Le calcul multi-parties sécurisé

1 INTROUCTION

La cryptographie génère une multitude de services : chiffrement, signature, identification et calcul multi-parties. Ce dernier permet à plusieurs parties de calculer en collaboration une fonction publique sans dévoiler les paramètres privés. Le premier protocole qui s'inscrit dans ce cadre est celui de Yao, Andrew Chi-Chih. 1982. Ce protocole consiste à résoudre le problème des millionnaires, ce qui permet à deux individus (ou plus) de comparer leur fortune respective sans la divulguer. Soit deux participants Alice et Bob dont les valeurs privées respectives sont notées a et b.

Alice désire calculer $f_1(a,b)$ et Bob souhaite déterminer $f_2(a,b)$.

Un protocole de calcul multi-parties peut être noté sous la forme de la fonction suivante

$f : (a,b) \rightarrow (f_1(a,b), f_2(a,b))$

Le protocole ne permet donc pas à un adversaire d'un apprendre plus qu'il ne sait déjà sur la valeur des participants.

Une solution sécurisée pour l'évaluation de la fonction f est d'envoyer las valeurs privées à une tierce partie de confiance. Cette dernière calcule la fonction f et envoies le résultat à chaque partie. Ce qui amène un partage de secret implicite entre les différentes sans le divulguer.

2 DEMARCHE :

Intuitivement, si Alice possède un secret (nombre) s ($s \in Zn$), elle veut distribuer son secret entre trois parties P_1,P_2, P_3 . Elle procède selon les étapes suivantes :

Etape1:

Alice choisit aléatoirement r_1, $r_2 \in \{0,1,\ldots,p-1\}$ où p est un nombre premier et calcule:

$r_3=s-r_1-r_2 \bmod p$ $\quad\quad$ $s= r_1+r_2+r_3 \bmod p$

Etape 2:

Alice fournit à P_1 les valeurs r_2, r_3

Alice fournit à P_2 les valeurs r_1, r_3

Alice fournit à P_3 les valeurs r_1, r_2

Les valeurs r_1, r_2, r_3 sont appelées les partages du secret

Etape 3:

Chacune deux parties peuvent reconstituer le secret ie P_1 et P_2 peuvent calculer $s = r_1+r_2+r_3$

Remarque: une partie seule ne peut pas retrouver le secret.

3 SCHEMA DE PARTAGE DE SECRET

Un donneur D qui possède le secret

N parties P1,…, Pn

C'est une méthode qui permet au donneur (possède un secret) de distribuer le partage du secret à n parties. La collaboration de plusieurs parties permet de reconstruire le secret.

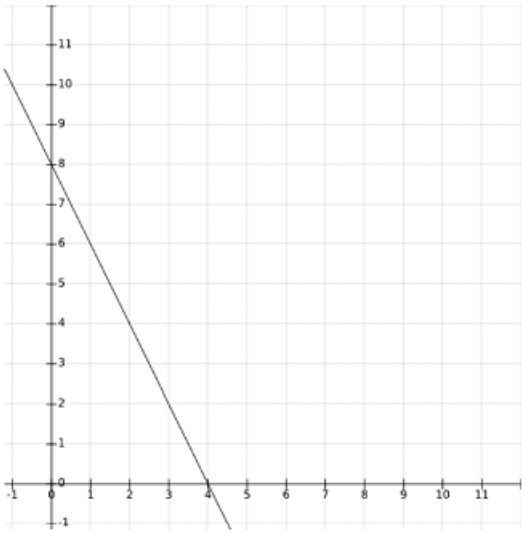
Définition :

Un schéma de partage de secret à seuil k (threshold secret sharing) est un schéma qui vérifie les conditions tel que :

- k parties prises parmi ces n peuvent reconstituer le secret
- Une partie seule ne peut retrouver aucune information sur le secret

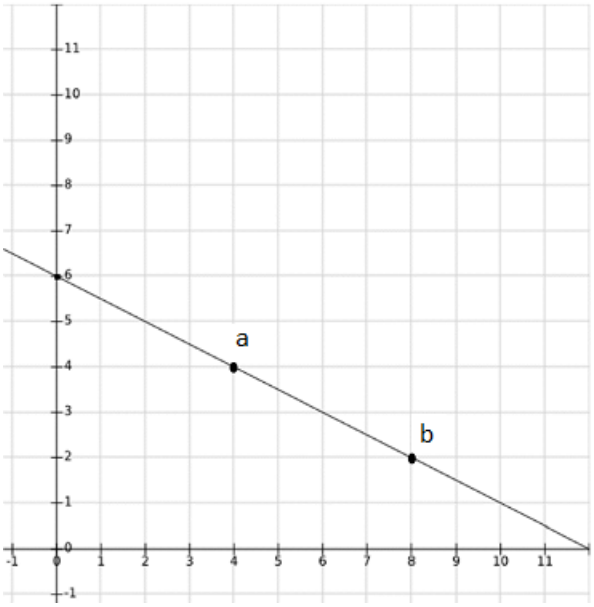
- (k − 1) parties ne peuvent pas reconstituer le secret.

Le partage de secret peut être réalisé grâce aux polynômes et du tracé de leurs graphes. Soit le droite f(x)= 8 – 2x. La projection de la droite sur les axes x et y respectivement sont 4 et 8 respectivement.



On peut se poser la question : combien de lignes droites passent par le point (5, 4)? La réponse, il y a une infinité de droites. De même, quelle est la valeur f(0) pour ces droites ? La réponse est que la projection sur l'axe des y est quelconque.

Cependant, si on prend deux points a et b de l'espace orthonormé, on est sûr qu'il y a une seule droite qui passe par ces deux points telle que le montre la figure suivante :



Maintenant, quelle est la projection de cette droite sur l'axe y ? la réponse est 6, f(0)=6 .

On utilisant les droites on peut partager le secret entre plusieurs parties tels que le point de projection de la droite avec l'axe des y est le secret et les partages de secret sont des points appartenant à la droite.

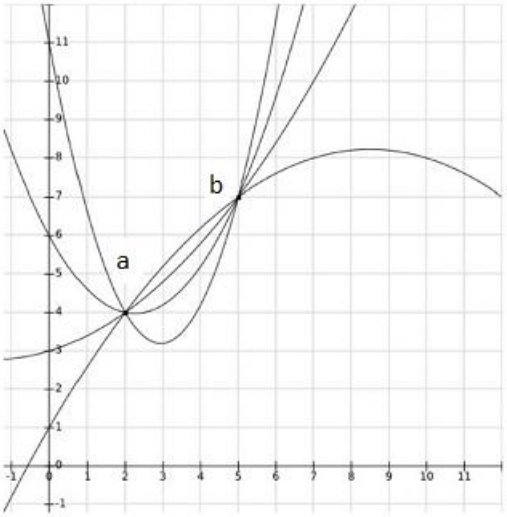
Si Alice possède un secret le nombre 6 et veut le partager entre Bob et Charlie. Alice peut choisir une ligne droite secrète f tel que f(0)=6 et donnera à chacun Bob (4, 4) et Charlie (8, 2) un point de la ligne droite.

La ligne secrète est f(x)=6-0.5x

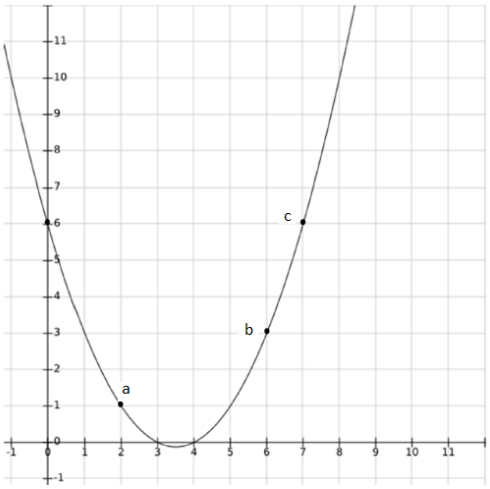
Ensemble Bob et Charlie peuvent calculer la ligne secrète et trouvent le secret f(0)=6

Si Alice donne un autre point à Dave. Qui peut calculer le secret ?

Chaque binôme (Bob, Charlie), (Bob, Dave), (Charlie, Dave) est capable de le faire.
On conclut que la droite permet de fixer le seuil de partage à 2. Si maintenant on désire avoir un seuil de partage supérieur à 2, il ne faut pas utiliser la droite. Cette dernière est exprimée par un polynôme de premier degré. Intuitivement, il faut utiliser des polynômes de degré supérieur.
On constate que pour une courbe quadratique, si on fixe deux points de l'espace orthonormé : il y a plusieurs courbes quadratiques qui passent par ces deux points tels que l'illustre la figure suivante.



Maintenant, si on fixe trois points de l'espace, il y a une seule courbe quadratique qui passe par ces trois points.



Les trois points a, b, c définissent la courbe quadratique définie par $f(x)=6-3.5x+0.5x^2$ et la valeur f(0)=6.
Ensemble Bob (point a), Charlie (point b) et Dave (point c) peuvent calculer la courbe quadratique secrète et trouvent le secret f(0)=6.
Si maintenant Alice donne un autre point à Eve, qui peut retrouver le secret ? Chaque trinôme peut calculer le secret.

Remarque : D'une manière générale, le seuil du partage est définit par le degré du polynôme.

Comment Alice peut-elle partager son secret s à n parties ?
Pour ce faire, Alice construit un polynôme de degré t tel que f(0)=s et calcule :
P_1= f(1), P_2= f(2), …., P_n(n)=f(n)

Exemple ; On a trois parties (points) d'un polynôme de degré 2 avec : f(3)=2, f(4)=1, f(5)=2 . Supposons qu'on est dans Z_{11}=(0,1,2,…,10), comment peut-on reconstruire le secret s = f(0)? Nous devons construire la fonction f qui vérifie ces points. On sait qu'il y a un seul polynôme de degré 2 (fonction f) qui passe par ces trois points. On trouve f et le secret n'est autre que s=f(0).

Voici le procédé pour retrouver f(x) à partir des points f(3)=2, f(4)=1 et f(5)=2. On peut écrire les trois équations suivantes :

f(3)= 1.f(3) +0.f(4) +0.f(5)
f(4)= 0.f(3) +1.f(4) +0.f(5)
f(5)= 0.f(3) +0.f(4) +1.f(5)

de plus f(x) doit être vérifiée pour les trois points fixés, ainsi on écrira :

$f(x)= \delta 3(x).f(3) + \delta 4(x).f(4) + \delta 5(x).f(5)$

avec $\delta 3(x)=1$ si $x=3$ et $\delta 3(x)=0$ si $x=4$ ou 5

$$\delta 3(x)= \begin{cases} 1 \text{ si } x=3 \\ 0 \text{ si } x\neq 3 \text{ et } (x=4 \text{ ou } x=5) \\ \text{on ne sait pas pour les autres valeurs de x} \end{cases}$$

Et si on définit $\delta 3(x)=(x-4)(x-5)/(3-4)(3-5)$

Pour x = 3, $\delta 3(3) = (3-4)(3-5)/(3-4)(3-5) = 1$

Pour x = 4, $\delta 3(4) = 0$ de même pour x = 5, $\delta 3(5) = 0$

En général, $\delta i(x) = \Pi(x-j)/(i-j)$ pour $j = \{3,4,5\}$ et $j \neq i$

$\beta i = \delta i(0) = \Pi(j)/(j-i)$ pour $j = \{3,4,5\}$ et $j \neq i$

ie $\beta 3 = (4/4-3)(5/5-3) = 10$, $\beta 4 = -15$, $\beta 5 = 6$

$f(x) = \delta 3(x).f(3) + \delta 4(x).f(4) + \delta 5(x).f(5)$

Pour f(3) = 2, f(4) = 1, f(5) = 2 on a

$f(x) = \delta 3(x).2 + \delta 4(x).1 + \delta 5(x).2$

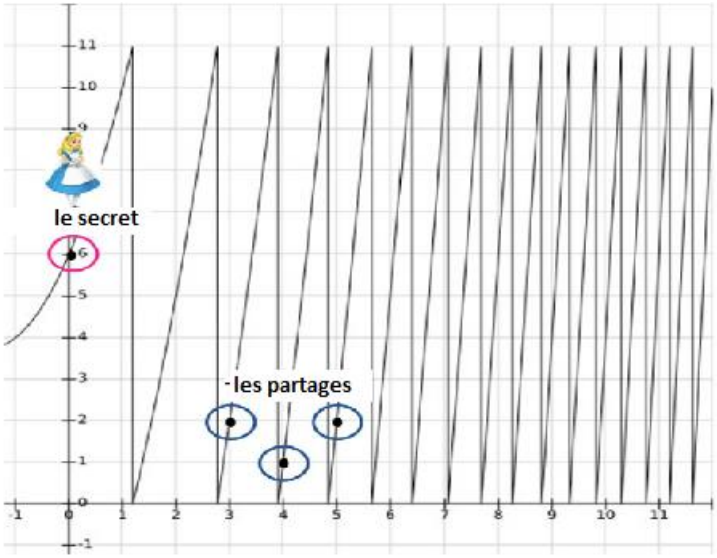
Pour calculer le secret s on a:

$s = f(0) = \beta 3.f(3) + \beta 4.f(4) + \beta 5.f(5)$

Ce qui donne :

$s = f(0) = \beta 3.2 + \beta 4.1 + \beta 5.2$
$=10*2 -15*1 + 6*2$
$=17 \mod 11 =6$ (on est dans Z_{11})

La courbe secrète est: $f(x)=6+3x+x^2 \mod 11$



3.1 PARTAGE DE SECRET DE SHAMIR AVEC SEUIL :
(Shamir Threshold Secret Sharing Scheme)

Le partage de Shamir est basé sur les polynômes, chaque ensemble de t+1 parties (ou plus) peut reconstruire le secret s.

L'algorithme de partage de Shamir est réparti sur trois étapes, comme suite :

étape1:

Soit s le secret que le donneur (Alice) veut partager,

Choisir deux entiers n (nombre de parties) et t (le seuil) tel que $n > t \geq 1$

Alice choisit t valeurs aléatoires $\in Z_p$ où p est un nombre premier et construit le polynôme:

$$f(x) = s+r_1x_1 +r_2x^2 +\dots +r_tx^t$$

rappel:

Le terme constant de f est le secret s = f(0)

Le seuil t: au moins t+1 parties peuvent reconstituer le secret s

étape2:

Pour chaque partie P_i, $i \in \{1,2,\dots, n\}$ le donneur (Alice) calcule :

$s_i= f(i)= s+r_1i^1 +r_2i^2 +\dots +r_ti^t \bmod p$

Et fournit s_i à la partie P_i

étape3: (découverte du secret)

Soient les t+1 parties P1, P2, …, Pt+1

Chaque partie Pi possède son partage $s_i= f(i) \bmod p$

Les t+1 parties peuvent calculer la valeur :

$s_1\beta_1 \quad +s_2\beta_2+\dots \quad +s_{t+1}\beta_{t+1}=s$

Où

$\beta_i= \Pi\, j/(j-i)$ pour $j\in\{1,2,\dots., t+1\}\backslash\{i\}$

Remarque : Le partage de secret de Shamir avec seuil peut être appliqué à différente situation telles que : clés de chiffrement, codes secrets, calcul multi parties sécurisé.

4 CALCUL MULTI PARTIES SECURISE (SMPC) :

Les protocoles SMPC permettent à plusieurs parties de calculer conjointement une fonction f à partir de données privées. Le résultat (valeur de f) est révélée et pas autre chose. On dispose de n parties $P_1, \dots P_n$ chacune possède un secret x_i pour la fonction f. les différentes parties $P_1, \dots, P_n$ collaborent pour calculer $y = f(x_1, \dots, x_n)$

Propriétés de SMPC :

- Correction (correctness) : le résultat y du protocole est la valeur correcte du calcul de $f(x_1, \ldots, x_n)$
- Intimité (Privacy): le résultat y est la seule information révélée à $P_1, \ldots, P_n$

4.1 LE PROTOCOLE SMPC :

Le protocole SMPC se déroule selon les trois étapes suivantes.

Etape1:

Les parties utilisent le protocole de partage de secret et leurs données $x_1, \ldots x_n$

Etape 2:

Chaque partie réalise des calculs sur les valeurs reçues et envoies aux autres parties le résultat calculé

Etape 3:

Chaque partie réalise un calcul pour retrouver le résultat final qui n'est autre que le résultat de la fonction $f(x_1, \ldots, x_n)$.

Soit l'application du protocole SMPC à un système de vote secret.

Etape 1: usage de partage de secret de Shamir (Shamir Secret Sharing Scheme) pour partager les votes x_1, x_2, x_3 d'une manière sécurisée . On choisira le seuil t = 1. On construit alors un polynôme p_1 de degré t=1 qui satisfait $p_1(0)=x_1$

$p_1(x) = x_1+r_1 .x$ où r1 est choisi aléatoirement dans $\{0, 1, \ldots, p-1\}$

On procède au calcul et la distribution des partages du secret x_1:

$p_1(1) = x_1 + r_1 * (1) = s_{1,1}$

$p_1(2) = x_1 + r_1 * (2) = s_{1,2}$

$p_1(3) = x_1 + r_1 * (3) = s_{1,3}$

On fera de même pour x_2 et x_3 en utilisant la construction des polynômes p2 et p3 :

On procède au calcul et la distribution des partages du secret x_2:

On construit alors un polynôme p_1 de degré t=1 qui satisfait $p_2(0)=x_2$

$p_2(x) = x_2+r_2 .x$ où r2 est choisi aléatoirement dans $\{0, 1, \ldots, p-1\}$

$p_2(1) = x_2 + r_2 * (1) = s_{2,1}$

$p_2(2) = x_2 + r_2 * (2) = s_{2,2}$

$p_2(3) = x_2 + r_2 * (3) = s_{",3}$

On procède au calcul et la distribution des partages du secret x_3:

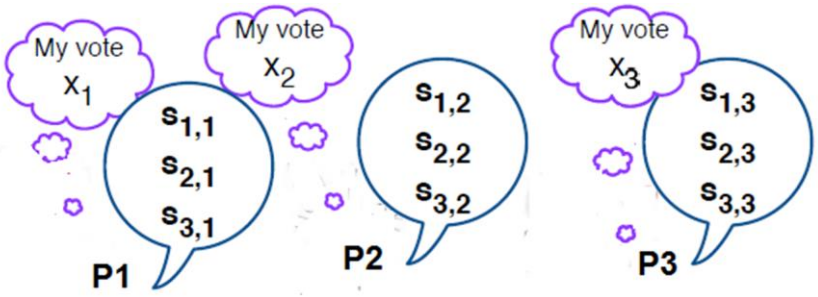
On construit alors un polynôme p_1 de degré t=1 qui satisfait $p_2(0)=x_2$

$p_3(1) = x_3 + r_3 * (1) = s_{3,1}$

$p_3(2) = x_3 + r_3 * (2) = s_{3,2}$

$p_3(3) = x_3 + r_3 \cdot (3) = s_{3,3}$

Après la distribution, chaque partie possède en plus de son secret, des valeurs distribuées par les autres parties. La situation est illustrée par la figure suivante :



Etape 2:

- On calcule pour chaque partie Pi le résultat partiel a_i
- Mettre à jour les partages

  pour P_1 on réalise le calcul suivant

  $$a_1 = s_{1,1} + s_{2,1} + s_{3,1}$$

  Rappel:

  $s_{1,1} = p_1(1)$ où $p_1(x) = x_1 + r_1 * x$

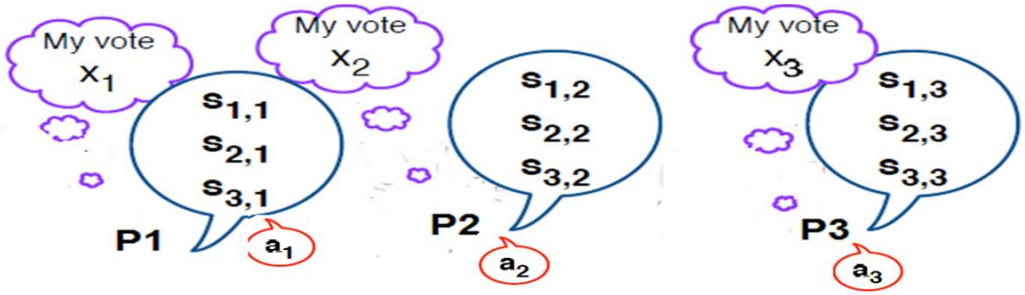
  Note: $a_1 = p_1(1) + p_2(1) + p_3(1)$.

  On fera le même calcul pour P_2 et P_3 on obtiendra a_2 et a_3

  $$a_2 = s_{1,2} + s_{2,2} + s_{3,2}$$

  $$a_3 = s_{1,3} + s_{2,3} + s_{3,3}$$

  on aura la situation illustrée par la figure suivante :



Etape 3:

Chaque partie peut alors calculer le résultat du vote

$y = a_1*\beta_1 + a_2*\beta_2 + a_3*\beta_3$

On peut montrer que :

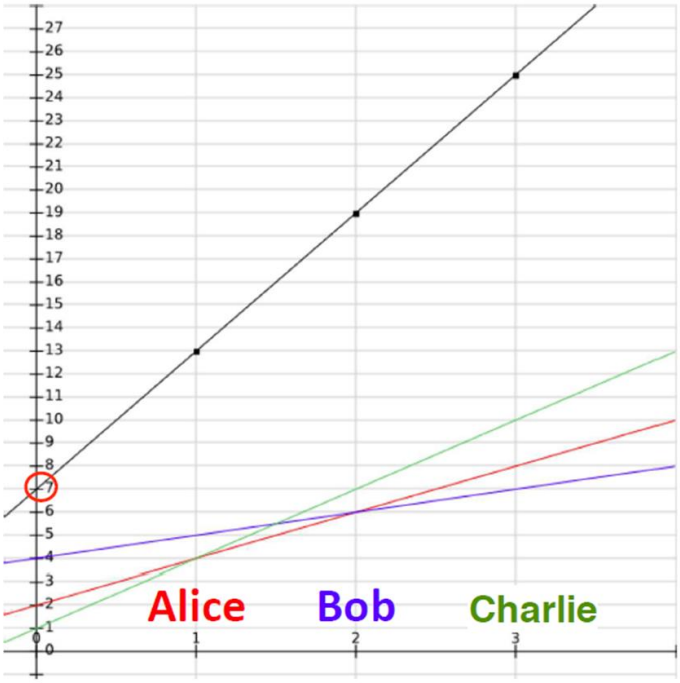
y = (p1(1) + p2(1) + p3(1)) * β1 + (p1(2) + p2(2) + p3(2)) * β2 +(p1(3) + p2(3) + p3(3))
*· β2 = p1(0) + p2(0) + p3(0)

= x1 + x2 + x3

Exemple :

Alice possède un secret a = 2, Bob possède un secret b = 4, Charlie possède un secret c = 1.
La fonction à calculer est f(a,b,c) = a + b + c sans révéler les secrets respectifs.
Alice choisit : $p_1(x) = a + 2*x = 2 + 2*x$
Bob choisit : $p_2(x) = b + x = 4 + x$
Charlie choisit : $p_3(x) = c + x = 1 + 3x$

A l'aide du protocole de partage de Shamir, Alice obtient:
Les valeurs 4, 5, 4 dont la somme =13
De même Bob, il obtient:
Les valeurs 6, 6, 7 dont la somme =19
Ainsi que Charlie, il obtient:
Les valeurs 7, 8, 10 dont la somme =25
Les trois sommes sont des points sur la droite qui permet de retrouver la somme qui est la projection de la droite sur l'axe y comme le montre la figure suivante :



4.2 PARTAGE DE SECRET À SEUIL DE MIGNOTTE
(Mignotte's threshold secret sharing scheme)
Le partage de secret de Mignotte est basé sur le théorème du reste chinois. Ce protocole est réalisé selon trois étapes.

Etape 1:
On Choisi deux entiers n qui est le nombre de parties et t qui est le seuil de partage tel que $t \leq n-1$
Soient $m_1 < m_2 < \ldots < m_n$ des entiers positifs, premiers deux à deux et qui vérifient :
$m_1 * m_2 * \ldots * m_{t+1} > m_{n-t+1} * m_{n-t+2} * \ldots * m_n$

Etape 2:
Soit s que le donneur qui veut partager avec n parties le secret s. Ce dernier doit satisfaire
$m_1 * m_2 * \ldots * m_{t+1} > s > m_{n-t+1} * m_{n-t+2} * \ldots * m_n$
Le donneur calcule $s_i \equiv s \bmod m_i$ et fournit s_i à P_i pour i=1 à n
Rappel : Chaque t+1 parties peut calculer la solution x

Etape 3:(retrouver le secret)
$x \equiv s_{i1} \pmod{m_{i1}}$
$x \equiv s_{i2} \pmod{m_{i2}}$
...
$x \equiv s_{it+1} \pmod{m_{it+1}}$
Par le CRT, ce système a une solution unique modulo $m_{i1} * m_{i2} * \ldots * m_{it+1}$ et par les propriétés des séquences de Mignotte,
Cette solution est le secret, ie x=s
Remarque : Chaque ensemble de t parties (ou inférieur) ne peut pas trouver s.

Exemple :
soit n = 4 et t = 2, $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$
Étape 1:
On doit vérifier que les valeurs forment une séquence de Mignotte
GCD(m_i , m_j) = 1 ? OUI pour tout i, j $\in \{1, 2, 3, 4\}$ et $i \neq j$
$m_1 < m_2 < m_3 < m_4$? en effet $3 < 4 < 5 < 7$
$m_1 * m_2 * m_3 > m_3 * m_4$? En effet $3 * 4 * 5 = 60 > 35 = 7 \cdot 5$
Étape 2: soit s = 40 le secret à partager
Vérifier que la valeur de s vérifie le rang de Mignotte :
$m_1 * m_2 * m_3 > s > m_3 * m_4$? En effet $60 > 40 > 35$
on procède au calcul des valeurs de partage $s_i = s \bmod m_i$
$s_1 = 40 \bmod 3 = 1 \bmod 3$
$s_2 = 40 \bmod 4 = 0 \bmod 4$
$s_3 = 40 \bmod 5 = 0 \bmod 5$
$s_4 = 40 \bmod 7 = 5 \bmod 7$
Étape 3: (retrouver le secret)
$x = s_2 \bmod m_2 = 0 \bmod 4$
$x = s_3 \bmod m3 = 0 \bmod 5$
$x = s_4 \bmod m4 = 5 \bmod 7$
En prenant les deux premières équations on a:
5*1 +4 * -1 = 1
Donc $x = 0 * 5 + 0 * (-4) = 0 \bmod 20$; on aura alors
$x = 0 \bmod 20$
$x = 5 \bmod 7$
de même pour les deux équations ci-dessus
20 * (-1) + 7 * 3 = 1
Donc $x = 5 * (-20) + 0 * 21 = -100 \bmod 140 = 40$
le secret s = x = 40