How to share a secret ?

Schémas de partage de secret et Constructions

Sommaire

- Définition : Schéma de partage de secret
- Un premier exemple : Le partage de secret de Shamir
- Introduction au codes linéaires : donner des exemples de code linéaires
- Construction de schéma de partage de secret à partir de code linéaire
- Vers une problématique de schéma de partage de secret “boite noir” (black box secret sharing scheme)

Définition : Schéma de partage de secret

“Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed ? What is the smallest number of keys to the locks each scientist must carry ?”

Liu, C.L. Introduction to Combinatorial Mathematics. McGrawHill, New York, 1968.

Définition : Schéma de partage de secret

Utilité ?

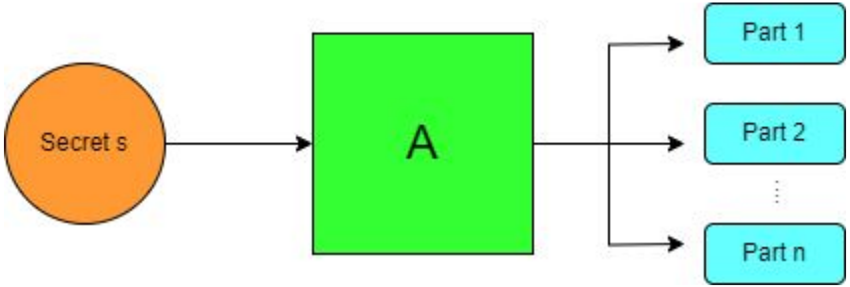
- Gestion de clés cryptographiques
- Trop peu sécure de stocker les clés dans un seul endroit (problème de disponibilité)
- Trop dangereux de stocker plusieurs copies de clés (augmente le risque de fuite de clés)

-> trouver un moyen de sorte qu'un certains nombre de jetons **k** permettent de retrouver un secret tandis que pour k-1 jetons ou moins, cette opération est impossible

Définition : Schéma de partage de secret

Composé de deux algorithmes :

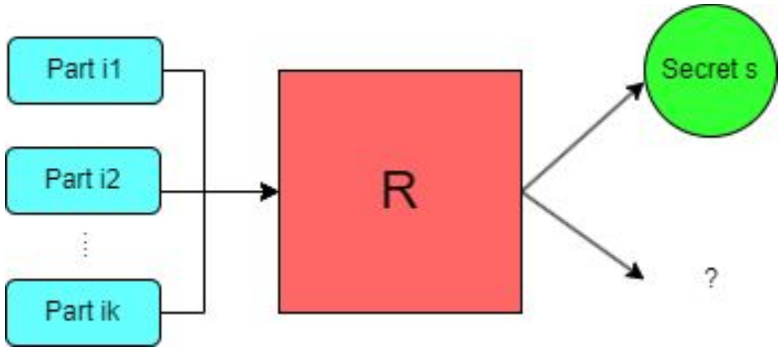
- Un algorithme non déterministe qui, étant donné un secret **s,** retourne **n** parts de ce secret



Définition : Schéma de partage de secret

Composé de deux algorithmes :

- Un algorithme **A** non déterministe qui, étant donné un secret **s,** retourne **n** parts de ce secret
- Un algorithme déterministe de reconstruction **R** qui retourne ou non le secret initial dépendant des parts données en input



Si suffisamment d'informations est données en input

Sinon

Propriétés d’un schéma de partage de secret : “à Seuil”

- Si il est possible de retrouver le secret à partir de **k** parts, peu importe lesquelles
- Dans le cas où on dispose de moins de **k** parts, on ne trouve AUCUNE information sur le secret

n = nombre de part, k = le seuil de reconstruction

Partage de secret de Shamir

1 - On utilise le polynôme suivant pour représenter le secret : $f(x) = s + a_1 * x + a_2 * x^2 + \cdots + a_{k-1} * x^{k-1}$

où les coefficients $a_1, a_2, \ldots, a_{k-1}$ sont générés aléatoirements et **s** est le secret

Partage de secret de Shamir

1 - On utilise le polynôme suivant pour représenter le secret : $f(x) = s + a_1 * x + a_2 * x^2 + \cdots + a_{k-1} * x^{k-1}$

où les coefficients $a_1, a_2, \ldots, a_{k-1}$ sont aléatoires et **s** est le secret

2 - Pour la générations des parts :

on considère **n** points d'évaluation $x_1, x_2, \ldots, x_n$ de sorte que chacunes des parts sera le couple (x_i, y_i)

Partage de secret de Shamir

1 - On utilise le polynôme suivant pour représenter le secret : $f(x) = s + a_1 * x + a_2 * x^2 + \cdots + a_{k-1} * x^{k-1}$

où les coefficients $a_1, a_2, \ldots, a_{k-1}$ sont aléatoires et **s** est le secret

2 - Pour la générations des parts :

on considère **n** points d'évaluation $x_1, x_2, \ldots, x_n$ de sorte que chacunes des parts sera le couple (x_i, y_i)

3 - La reconstruction du secret : reconstruire le polynôme initial avec les k points (ou parts) donnés en input

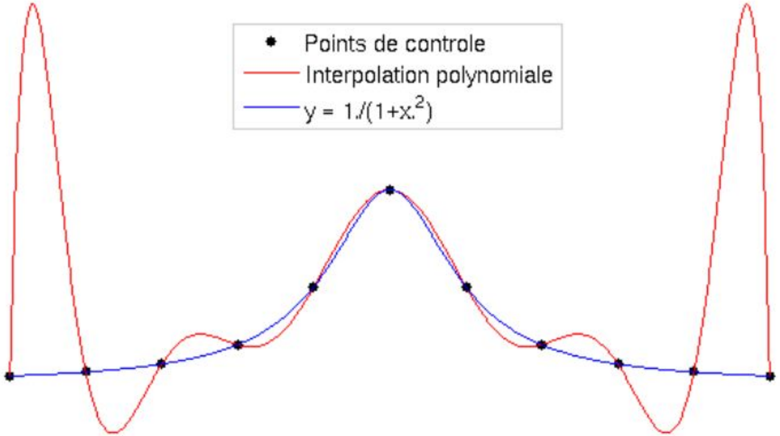
$$P_n(x) = \sum_{j=0}^{n} y_j L_j(x) \quad \text{, avec} \quad L_j(x) = \prod_{\substack{k=0 \\ k \neq j}}^{n} \frac{x - x_k}{x_j - x_k}$$

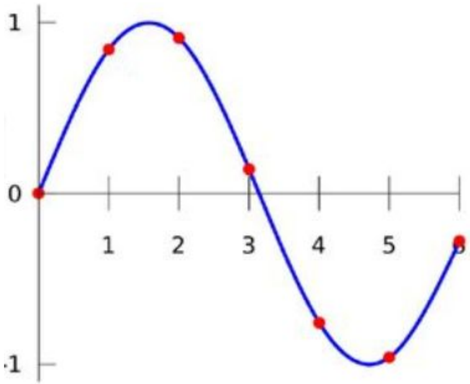
Partage de secret de Shamir

Quelque commentaires :

- Avec k parts, on obtient l'unique polynôme de degrés k qui passe par les points donnée en entré, on retrouve bien un seul et même résultat
- Si on a strictement plus de k parts : les coefficients de degré supérieur à k-1 s'annulent et le résultat reste inchangé (propriété de l'interpolation polynomiale)
- Si on a strictement moins de k part, il est impossible de retrouver le polynôme initial (et le brute-force est, par conséquent, impossible)

Interpolation polynomiale





Partage de secret de Shamir : implémenté sur Ubuntu

NAME

```
ssss - Split and Combine Secrets using Shamir's Secret Sharing Scheme.
```

SYNOPSIS

```
ssss-split -t threshold -n shares [-w token] [-s level] [-x] [-q] [-Q] [-D] [-v]

ssss-combine -t threshold [-x] [-q] [-Q] [-D] [-v]
```

DESCRIPTION

```
ssss  is an implementation of Shamir's Secret Sharing Scheme. The program suite does both:
the generation of shares for a known secret, and the  reconstruction  of  a  secret  using
user-provided shares.
```

COMMANDS

```
ssss-split: prompt the user for a secret and generate a set of corresponding shares.

ssss-combine: read in a set of shares and reconstruct the secret.
```

https://manpages.ubuntu.com/manpages/trusty/man1/ssss-combine.1.html

Code linéaires : Définition

On défini un code sur le corps $\mathbb{F}_q$ de longueur **n** et de dimension **k,** un sous-espace linéaire de $\mathbb{F}_q^n$ de dimension **k.**

Un code linéaire est généré par une matrice de taille k x n à valeur dans $\mathbb{F}_q$

$$\begin{array}{cc} & \xrightarrow{\qquad n \qquad} \\ k \Big\downarrow & \begin{matrix} a11 & a12 & \dots & a1n \\ . & & & \\ . & & & \\ . & & & \\ ak1 & ak2 & \dots & akn \end{matrix} \end{array}$$

$\mathbb{F}_q$ = Corps de taille q

Une propriété intéressante : Codes MDS

- MDS pour “minimum distance separable”
- Signifie que “pour **k** colonnes de la matrice génératrice (peu importe lesquelles), la sous-matrice carrée composée de ces k colonnes est de rang **k**”
- Lien direct entre les schéma de partage de secret à seuil et les codes MDS

$$\mathbf{Rang}\left(\begin{array}{c} \xrightarrow{\quad k \quad} \\ \begin{array}{cccc} a(1,i\_1) & a(1,i\_2) & \dots & a(1,i\_n) \\ . & & & \\ . & & & \\ . & & & \\ a(k,i\_1) & a(k,i\_2) & \dots & a(k, i\_n) \end{array} \end{array} \Bigg\downarrow k \right) = \mathbf{k \ (max)}$$

Code linéaires : Schéma à partir de codes ?

On défini un code sur le corps $\mathbb{F}_q$ de longueur **n** et de dimension **k,** un sous-espace linéaire de $\mathbb{F}_q^n$ de dimension **k.**

Un code linéaire est généré par une matrice de taille k x n à valeur dans $\mathbb{F}_q$

n

k

a11 a12 … a1n
.
.
.
ak1 ak2 … akn

s , g1 , g2 , … , gk-1 X [matrice k x n] = Share 1 Share 2 … Share n

s = secret
gi = aléas

Code linéaires : Décoder un secret ?

Supposons avec un ensemble suffisant de **k** parts

Share i_1 | Share i_2 | … | Share i_k

et la sous-matrice correspondante

$$\begin{array}{c} \xrightarrow{\quad k \quad} \\ \begin{bmatrix} a(1,i\_1) & a(1,i\_2) & \dots & a(1,i\_n) \\ . & & & \\ . & & & \\ . & & & \\ a(k,i\_1) & a(k,i\_2) & \dots & a(k, i\_n) \end{bmatrix} \end{array} \Big\downarrow k$$

s = secret

gi = aléas

Code linéaires : Décoder un secret ?

Le message peut-être retrouvé si on **inverse** cette dernière sous-matrice

$$\text{Share } i\_1 \quad \text{Share } i\_2 \quad \dots \quad \text{Share } i\_k \; \text{X} \begin{pmatrix} a(1,i\_1) & a(1,i\_2) & \dots & a(1,i\_n) \\ . & & & \\ . & & & \\ . & & & \\ a(k,i\_1) & a(k,i\_2) & \dots & a(k, i\_n) \end{pmatrix}^{-1} = \mathbf{s}\text{ , g1 , g2 , } \dots \text{ , gk-1}$$

s = secret
gi = aléas

Exemple de code linéaires : code de Reed-Solomon

- définie par la matrice génératrice suivante :

$$\begin{bmatrix} 1 & a_0 & a_0^2 & \dots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \dots & a_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \dots & a_{n-1}^{k-1} \end{bmatrix}$$

où $a_0, a_2, \dots, a_{n-1}$ sont des coefficients distincts deux à deux

Exemple de code linéaires : code de Reed-Solomon

On génère un vecteur de taille k contenant le secret (ici **m0** est le secret et le rest des coefficients sont des aléas)

$$\begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \cdots & a_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ \vdots \\ m_{k-1} \end{bmatrix}$$

s

aléatoires

Pour aller plus loin : Les partages de secret “Boite Noire”

- Pour un corps donné, n et k connues : facile de construire un schéma de partage de secret (limitation sur la taille du corps qui doit être supérieure à **n** pour RS)
- Le but : pouvoir instancier un seul et même schéma qui fonctionnerait pour tous les groupes
- Plus versatile mais aussi plus compliqué à faire

-> des schémas existent déjà mais ils demandent à chaque parties de gérer un nombre de parts important (facteur d'expansion)

Pour aller plus loin : Les partages de secret “Boite Noire”

-> Lecture : “Blackbox Secret Sharing Revisited: A Coding-Theoretic Approach with Application to Expansionless Near-Threshold Schemes” R. Cramer & C. Xing

Expliquent comment générer la matrice sur Z d’un schéma de partage de secret à seuil boite noire avec un facteur d'expansion satisfaisant

Références :

- https://eprint.iacr.org/2019/1134 (BBSSS)
- https://membres-ljk.imag.fr/Pierre.Karpman/cry_adv2021_secsha.pdf (codes linéaires)
- https://en.wikipedia.org/wiki/Reed–Solomon_error_correction (Reed solomon)
- https://web.mit.edu/6.857/OldStuff/Fall03/ref/Shamir-HowToShareASecret.pdf (partage de Shamir)
- https://manpages.ubuntu.com/manpages/trusty/man1/ssss-combine.1.html