

Au Fil des Maths

15 FÉVRIER 2021

Partage d'un secret

Comment faire pour que votre secret le plus précieux ne soit pas perdu, sans pour autant le divulguer ? Eh bien, en le partageant entre plusieurs personnes... moyennant quelques précautions mathématiques, que nous racontent Fabien Herbaut et Pascal Véron. Qui a dit que les mathématiques ne servaient à rien ?

Fabien Herbaut & Pascal Véron

© APMEP Décembre 2020



Introduction

L'inventeur inquiet d'une recette inimitable et jalousée (pâte à tartiner aux noisettes, célèbre soda, médicament efficace, ...) souhaite pouvoir la transmettre à ses héritiers... sans que personne n'en profite en attendant ! Il voudrait déposer des recettes incomplètes chez trois notaires, de sorte qu'il faille la coopération de deux des notaires pour reconstituer la recette originale. Aucun des notaires ne doit être en mesure de reconstituer seul la recette originale, ni même d'obtenir le moindre indice sur aucun des ingrédients. Les mathématiques peuvent-elles aider notre inventeur ?

Un second exemple : on souhaite conserver un fichier important en ligne, mais en limitant les risques de perte ou de piratage. Pour cela, on compte le diviser en cinq parties, et enregistrer ces cinq parties sur cinq serveurs différents, mais de sorte qu'avoir accès à trois de ces parties soit nécessaire et suffisant pour reconstituer ce fameux fichier. Ainsi, si un (ou même deux) des serveurs tombent en panne, on peut toujours reconstituer le fichier. De même, si un (ou même deux) des serveurs sont piratés, les informations ne sont pas compromises. Comment faire ?

Dans ce qui suit, nous allons tenter de donner un peu de formalisme à ces problèmes de partage de secret. Ensuite, nous proposerons essentiellement deux méthodes pour partager un secret. La première de ces méthodes est géométrique : elle permet de partager un problème entre trois (ou quatre) personnes, tout en restant dans le cadre des programmes de géométrie plane (ou spatiale) de collège ou de lycée. Précisément, il s'agit d'étudier l'intersection de droites du plan (ou de plans dans l'espace). La deuxième des méthodes que nous présentons est la solution générale proposée par Adi Shamir dans son célèbre article *How to share a secret ?* [1]. Elle utilise l'interpolation de Lagrange et pourrait ainsi illustrer l'item *interpolation polynomiale* qui est une application de la partie *Graphes et matrices* du programme de Mathématiques Expertes de la classe de Terminale. La partie 4 contient des premières propositions d'exercices ou d'activités correspondant à ces niveaux évoqués, qui pourront être adaptées selon les classes. Dans la version numérique de cette note, celle que vous avez sous les yeux, nous proposons plusieurs variantes de ces exercices. Les plus intéressés peuvent y poursuivre leur lecture plus loin : dans une dernière partie nous évoquons comment la théorie des codes permet de reconstituer un secret, même si parmi les personnes détentrices d'une partie du secret certaines mentent ! Il existe également une version papier de cette note, plus synthétique.

Le problème du partage de secret

Dans les exemples donnés, on souhaite pouvoir conserver une donnée secrète d'importance. Si l'on dispose d'un seul exemplaire de cette donnée, confié à une personne de confiance, il y a un risque de perte totale du secret en cas de défaillance de la personne (disparition, malhonnêteté, piratage, ...). Si l'on distribue des copies exactes du secret à plusieurs personnes, en augmentant le nombre de personnes on augmente la probabilité que l'une d'entre elles soit compromise. Ainsi germe l'idée de trouver un moyen pour découper le secret en plusieurs morceaux. Ces morceaux seraient distribués à n personnes (ou n machines, selon le contexte), avec le cahier des charges suivant : on souhaite qu'à partir d'un certain nombre k de personnes collaborant, le secret puisse être reconstruit. Si moins de k personnes se réunissent, elles ne doivent pas pouvoir obtenir le secret. Dans la littérature spécialisée en cryptographie, on parle de schéma de partage de secret à seuil et on appelle k le seuil. En anglais on utilise l'expression (k, n) -threshold scheme.

Évoquons une autre contrainte que le lecteur pourra omettre lors d'une première lecture : aucune portion du secret ne doit permettre de déduire une quelconque information sur le secret. Le lecteur curieux d'un formalisme exprimant cette contrainte pourra consulter [2].

Enfin, dans ce qui suit le secret partagé sera un nombre. Cela n'étonnera sans doute pas le lecteur, car à l'heure actuelle les données (texte, image, musique, vidéo, logiciel, etc.) sont numérisées et stockées sous la forme d'une suite de nombres.

Une solution géométrique

Pour simplifier les choses lors d'un premier contact, nous commençons par présenter dans cette



section des schémas de partage entre n personnes avec seuil $n - 1$.

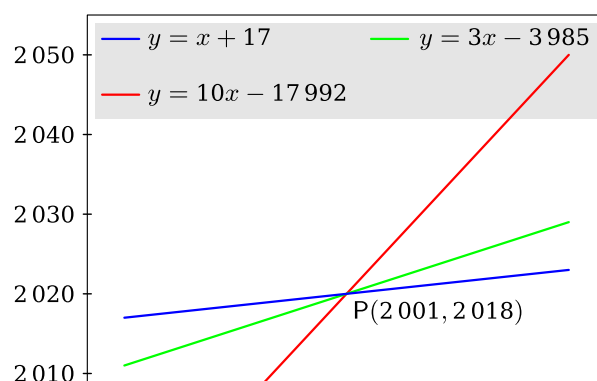
Cas de trois personnes

Le premier cas à aborder est naturellement celui d'un schéma de partage à seuil $(2, 3)$, c'est-à-dire qu'il y a trois protagonistes, et qu'on souhaite partager le secret de sorte que ce dernier ne puisse être reconstitué que si deux personnes au moins mettent en commun leurs informations. Profitons-en pour donner un exemple iconique, parfois utilisé dans la littérature. D'après le journal *Time Magazine* du 4 Mai 1992, le contrôle de l'arme nucléaire russe nécessitait la présence ou l'accord de deux personnes parmi le président, le ministre de la défense et un représentant des armées. Il s'agit bien d'un schéma de partage à seuil $(2, 3)$.

Une solution géométrique (dont la plupart des auteurs créditent Georges Robert Blakley [3]) consiste à considérer le secret comme l'ordonnée d'un point P du plan choisi par la personne chargée de distribuer le secret aux trois intervenants. Ce dernier détermine ensuite trois droites distinctes passant par le point P et attribue chacune d'elles à un intervenant (par exemple chaque intervenant détiendra soit l'équation d'une droite, soit les coordonnées de deux points de la droite). Quand deux intervenants se réunissent, ils peuvent facilement déterminer le point d'intersection P et en déduire la valeur du secret. En revanche, un seul intervenant ne peut identifier sur la droite le point P .

Remarque : pourquoi n'utiliser que l'ordonnée du point P pour représenter le secret et non pas le couple (abscisse, ordonnée) ? Une contrainte générale au niveau de la sécurité, évoquée dans la partie précédente, est qu'aucun participant ne possède plus d'informations sur le secret qu'une personne hors de la clique. Si les coordonnées du point P constituent le secret, un individu extérieur n'aurait aucune information sinon le fait que le secret est un point du plan. En revanche, un des trois membres saurait limiter sa recherche à une droite (même si celle-ci contient une infinité de points).

Exemple : considérons un cas où trois personnes Nicolas, Valérie et Yves doivent se partager pour secret la valeur 2018. La personne chargée de distribuer le secret aux trois intervenants choisit par exemple le point P de coordonnées $(2001, 2018)$. Elle construit alors trois droites concourantes en ce point (cf. fig. 1). Elle communique à Nicolas l'équation $y = x + 17$, à Valérie l'équation $y = 10x - 17992$ et à Yves l'équation $y = 3x - 3985$.



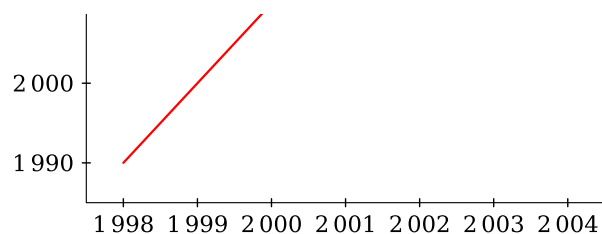


Figure 1. Une configuration possible du système de partage pour $s = 2018$.

Si Nicolas et Valérie se rencontrent, ils peuvent calculer le point d'intersection de leurs droites respectives et en déduire l'ordonnée de ce dernier qui est la valeur du secret (cf. fig. 2).

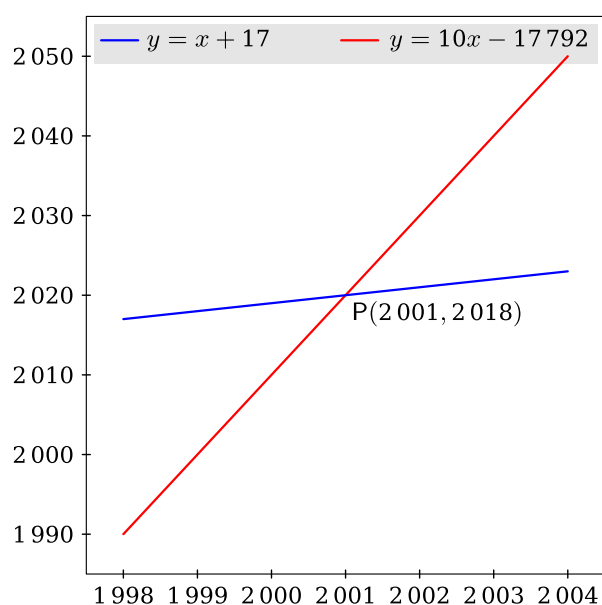


Figure 2. Deux personnes se rencontrent et reconstituent le secret.

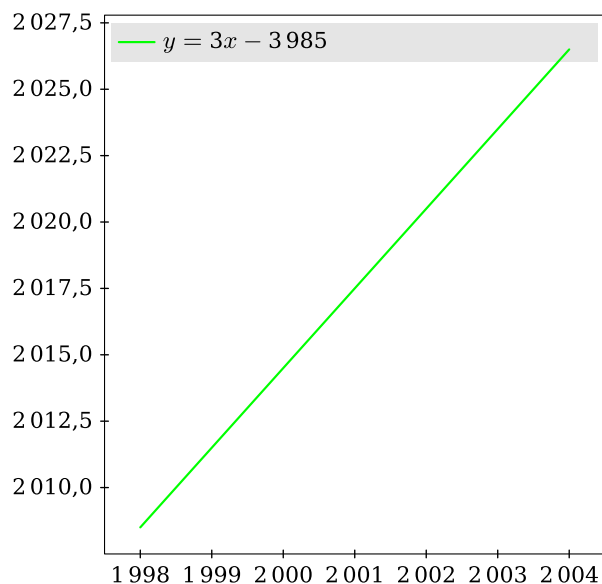


Figure 3. Une personne seule n'a aucune information sur le secret.

À partir de son équation, Yves ne peut déduire aucune information sur la valeur du secret (cf. fig. 3).

Cas de quatre personnes



Étendons la méthode précédente au cas de quatre personnes : cette fois, trois personnes au moins doivent être présentes pour reconstituer le secret s . La personne chargée de le répartir choisit un point $P(x, y, s)$ de l'espace. Elle construit quatre plans concourants en ce point. Elle communique alors à chaque personne une équation de plan. Si trois personnes se réunissent, elles peuvent calculer les coordonnées de P , le point d'intersection de leurs plans, et en déduire s . Si deux personnes se réunissent, elles obtiennent l'équation d'une droite ce qui ne leur permet pas de déterminer la valeur de s .

Généralisation à un schéma de partage $(n - 1, n)$

La méthode se généralise au cas de n personnes avec $n \geq 5$: on considère cette fois n hyperplans affines de \mathbb{R}^{n-1} en position générale, concourants au point P . Chacun de ces hyperplans peut être représenté par une équation linéaire qui sera communiquée à l'un des participants. Si k participants se réunissent, ils obtiennent un espace affine de dimension $n - 1 - k$. Ainsi il faut et il suffit que $n - 1$ personnes se réunissent pour retrouver le point P .

On peut remarquer que ces méthodes fournissent également des schémas de partage $(n - 1, m)$ pour tout entier $m \geq n$: il suffit de choisir m hyperplans affines de \mathbb{R}^{n-1} , passant par P , et toujours en position générale.

Une solution basée sur l'interpolation polynomiale et les matrices

Dans cette partie nous détaillons une méthode basée sur l'interpolation décrite en 1979 par Adi Shamir dans son article fondateur *How to share a secret* [1].

Cas d'un seuil fixé à 2

Considérons à nouveau

le problème étudié dans le cas d'un schéma de partage $(2, 3)$: partager un secret en trois parties, de façon à ce qu'il puisse être reconstitué par deux personnes. Dans ce contexte, la méthode proposée par Shamir peut être expliquée dès le cycle 4 sans avoir à aborder la notion de polynôme. L'idée clé repose sur le fait que lorsque l'on fixe deux points du plan, il existe une unique droite passant par ces points. Si de plus ces points ne sont pas alignés verticalement, cette droite coupe l'axe des ordonnées en un point dont l'ordonnée sera le secret s .

Concrètement, la personne chargée de distribuer un secret s place le point P de coordonnées $(0, s)$ et trace une droite non verticale passant par P . Elle choisit alors 3 points sur cette droite. Chaque intervenant reçoit les coordonnées de l'un de ces trois points. Lorsque deux personnes se rencontrent, elles peuvent tracer la droite passant par les deux points détenus et trouver le point d'intersection avec l'axe des ordonnées.



En choisissant n points (avec $n > 3$), ceci permet de partager le secret entre n personnes tout en assurant un seuil de deux (cf. fig. 4). Un des participants, seul, ne peut retrouver le secret. En effet, il passe, par le seul point qu'il connaît, une infinité de droites.

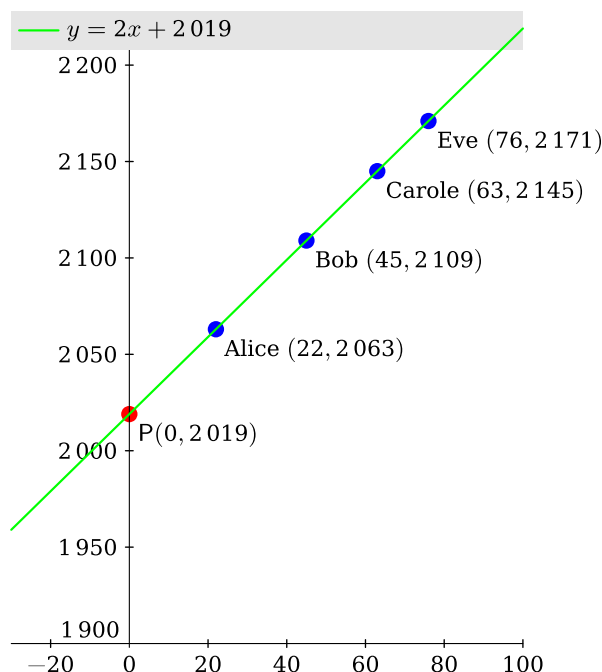


Figure 4. Une configuration possible du système de partage pour $n = 4$ et $s = 2019$.

Cas d'un seuil fixé à 3

Considérons le cas d'un secret à partager entre quatre personnes, de façon à ce qu'il puisse être reconstitué par trois personnes. La méthode repose cette fois sur le résultat suivant : par trois points non alignés du plan, dont deux ne sont jamais sur une même droite verticale, il passe une unique parabole d'axe vertical. Celle-ci coupe l'axe des ordonnées en un point dont l'ordonnée sera le secret s .

En pratique, la personne chargée de distribuer un secret s choisit $Q(x) = s + a_1x + a_2x^2$, un polynôme de degré 2, obtenu en tirant au hasard deux coefficients a_1 et a_2 . Elle choisit ensuite au hasard quatre valeurs x_1, x_2, x_3 et x_4 (deux à deux distinctes), et calcule $y_i = Q(x_i)$ pour $i \in \{1, 2, 3, 4\}$. Chaque personne reçoit un couple (x_i, y_i) . Lorsque trois personnes se réunissent, elles peuvent constituer un système linéaire de trois équations à trois inconnues. Supposons que les personnes détenant les couples (x_1, y_1) , (x_2, y_2) et (x_3, y_3) mettent en commun leurs informations, elle obtiennent alors le système d'équations suivant :

$$\begin{cases} a_2x_1^2 + a_1x_1 + s = y_1 \\ a_2x_2^2 + a_1x_2 + s = y_2 \\ a_2x_3^2 + a_1x_3 + s = y_3 \end{cases}$$

dont la forme matricielle est $Va = y$, si l'on note :



$$V = \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix}, \quad a = \begin{pmatrix} s \\ a_1 \\ a_2 \end{pmatrix}, \quad \text{et } y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

La matrice V est appelée matrice de Vandermonde et il est bien connu qu'elle est inversible, car les x_i sont deux à deux distincts. La solution du système est donc unique, ce qui permet aux trois personnes de calculer s (cf. fig. 5).

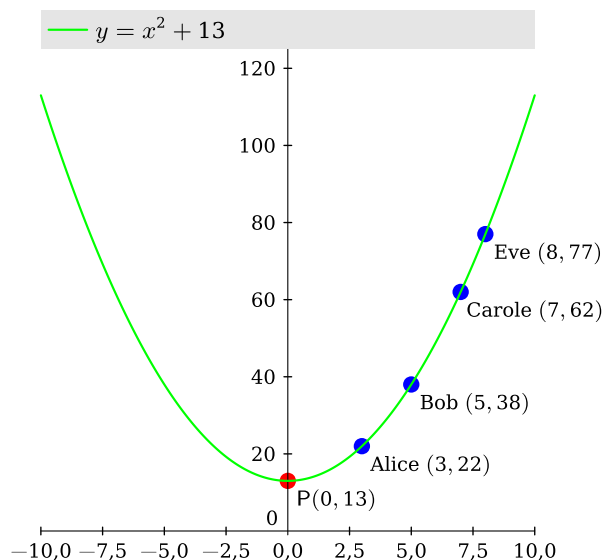


Figure 5. Une configuration possible du système de partage pour $n = 4$ et $s = 13$.

En revanche, deux des participants ne peuvent retrouver seuls le secret car il existe une infinité de paraboles d'axe vertical passant par les points qu'ils détiennent.

Cas d'un seuil fixé à 3 avec au moins 4 personnes

Si l'on augmente le nombre de personnes mais pas le seuil, la méthode précédente s'applique toujours.

Si la personne chargée de distribuer le secret calcule n couples $(x_i, Q(x_i))$ pour $n \geq 4$, trois participants se réunissant pourront toujours reconstruire le secret s . On obtient ainsi un schéma de partage de secret à seuil $(3, n)$ pour tout $n \geq 4$. À nouveau deux des participants ne peuvent seuls retrouver le secret.

Généralisation à un schéma de partage de secret (k, n)

Considérons des entiers k et n tels que $2 \leq k \leq n - 1$. La personne chargée de distribuer le secret choisit $k - 1$ coefficients a_1, a_2, \dots, a_{k-1} et fixe le polynôme $Q(x) = s + a_1x + \dots + a_{k-1}x^{k-1}$. Elle calcule par la suite n couples $(x_i, Q(x_i))$ et les distribue aux n participants. Lorsque k d'entre eux se réunissent, ils obtiennent un système linéaire (de Vandermonde) à k équations et k inconnues leur permettant de calculer la valeur de s .

Remarque : pour des raisons de sécurité et de réalisation pratique sortant du cadre de cette note, tous les calculs détaillés dans cette partie sont généralement effectués modulo un grand nombre premier p , c'est-à-dire que l'ensemble des calculs se font dans le corps $\mathbb{Z}/p\mathbb{Z}$ et non dans le corps \mathbb{R} .

Proposition d'exercices en lien avec les programmes du secondaire

Dans cette partie, nous proposons des activités illustrant les notions présentées qui pourront être utilisées dans les classes.

Cycle 4

Le calcul effectif du point d'intersection de deux droites à partir de leur équation n'est pas au programme du Cycle 4 (d'après le BO de novembre 2015). Il est cependant possible de proposer une activité basée sur la représentation graphique d'une droite ou sur l'utilisation d'un logiciel de géométrie. Afin de faciliter la recherche du point d'intersection, on n'oubliera pas de préciser dans l'énoncé que le secret s est un entier.

Cycle 4 – Exercice 1

Nous présentons dans cette activité une méthode pour partager un secret entre trois personnes. Nous partons du principe que ce secret à partager est un nombre entier (cela peut avoir des applications pratiques : par exemple on souhaite partager un code d'accès). Nous allons vous montrer comment partager ce secret de sorte que ce nombre ne puisse être retrouvé par ces personnes que si au moins deux d'entre elles se réunissent.

Dans notre exemple, ces trois personnes seront appelées Amidala, Bobba et Chewie. Une personne insoupçonnable (que l'on appelle en général *un tiers de confiance*) choisit trois droites concourantes. Elle confie à Amidala l'équation d'une de ces droites, à Bobba l'équation d'une autre droite, et à Chewie l'équation de la dernière droite. Le secret partagé est l'ordonnée du point d'intersection de ces droites.

Le tiers de confiance confie à Amidala l'équation de sa droite que nous appellerons \mathcal{A} : $y = 2x - 4$, à Bobba l'équation de sa droite \mathcal{B} : $y = x - 1$ et enfin à Chewie l'équation de sa droite \mathcal{C} : $y = -3x + 11$.

1. À votre avis, Amidala peut-elle retrouver seule l'ordonnée du point d'intersection des droites, avec sa seule connaissance de la droite \mathcal{A} ?
2. Amidala et Chewie se rencontrent : ils mettent en commun leurs informations. Tracer les droites dont ils ont connaissance et déterminer la valeur entière de l'ordonnée du point d'intersection de ces droites, c'est à dire la valeur du secret s .
3. Chewie rencontre cette fois Bobba : montrer qu'il peuvent retrouver le même secret. Comment cela s'explique-t-il ?

Conclusion

Finalement, nous avons vu qu'aucune des trois personnes ne peut retrouver le secret avec la connaissance d'une seule droite ! Mais si deux d'entre elles se réunissent, elles peuvent mettre leurs informations en commun, trouver le point d'intersection de leurs droites, et retrouver le secret.

Cycle 4 – Exercice 2 (méthode de Shamir avec utilisation d'un logiciel de géométrie)

Pour partager un secret s entre Amidala, Bobba et Chewie, un tiers de confiance décide d'utiliser la méthode de Shamir. Pour cela, il trace une droite (non verticale) passant par le point de coordonnées $(0, s)$, puis choisit au hasard 3 points sur cette droite. Il confie à chaque personne les coordonnées de l'un des trois points. Chewie s'est vue attribuer le point $(-10, -3)$, Amidala le point $(4, 4)$ et Bobba le point $(12, 8)$.

Amidala et Chewie se rencontrent. Tracer à l'aide d'un logiciel de géométrie la droite passant par leur deux points et déterminer la valeur entière de l'ordonnée du point d'intersection avec l'axe des ordonnées, c'est-à-dire la valeur du secret s .

Suite à une fuite, la valeur du secret s doit être changée. Vous êtes l'au-



torité chargée d'effectuer cette modification. Choisir un nouveau nombre secret s et placer le point P de coordonnées $(0,s)$. Tracer une droite passant par ce point, puis choisir 3 points à distribuer à Amidala, Bobba et Chewie.

En Seconde.

Concernant le programme de Seconde au BO de janvier 2019, la *détermination des coordonnées du point d'intersection de deux droites sécantes* est une des capacités attendues.

On propose alors d'adapter le premier exercice de Cycle 4 proposé plus haut de sorte que la résolution soit effectuée de façon algébrique et non plus géométrique.

Seconde – Exercice 3

Nous présentons dans cette activité une méthode pour partager un secret entre trois personnes. Nous partirons du principe que ce secret à partager est un nombre (cela peut avoir des applications pratiques : par exemple on souhaite partager un code d'accès). Nous allons vous montrer comment partager ce secret de sorte que ce nombre ne puisse être retrouvé par ces personnes que si au moins deux d'entre elles se réunissent.

Dans notre exemple, ces trois personnes seront appelées Amidala, Bobba et Chewie. Une personne insoupçonnable (que l'on appelle en général *un tiers de confiance*) choisit trois droites concourantes. Elle confie à Amidala l'équation d'une de ces droites, à Bobba l'équation d'une autre droite, et à Chewie l'équation de la dernière droite. Le secret partagé est l'ordonnée du point d'intersection de ces droites.

1. Un exemple pour comprendre

Le tiers de confiance confie à Amidala l'équation de sa droite que nous appellerons \mathcal{A} : $y = x + 17$, à Bobba l'équation de sa droite \mathcal{B} : $y = 10x - 17992$ et enfin à Chewie l'équation de sa droite \mathcal{C} : $y = 3x - 3985$.



1. Pourquoi Amidala ne peut-elle pas retrouver seule l'ordonnée du point d'intersection des trois droites ?
2. Amidala et Chewie se rencontrent : ils mettent en commun leurs informations. Expliquer comment ils peuvent retrouver le secret partagé, c'est-à-dire l'ordonnée du point d'intersection de leurs droites. Quelle est la valeur du secret s ?
3. Chewie rencontre cette fois Bobba : montrer qu'il peuvent retrouver le même secret. Comment cela s'explique-t-il ?

Conclusion

Aucune des trois personnes ne peut retrouver le secret avec la connaissance d'une seule des droites ! Mais si deux d'entre elles se réunissent, elles peuvent mettre leurs informations en commun, trouver le point d'intersection de leurs droites, et retrouver le secret.

2. Dans la peau du tiers de confiance

Vous allez jouer le rôle du tiers de confiance et partager un secret entre trois personnes. Choisir un nombre (le secret), puis un point qui ait pour ordonnée ce nombre. Trouver trois équations de droite passant par ce point. Vous pouvez vérifier que le secret est bien partagé en confiant ces trois équations à trois élèves : aucun d'entre eux ne doit pouvoir retrouver le secret seul, mais dès que deux d'entre eux décident de mettre en commun leurs informations, ils doivent pouvoir le retrouver.

3. Python à la rescousse

Écrire un programme en Python qui demande de saisir un entier (ce sera le secret à partager), puis qui renvoie trois équations de droite partageant ce secret. Pour construire ces équations de droite en introduisant de l'aléa, on pourra utiliser la commande `randint(a,b)` qui renvoie un entier tiré aléatoirement entre a et b . On rappelle que la commande `randint` se trouve dans la bibliothèque `random` à laquelle on peut avoir ac-

cès après avoir par exemple utilisé la commande `import random`.

En Terminale (enseignement de spécialité).

Considérons dans cette partie le programme d'enseignement de spécialité de la classe de Terminale au BO de juillet 2019. Les notions de géométrie dans l'espace liées aux capacités attendues du paragraphe *Représentations paramétriques et équations cartésiennes* permettent d'aborder le partage de secret dans un groupe constitué d'au moins quatre personnes avec un seuil de trois personnes. Proposons deux déclinaisons d'une activité sur ce thème mettant en jeu ces éléments des programmes.

Dans la première version proposée ci-dessous, le problème est ouvert concernant le choix de la méthode à utiliser. Il est suggéré d'utiliser des notions de géométrie spatiale pour résoudre le problème. Dans la deuxième version, la méthode est détaillée et le travail guidé. Il s'agit cette fois d'un exercice motivé de calcul d'intersections de plans dans l'espace.

Terminale – Activité 1 – Spécialité Mathématiques.

Nous présentons dans cette activité une méthode pour partager un secret entre plusieurs personnes. Nous partons du principe que ce secret à partager est un nombre (cela peut avoir des applications pratiques : par exemple on souhaite partager un code d'accès). Nous allons vous montrer comment partager ce secret de sorte que ce nombre ne puisse être retrouvé par ces personnes que si au moins un certain nombre d'entre elles se réunissent.

Considérons un premier exemple avec trois personnes appelées Amidala, Bobba et Chewie. Une personne insoupçonnable (que l'on appelle en général *un tiers de confiance*) choisit trois droites concourantes. Elle confie à Amidala l'équation d'une de ces droites, à Bobba l'équation d'une autre droite, et à Chewie l'équation de la dernière droite. Le secret partagé est l'ordonnée du point d'intersection de ces droites. Aucune des trois personnes ne peut retrouver l'ordonnée secrète avec la connaissance d'une seule des droites ! Mais si deux d'entre elles se réunissent, elles peuvent mettre leurs informations en commun, trouver le point d'intersection de leurs droites, et retrouver le secret.



Essayons d'abord de comprendre sur un exemple avant de généraliser à un plus grand nombre de personnes.

1. Un exemple pour comprendre

Le tiers de confiance confie à Amidala l'équation de sa droite que nous appellerons \mathcal{A} : $y = x + 17$, à Bobba l'équation de sa droite \mathcal{B} : $y = 10x - 17992$ et enfin à Chewie l'équation de sa droite \mathcal{C} : $y = 3x - 3985$.

1. À votre avis, Amidala peut-elle retrouver seule l'ordonnée du point d'intersection des droites, avec sa seule connaissance de l'équation de la droite \mathcal{A} ?
2. Amidala et Chewie se rencontrent : ils mettent en commun leurs informations. Expliquer comment ils peuvent retrouver le secret partagé, c'est-à-dire l'ordonnée du point d'intersection de leurs droites ?
3. Chewie rencontre cette fois Bobba : montrer qu'il peuvent retrouver le même secret. Comment cela s'explique-t-il ?

2. Dans la peau du tiers de confiance

Vous allez jouer le rôle du tiers de confiance et partager un secret entre trois personnes. Choisir un nombre (le secret), puis un point qui ait pour ordonnée ce nombre. Trouver trois équations de droite passant par ce point. Vous pouvez vérifier que le secret est bien partagé en confiant ces trois équations à trois élèves : aucun d'entre eux ne doit pouvoir retrouver le secret seul, mais dès que deux d'entre eux décident de mettre en commun leurs informations, ils doivent pouvoir le retrouver.

3. Généralisation

On considère cette fois le cas de quatre personnes : Amidala, Bobba, Chewie et Dark. On voudrait cette fois partager le secret de sorte

- qu'aucune des quatre personnes ne puisse le retrouver seule



- que si deux personnes se retrouvent elles ne puissent pas le retrouver non plus
- mais que dès que trois personnes parmi les quatre se retrouvent, elles puissent retrouver le secret.

Proposer une méthode en vous inspirant de ce qui précède. On pourra penser au cours de géométrie dans l'espace.

Terminale – Activité 2 – Spécialité Mathématiques.

Nous présentons dans cette activité une méthode pour partager un secret entre plusieurs personnes. Nous partirons du principe que ce secret à partager est un nombre (cela peut avoir des applications pratiques : par exemple on souhaite partager un code d'accès). Nous allons vous montrer comment partager ce secret de sorte que ce nombre ne puisse être retrouvé par ces personnes que si au moins un certain nombre d'entre elles se réunissent.

Considérons un premier exemple avec trois personnes appelées Amidala, Bobba et Chewie. Une personne insoupçonnable (que l'on appelle en général *un tiers de confiance*) choisit trois droites concourantes. Elle confie à Amidala l'équation d'une de ces droites, à Bobba l'équation d'une autre droite, et à Chewie l'équation de la dernière droite. Le secret partagé est l'ordonnée du point d'intersection de ces droites. Essayons d'abord de comprendre sur un exemple avant de généraliser à un plus grand nombre de personnes.

1. Un exemple pour comprendre

Le tiers de confiance confie à Amidala l'équation de sa droite que nous appellerons \mathcal{A} : $y = x + 17$, à Bobba l'équation de sa droite \mathcal{B} : $y = 10x - 17992$ et enfin à Chewie l'équation de sa droite \mathcal{C} : $y = 3x - 3985$.

1. À votre avis, Amidala peut-elle retrouver seule l'ordonnée du point



d'intersection des droites, avec sa seule connaissance de la droite \mathcal{A} ?

2. Amidala et Chewie se rencontrent : ils mettent en commun leurs informations. Expliquer comment ils peuvent retrouver le secret partagé, c'est-à-dire l'ordonnée du point d'intersection de leurs droites ?
3. Chewie rencontre cette fois Bobba : montrer qu'il peuvent retrouver le même secret. Comment cela s'explique-t-il ?

2. Dans la peau du tiers de confiance

Vous allez jouer le rôle du tiers de confiance et partager un secret entre trois personnes. Choisir un nombre (le secret), puis un point qui ait pour ordonnée ce nombre. Trouver trois équations de droite passant par ce point. Vous pouvez vérifier que le secret est bien partagé en confiant ces trois équations à trois élèves : aucun d'entre eux ne doit pouvoir retrouver le secret seul, mais dès que deux d'entre eux décident de mettre en commun leurs informations, ils doivent pouvoir le retrouver.

3. Généralisation

On considère cette fois le cas de quatre personnes : Amidala, Bobba, Chewie et Dark. On voudrait cette fois partager le secret de sorte

- qu'aucune des quatre personnes ne puisse le retrouver seule
- que si deux personnes se retrouvent, elles ne puissent pas le retrouver non plus
- mais que dès que trois personnes parmi les quatre se retrouvent, elles puissent retrouver le secret.

Nous allons proposer une méthode utilisant le cours de géométrie dans l'espace. Le secret sera à nouveau la (dernière) coordonnée z d'un point d'intersection... non plus celui de deux droites, mais celui de trois plans ayant un unique point d'intersection. A chaque personne sera

confiée une équation de plan : pour retrouver le point d'intersection, deux équations ne suffiront pas.

1. On considère un exemple pour comprendre. Le tiers de confiance confie à Amidala l'équation du plan $\mathcal{A} : 5x + 4y - 2z = 5097$, à Bobba l'équation du plan $\mathcal{B} : 3x - 7y + 2z = 10250$, à Chewie l'équation du plan $\mathcal{C} : 5x + 5y - 4z = 2284$, et enfin à Dark l'équation du plan $\mathcal{D} : -6x + 11y + 9z = -3423$. On suppose que Amidala et Bobba se rencontrent. Montrer que l'intersection de \mathcal{A} et de \mathcal{B} est une droite.
2. Montrer que si Chewie se joint à eux, ils peuvent retrouver les coordonnées du point d'intersection et donc le secret partagé.
3. Vérifier que pour d'autres rencontres de trois personnes parmi les quatre le secret peut être retrouvé. (À ce propos, combien y a-t-il de façons de choisir ces trois personnes parmi les quatre ?)
4. Vous êtes à nouveau dans la peau du tiers de confiance : à vous de choisir un secret (nombre) à partager entre quatre personnes et de déterminer les équations de plans concourants.

En Terminale (Mathématiques expertes)

Une dernière activité est proposée pour montrer comment les connaissances du programme de Mathématiques expertes en lien avec les matrices permettent d'illustrer la méthode d'Adi Shamir (cf. partie intitulée « Une solution basée sur l'interpolation polynomiale et les matrices »). En effet, l'interpolation polynomiale est l'un des problèmes possibles de la partie *Graphes et matrices* du programme de Mathématiques expertes.

La première partie de l'activité consiste en l'étude d'un schéma de partage de secret $(3, 4)$ reposant sur la manipulation de matrices carrées de dimension 3. Dans la deuxième partie, on étend la construction à un schéma de partage de secret $(4, 5)$. L'activité se termine par des questions ouvertes de difficulté croissante permettant de généraliser ce qui précède afin de construire un schéma de partage de secret (k, n) pour $k < n$.



Nous présentons dans cette activité une méthode pour partager un secret entre plusieurs personnes. Nous partirons du principe que ce secret à partager est un nombre (cela peut avoir des applications pratiques : par exemple on souhaite partager un code d'accès). Nous allons vous montrer comment partager ce secret de sorte que ce nombre ne puisse être retrouvé par ces personnes que si au moins un certain nombre d'entre elles se réunissent.

Considérons un premier exemple avec quatre personnes appelées Amidala, Bobba, Chewie et Dark. Une personne insoupçonnable (que l'on appelle en général *un tiers de confiance*) choisit un secret s , qui est un nombre, et deux autres nombres t et u . Ce tiers de confiance considère le polynôme du second degré $Q(x) = s + tx + ux^2$. Il choisit ensuite quatre nombres x_A, x_B, x_C et x_D . Il calcule $y_A = Q(x_A)$, $y_B = Q(x_B)$, $y_C = Q(x_C)$ et $y_D = Q(x_D)$. À Amidala, le tiers de confiance confie x_A et y_A . À Bobba, le tiers de confiance confie x_B et y_B et ainsi de suite pour Chewie et Dark. Si trois des personnes se rencontrent, elles peuvent obtenir un système d'équations permettant de calculer u, t et $s...$ et en particulier retrouver le secret s .

Essayons d'abord de comprendre sur un exemple avant de généraliser à un plus grand nombre de personnes.

1. Un exemple pour comprendre

Le tiers de confiance choisit des nombres s, t et u , puis considère le polynôme du second degré $Q(x) = s + tx + ux^2$. Il confie à Amidala les coordonnées $x_A = 5$ et $y_A = Q(x_A) = 148$, à Bobba les coordonnées $x_B = -12$ et $y_B = Q(x_B) = 1508$, à Chewie les coordonnées $x_C = 11$ et $y_C = Q(x_C) = 634$, et enfin à Dark les coordonnées $x_D = -9$ et $y_D = Q(x_D) = 974$.

1. Amidala, Bobba et Chewie se rencontrent : traduire les égalités $y_A = Q(x_A)$, $y_B = Q(x_B)$ et $y_C = Q(x_C)$ en un système de trois équations en les trois inconnues s, t et u .

2. Donner une interprétation matricielle de ce système.



3. Utiliser un logiciel pour inverser la matrice et en déduire le secret s .
4. Si seuls Amidala et Bobba se rencontrent, quel système d'équations obtiennent-ils ? Combien y a-t-il d'équations et combien d'inconnues ?
5. Vérifier que pour un autre choix de trois personnages parmi les quatre se rencontrant, il est possible de retrouver le secret.
6. Pouvez-vous donner une interprétation géométrique de cette méthode, en introduisant la courbe représentative de la fonction associée à P ?

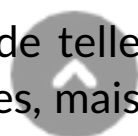
2. Généralisation

On considère cette fois cinq personnages : Amidala, Bobba, Chewie, Dark et Empereur. Le tiers de confiance choisit cette fois un polynôme de degré trois $Q(x) = s + tx + ux^2 + vx^3$, des nombres x_A, x_B, x_C, x_D et x_E puis distribue cette fois les coordonnées $x_A = -4$ et $y_A = Q(x_A) = -517$ à Amidala, $x_B = 3$ et $y_B = Q(x_B) = 127$ à Bobba, $x_C = 2$ et $y_C = Q(x_C) = 35$ à Chewie, $x_D = -5$ et $y_D = Q(x_D) = -1001$ à Dark et enfin $x_E = 8$ et $y_E = Q(x_E) = 3107$ à Empereur.

1. Choisir quatre personnages se rencontrant parmi les cinq et former un système de quatre équations en les quatre inconnues s, t, u et v .
2. Le résoudre en utilisant à nouveau les matrices.
3. En déduire le secret.

Un peu de recul... Comment partager un secret entre cinq personnes de telle sorte que sa reconstitution puisse se faire par trois d'entre elles, mais pas par deux ?

Plus dur ! Comment partager un secret entre six personnes de telle sorte que sa reconstitution puisse se faire par cinq d'entre elles, mais



pas par quatre ?

Encore plus dur ! Avec des entiers k et n tels que $2 \leq k < n$, comment partager un secret entre n personnes de telle sorte que sa reconstitution puisse se faire par k d'entre elles, mais pas par $k - 1$?

Remarques : cette méthode désormais célèbre a été introduite par Adi Shamir en 1979. Non moins célèbre est l'algorithme RSA dont Adi Shamir est l'un des concepteurs : le S du milieu, c'est lui ! L'algorithme RSA est un des algorithmes les plus employés en cryptographie à clé publique, et que vous utilisez sans doute quotidiennement de façon transparente.

Les cas présentés sont des cas d'école pour découvrir la méthode : en pratique on préférera travailler modulo une congruence par un nombre premier !

Pour aller plus loin : contrecarrer les menteurs

Dans cette partie, nous supposons que parmi les personnes se réunissant, certaines communiquent une information erronée (soit de façon intentionnelle pour perturber la reconstruction du secret, soit parce que la portion du secret qu'elles détiennent a été altérée). Nous allons voir comment la théorie des codes permet d'apporter une solution à ce problème.

À propos de la théorie des codes.

Connaissez-vous la théorie des codes ? Cette discipline initiée par les travaux de Claude Shannon dans son article de 1948 *A Mathematical Theory of Communication* a pour objet la communication d'une information via un canal éventuellement perturbé. On souhaite détecter si le message reçu est entaché ou non d'une ou plusieurs erreurs et pouvoir, le cas échéant, corriger.

De façon informelle et en oubliant les structures algébriques sous-jacentes, un code de longueur n est un ensemble de n -uplets où chaque composante est un élément d'un certain ensemble Σ . Par exemple, pour $\Sigma = \{0, 1, 2, 3, 4\}$, l'ensemble $C = \{(0, 1, 1), (1, 2, 4), (4, 3, 1), (3, 3, 3)\}$ est un code de longueur 3. Traditionnellement les éléments de C sont appelés les *mots du code*. Pour deux n -uplets quelconques x et y , on définit la distance d entre x et y par le nombre de composantes en lesquelles ils diffèrent. Par exemple, la distance entre $(1, 0, 2, 3)$ et $(1, 1, 2, 4)$ est 2. On dit qu'un code C est t -correcteur si pour tout n -uplet y , il existe au plus un mot c de C tel que la distance entre y et c soit inférieure ou égale à t . Illustrons ce qui précède en choisissant

$\Sigma = \{0, 1\}$ et $C = \{(0, 0, 0), (1, 1, 1)\}$. Le code ainsi défini est un code 1-correcteur. En effet, pour tout triplet de $\{0, 1\}^3$, il existe exactement un mot de C à distance au plus 1 de ce triplet. L'un des objectifs de la théorie des codes est de construire pour une longueur n donnée et une capacité de correction t fixée, le plus grand code C qui soit t -correcteur. Pour des applications pratiques, on cherchera de plus des classes de code pour lesquelles on dispose d'un algorithme efficace de correction des erreurs.

Pour convaincre le lecteur de l'utilité de ces codes, faisons remarquer que les lecteurs de DVD et de Blu-ray intègrent un mécanisme permettant de lire un support légèrement défectueux, lequel s'appuie sur un code (de la classe des Reed-Solomon) de longueur 255 qui est 2-correcteur et qui est défini sur le corps fini à 256 éléments. Le lecteur curieux pourra aussi consulter l'appel à standardisation du NIST (National Institute of Standards and Technology) de 2017 pour définir les protocoles cryptographiques devant résister à un potentiel ordinateur quantique [4]. Parmi les candidats en lice, certains algorithmes utilisent des codes correcteurs d'erreurs.

Une propriété intéressante des codes de Reed-Solomon est qu'ils disposent d'un algorithme efficace permettant de corriger les erreurs et les effacements. Un effacement est une erreur dont on connaît la position. Le nombre de mots d'un code de Reed-Solomon de longueur n est toujours un entier de la forme q^k où q est la taille de Σ . On dit que k est la dimension du code. L'algorithme de décodage permet de corriger n_e erreurs et n_ε effacements si

$$2n_e + n_\varepsilon \leq n - k.$$

Construction d'un schéma à seuil (k, n) à partir d'un code de Reed-Solomon

On considère un code de Reed-Solomon de longueur n et de dimension k pour un certain ensemble Σ . Le secret à partager entre les n participants est un mot du code. Le participant numéro i reçoit la $i^{\text{ème}}$ composante de ce mot. Lorsque k participants se réunissent, ils peuvent reconstituer un mot dans lequel il manque $n - k$ composantes à des positions connues, c'est-à-dire des effacements. On est ici dans le cas où $n_e = 0$ (il n'y a pas d'erreurs), on peut donc reconstituer entièrement le mot de code à l'aide de l'algorithme de décodage.


Contrecarrer les menteurs

Supposons que parmi les n participants, on soupçonne l'existence d'un menteur (mais pas plus), c'est à dire d'une personne qui divulguera une fausse composante. Si ce dernier fait partie des k personnes se réunissant, le mot reconstitué par ces derniers est donc composé de $n - k$ effacements et d'une erreur (une valeur parmi les k révélées est fausse). Dans ce contexte, l'algorithme de décodage va échouer car $n_e = 1$ et $n_\varepsilon = n - k$. Ainsi l'inégalité ([decodage]) n'est pas vérifiée puisque $2 + n - k > n - k$. En revanche, si l'on convoque $k + 2$ participants, le nombre d'effacements diminue, il vaut $n - k - 2$ et l'inégalité ([decodage]) est à nouveau vérifiée. On est donc en mesure de reconstituer entièrement le secret. Nous laissons au lecteur le soin de vérifier que si

au plus j menteurs sont susceptibles d'être présents lors du processus de distribution du secret, il suffira de convoquer $k + 2j$ personnes afin de pouvoir toujours reconstituer ce dernier.

Remerciements : un grand merci à Luc Ponsonnet pour sa relecture et ses conseils, ainsi qu'aux relecteurs de la revue *Au fil des maths*.

Références

- [1] A. Shamir. *How to share a secret*. T. 22. No 11. Commun. ACM, 1979, pp. 612-613. ↩
- [2] A. Beimel et M. Franklin. *Weakly-Private Secret Sharing Schemes, Theory of Cryptography TCC 2007*. T. 4392. Lecture Notes in Computer Science, pp. 253-272. ↩
- [3] G.R. Blakley. *Safeguarding cryptographic keys, Proceedings of the 1979 AFIPS National Computer Conference*. 1979, pp. 313-317. ↩
- [4] Appel à standardisation du NIST pour les protocoles de Cryptographie Post-Quantique.  ↩



Fabien Herbaut et Pascal Véron sont enseignants-chercheurs, respectivement à l'INSPÉ Nice-Toulon de l'Université Côte d'Azur et à l'Université de Toulon. Leur collaboration au sein du laboratoire IMATH se situe en cryptographie, à la frontière entre l'informatique et les mathématiques.

herbaut@univ-cotedazur.fr

veron@univ-tln.fr

Pour citer cet article : HERBAUT F. ET VÉRON P., « Partage d'un secret », in *Au Fil des Maths* (APMEP), 15 février 2021, <https://afdm.apmep.fr/rubriques/ouvertures/partage-dun-secret/>.

