 4\}$ (c) $x_i = \{2, 5, 6, 7\}$

FIGURE 5 – Reconstruction d'une image de N pixels dans $GF(251)$ avec $k = 4$ et $n = 8$ par la méthode de Thien & Lin [2]

3 Travail à effectuer

1. Continuer la recherche et le développement de méthodes de partage d'images secrètes de l'état de l'art.
2. Commencer la recherche ainsi que l'analyse de la reconstruction d'image secrètes lorsque des parts sont bruitées.

4 Activités

— **Réunions :**

1. Réunion d'accueil en doctorat, explication du sujet et des pistes de recherche, du fonctionnement du doctorat, des attendus et du travail à effectuer – Mercredi 01/10/2025

Références

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

[2] Chih-Ching Thien and Ja-Chen Lin. Secret image sharing. *Computers Graphics*, 26(5) :765–770, 2002.

[3] Chuan Qin, Chanyu Jiang, Qun Mo, Heng Yao, and Chin-Chen Chang. Reversible data hiding in encrypted image via secret sharing based on gf(p) and gf(2**8). *IEEE Transactions on Circuits and Systems for Video Technology*, 32(4) :1928–1941, 2022.

[4] Ching-Nung Yang, Tse-Shih Chen, Kun Hsuan Yu, and Chung-Chun Wang. Improvements of image sharing with steganography and authentication. *Journal of Systems and Software*, 80(7) :1070–1076, 2007. Dynamic Resource Management in Distributed Real-Time Systems.