الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Projet de Fin d'Études

présenté par

AOUFLA Lilia

&

BERKANI Nabila

pour l'obtention du diplôme de Master en Électronique option communication

(Réseaux & Télécoms)

Thème

Cryptographie par Courbes Elliptiques d'un Cloud Computing

Proposé par : Dr. ANOU Abderrahmane

Année Universitaire 2012-2013

Remerciements

C'est avec un grand plaisir qu'on réserve cette page en signe de gratitude et de profonde reconnaissance à tous ceux qui ont bien voulu apporter l'assistance nécessaire au bon déroulement de ce travail.

On veut d'abord remercier notre encadreur M. Anou Abderrahmane, Docteur à l'université Saad Dahlab de Blida, pour la confiance qu'il nous a accordé en acceptant de diriger nos travaux de master.

Nos vifs remerciements s'adressent également à Mme. Azine Houria, pour la qualité de son encouragement, ses remarques pertinentes et le soutient continus et ses compétences qu'elle nous a apporté. On apprécie ses grandes qualités morales et son extrême modestie.

On tient à remercier les membres du jury qui nous ont fait le grand honneur d'évaluer ce travail.

Sans oublier les membres de l'unité de recherche du laboratoire de détection d'information et communication : M. Bensebti Massoud, M. Hebib Sami et M. Djandi Mohamed.

On remercie particulièrement nos parents, nos sœurs et nos frères pour leur patience et leur soutient tout au long de notre cycle d'étude.

Les plus profond remerciements vont à tous nos amies : H.Saida, N.Wissam, Z.Chahra, L.Merième, H.Fethia, C.Samia, S.Akila, H.Ghania, K.Amina, N.Merieme, F.Yasmine, H. Assia et notre délégué K.Bari, pour leurs encouragements et l'atmosphère agréable de travail.

Je dédie ce travail

A mon grand père,

A ma grande mère,

A mon père,

A ma mère,

A ma sœur Imene,

A mon frère Aberrahmane,

A mes amies Razika, Sanaa,

A mon binôme Nabila.

Lilia

Je dédie ce travail

A mon père,

A ma mère,

A mes sœurs Chahiness, Sabrina, Hasnae,

A mes frères Sidahmed, Walid,

A mes beaux frères Sidahmed, Hakim, Ramzi,

A mes neveux Wassim, Housam,

A mes nièces Malak, Douaa,

A Dr. Allal Azeddine,

A mon binôme Lilia.

Nabila

ملخص

"الشبكة المعلوماتية على السحاب" تمثل مفهوم جديد يستند على مبدأ الافتراضية والتخزين على الانترنت التي تتطلب حماية ناجحة وفعالة، و لهذا نتطرق لمعيار التشفير الذي يعتمد على المنحنيات البيضاوية الذي يتميز ببساطة وسرعة الحساب، و تخفيض التكلفة مع فعالية جيدة جدا ضد الهجمات المتعددة.

الكلمات الجوهرية:

التشفير، السحاب، الجداء الخطي، المنحنيات البيضاوية، الجمل.

Résumé :

Le cloud computing « l'informatique sur les nuages » est un nouveau concept est basé sur la notion de virtualisation et de stockage en ligne, qui nécessite une sécurité performante et efficace, d'où apparait le critère de cryptographie basée sur les courbes elliptique qui minimise le coût et offre une simplicité et une rapidité de calcul de plus, une très bonne efficacité face à de nombreuses attaques.

Mots clés :

Cryptographie, Cloud, multiplication scalaire, Courbe elliptique, El-Gamal.

Abstract :

« The cloud computing » is a new concept based on virtualization and online storage, that requires an efficient and effective security to the criterion of cryptography based on elliptic curves, appears that minimizes cost and offers simplicity and speed of calculation again, very good efficacy against many attacks.

Keywords :

Cryptography, Cloud, Scalar multiplication, Elliptic curve, El-Gamal.

Listes des acronymes et abréviations

3DES	Triple Data Enryption Standard
AES	Advenced Encryption Standard
Cloud	Nuage
DES	Data Enceyption Standard
DLP	Discret Logarithm Problem
ECC	Elliptic Curve Cryptography
ECDH	Echange Clé Diffie Hellman
GTR	Garantie de Temps de Retablissement
IP	Intenet Protocol
Matlab	Matrix Laboratory
NAF	Non Adjacent Form
NIST	National Institute of standards and technologye
PC	Personal Computer
PDH	Probleme Deffie Hellman
QOS	Quality Of Service
RSA	Rivest Samir Adeleman
TIC	Technology Information Communication

Table des matières

Liste des figures

Liste des tableaux

Liste des algorithmes

Introduction générale

La technologie de l'internet se développe de manière exponentielle depuis sa création. Actuellement, une nouvelle "tendance" à fait son apparition dans le monde des TIC (Technologies de l'Information et de la Communication), il s'agit du cloud computing. Cette technologie offre des opportunités aux sociétés pour réduire les coûts d'exploitation des logiciels par leurs utilisations directement en ligne. Cette technologie vient juste de surgir. Le cloud computing est un ensemble de services visant à disposer d'applications, de puissance de calcul, et de moyens de stockage. Ceux-ci seront mutualisés, dématérialisés, contractualisés (en termes de performances, niveau de sécurité, coûts…), évolutifs (en volume, fonction, caractéristiques…) et en libre-service. Malgré ces avantages attractifs, de nombreuses entreprises hésitent encore à adopter le cloud computing. Le plus souvent, les raisons de cette hésitation tournent autour de la sécurité.

La sécurité d'un cloud repose sur plusieurs critères, dans notre cas on s'intéresse à la sécurité par cryptage, en particulier la cryptographie basée sur les courbes elliptiques. Ces cryptosystèmes permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels cryptosystèmes nécessitent des clés de taille beaucoup plus modeste (par exemple, une clé de 160 bits lorsque RSA utilise une clé de 1024 bits, à un niveau de sécurité équivalent) ce qui représente un avantage pour les systèmes utilisant un espace mémoire très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de générations et d'échanges de clé beaucoup plus important, et présente une complexité résistante face aux attaques.
Afin de couvrir les notions mentionnées précédemment, notre mémoire est organisé comme suit :

Le Chapitre 1, introduit les concepts liés aux clouds computing ainsi que la notion de virtualisation et le stockage. On discute les risques et les solutions.

Le Chapitre 2, décrit en premier lieu les principes de base des différents cryptosystèmes. En second lieu, les deux grandes familles du cryptage, soit la cryptographie symétrique, et la cryptographie asymétrique.

Le Chapitre 3, présente de façon mathématique la cryptographie à base des courbes elliptiques, les algorithmes de chiffrement ainsi que les différentes coordonnées affines et projectives, principe du protocole d'échange de clé de « Diffie Hellman » et le problème du logarithme discret.

Le Chapitre 4, regroupe l'implémentation et l'interprétation des algorithmes et les protocoles cryptographiques présentés dans le chapitre précédent**.**

Une conclusion générale résume les résultats théoriques et pratiques obtenus.

Chapitre 1 Généralités sur les clouds computing

1.1 Introduction

La généralisation d'internet, le développement des réseaux hauts débit ainsi que la location d'application, résultent une apparition d'un nouveau concept : Le cloud computing qui est devenu, le sujet le plus débattu aujourd'hui dans le secteur des technologies de l'information et la communication (TIC). Il jouera un rôle de plus en plus important dans les opérations informatiques des entreprises. Le cloud computing, ou « informatique dans les nuages », est un modèle informatique consistant à proposer des services informatiques à la demande et accessibles de n'importe où, n'importe quand et par n'importe qui. Cette approche n'est pas tout à fait nouvelle, la réelle nouveauté réside dans son approche systématique. Il est important de comprendre ce qu'il va pouvoir apporter à l'informatique d'aujourd'hui et de demain ce qui le qualifier d'être un ensemble de services et de données consommables.

1.2 Présentation d'un cloud computing

Les services dans le cloud sont des technologies puissantes, adoptées par un grand nombre d'entreprises et de particuliers. Il s'articule sur le stockage et la gestion des informations utilisées par les fournisseurs de services. La raison pour laquelle ce service est appelé "Cloud" est que on ne sait jamais vraiment ou sont stockées physiquement les données. Parmi ses services on peut citer : la création de documents, partage de fichiers et le stockage. Ce qui permet l'amélioration de la productivité où les entreprises ne sont plus gérants de leurs serveurs informatiques mais peuvent ainsi accéder de manière évolutive à de nombreux services en ligne [1]. L'accès au service se fait par une application standard facilement disponible, la plupart du temps un navigateur web. Le NIST(National Institute of standards and technology) en a donné une définition qui reprend ces principes de base : « Le cloud computing est un modèle pratique, à la demande, pour établir un accès par le réseau à un réservoir partagé de ressources informatiques configurables (réseau, serveurs, stockage, applications et

services) qui peuvent être rapidement mobilisées et mises à disposition en minimisant les efforts de gestion ou les contacts avec le fournisseur de service» [2] . Comme c'est indiqué dans la figure 1.1

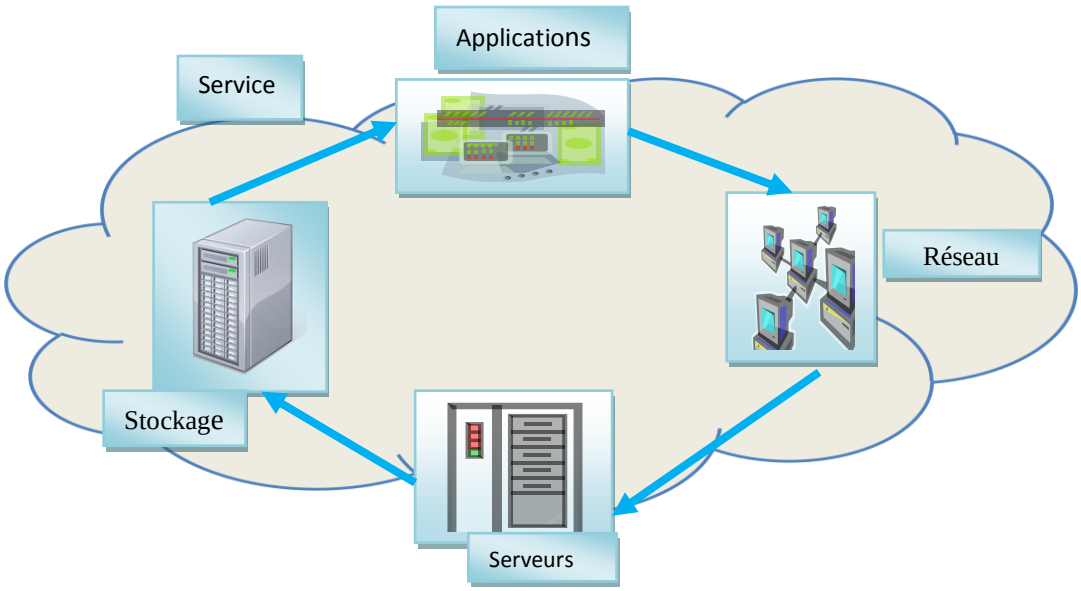


Figure 1. 1. Présentation d'un cloud computing

1.3 Evolution du cloud computing

L'adoption du cloud computing a évolué progressivement et continuellement depuis de nombreuses années. Auparavant, les informations étaient stockées massivement dans des archives papier dans des salles sur site ou hors site dédiées, et circulaient de main en main ou étaient envoyées par courrier postal. Aujourd'hui, la plupart des données sont stockées sur des serveurs que l'utilisateur ne peut pas contrôler directement et partagées dans toute l'entreprise, sans tenir compte des frontières, via de nouveaux outils tels que la messagerie électronique, les sites Web collaboratifs et les réseaux sociaux. Ce concept a été mis en œuvre en 2002 par Amazon [2], pour absorber la charge importante des commandes faites sur leur site. Récemment, d'autres acteurs comme Google et Microsoft proposent à leur tour des services similaires.

1.4 Les types du cloud computing

Un service dans le cloud doit reposer sur des ressources physiques. Une entreprise a le choix d'avoir ses propres ressources, bénéficié des offres dans un cloud publique ou bien un cloud hybride en combinant les deux, démontré dans la figure si dessous. Analysons ces trois possibilités.

Figure 1. 2. Les types du cloud computing

1.4.1 Cloud publique

Il est géré par des entreprises spécialisées qui louent leurs services à de nombreuses entreprises. Le cloud publique peut être sélectionné pour les applicatifs moins risqués comme la messagerie. Il est accessible selon le modèle « payer selon la consommation » [4].

1.4.2 Cloud privé

Il existe deux cloud privé [3] :

- Les clouds privés internes, gérés en interne par une entreprise pour ses besoins.
- Les clouds privés externes, dédiés aux besoins propres d'une seule entreprise, mais dont la gestion est externalisée chez un prestataire.

L'avantage de ce type de cloud par rapport au cloud publique réside dans l'aspect de la sécurité et la protection des données.

1.4.3 Coud hybride

- Un cloud hybride est la combinaison de cloud publique et privé. (Par exemple, un cloud dédié pour les données et un autre pour les applications) [4].
- Stockage en nuage hybride est une méthode d'évolution de stockage qui utilise les ressources de stockage locales et en nuage.

1.5 Stockage

Les services de stockage en ligne permettent de stocker des données et des documents sans avoir à augmenter continuellement le nombre de serveurs. Le cloud computing a profondément modifié notre façon de conserver nos données en les

déplaçant d'un disque dur à Internet [9]. Le stockage en nuage est une méthode de séparation de sauvegarde avec une interface bien définie de sorte qu'il peut être utilisé comme une application libre-service [8]; il doit prendre en charge une architecture multi-tenante de sorte que les données de nuages de chaque utilisateur sont gérées indépendamment de l'autre. Le stockage en nuage peut servir plusieurs objectifs:

- Le stockage pour une utilisation au jour le jour ou périodique ;
- La protection des données et de continuité, ce qui peut inclure la sauvegarde et la restauration de fonctionnalité ;
- L'archives et la gestion des dossiers, ce qui signifie recouvrable à long terme de conservation des données.

1.6 Virtualisation

La virtualisation est un ensemble de méthodes et d'outils, permettant de faire tourner plusieurs systèmes d'exploitation sur une même machine physique, c'est une technologie qui permet une gestion optimisée des ressources matérielles en disposant de plusieurs machines virtuelles sur une machine physique [10]. Aujourd'hui la plupart des serveurs possèdent des ressources matérielles importantes, mais celles-ci sont rarement utilisées à 100%, par exemple une entreprise dispose d'une quinzaine de serveurs fonctionnant chacun à 15% de ses capacités [5]. C'est pourquoi les prestataires d'un cloud y installent des outils de virtualisation qui vont permettre de disposer, sur une machine, de plusieurs systèmes d'exploitation. Lorsque l'on sait qu'un serveur tournant à 90% de ses capacités ne consomme pas beaucoup plus qu'un serveur à 10% on comprend logiquement la démarche de virtualisation.

Cette technologie vient pour répondre à certains problèmes tels que:

- L'augmentation du nombre de serveurs physiques : les ressources physiques d'un serveur seront partagées entre différents serveurs virtuels ce qui permet de ne pas acheter plusieurs serveurs physiques ;
- La sécurité et la fiabilité : isoler les services sur des serveurs différents ;
- Partage des ressources physiques : les différentes machines virtuelles installées sur le serveur partagent ces ressources à savoir le processeur, les disques durs et d'autres périphériques ;
- Isolation : les machines virtuelles sont considérées comme des ordinateurs physiques et donc possèdent chacune sa propre adresse IP [10];

- Manipulation des machines virtuelles : une machine virtuelle est un fichier situé sur un disque du serveur.

1.7 Les risques de cloud computing

Le cloud est un espace virtuel, on l'utilise sans cesse et sans se méfier. D'où, on doit être au courant des risques qu'il présente.

- **Une perte de contrôle des entreprises** ; les données les plus sensibles peuvent être stockées en local, car l'entreprise n'est plus vraiment maître du fonctionnement de son réseau informatique et de ses bases de données [1]. Supposons un instant qu'il crash, toutes les données qui y sont enregistrées, aussi confidentielles, pourraient être perdues en quelques secondes (codes de carte bancaire, mots de passe en tout genre, documents personnels…). Même un idéal fournisseur, il ne peut que bloquer l'accès aux comptes personnels durant quelques heures ;
- **Le cloud facilite le piratage informatique** : le cloud computing, c'est la cible préférée des pirates. Alors que craquer un mot de passe pouvait prendre plusieurs jours mais avec cette méthodes, cela prend à peine quelques secondes [1] ;
- Il est indispensable d'avoir la garantie de disposer des moyens pour la récupération de données en cas de problèmes (**L'usurpation d'identité** d'utilisateurs) ;
- **Feu électrique** : destruction du générateur de secours, commutateurs, etc… consigné sur la figure suivante :

Figure 1. 3. Destruction du matériel par un feu électrique

1.8 La sécurité dans le cloud

La sécurité d'un cloud peut se présenter sous plusieurs aspects :

- **La sécurité physique**

Le cloud computing par nature, est associé à une sorte de « dématérialisation » de l'hébergement. En effet, son lieu d'hébergement est généralement multiple, et réparti sur plusieurs sites de données [11]. Dans le cas du cloud publique, le client ne connaît pas précisément le ou les lieux d'hébergement. Le prestataire doit être en mesure d'apporter des garanties sur les conditions d'hébergement associées à son offre. On doit protéger les infrastructures contre les menaces physiques, comme c'est illustré sur la figure ci-dessous.

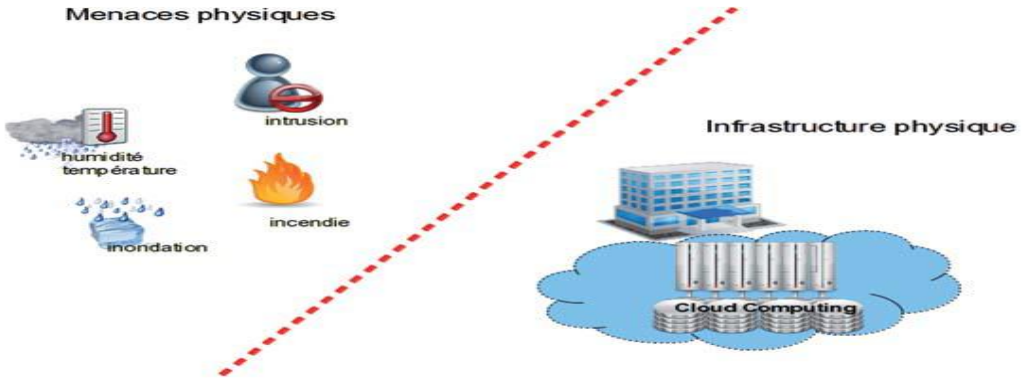


Figure 1. 4. Sécurisation de l'environnement

Le contrôle des accès doit être maitrisé, que l'on soit dans un cloud privé ou publique. Dans ces deux derniers cas, c'est au client final de s'assurer que les bonnes pratiques sont mises en œuvre chez son prestataire de service cloud. Il faut également que l'environnement physique soit aussi sécurisé. Les centres de données sont conçus pour fonctionner 24/24 et utilisent diverses mesures afin de protéger les pannes de courant, les intrusions physiques et les pannes réseaux [5]. Ces centres de données conformes aux normes de l'industrie en termes de sécurité physique et de fiabilité, surveillés et administrés par un très petit nombre de personnes dont les informations d'identification changent très régulièrement [12].

Il faut assurer les outils physiques suivants :

- Contrôle précis de la poussière environnante ;
- Unité de distribution de l'énergie ;
- Bloc d'alimentation d'urgence, ainsi que l'unité de secours ;
- Système perfectionné d'alerte d'incendie ;

- Systèmes de surveillance extérieure permanente (caméras, détecteurs de présence...).

- **Les points clés d'une architecture sécurisée dans le cloud**

a- La confidentialité

La confidentialité assure que les données d'un client ne soient accessibles que par les entités autorisées. Les différentes solutions de cloud computing comportent des mécanismes de confidentialité comme la gestion des identités et des accès, et le cryptage [11] ;

b- La disponibilité

Afin de rétablir la disponibilité totale du service, les agents surveillent l'état des machines. En cas de défaillance du matériel, le contrôleur déplace la concentration du rôle vers un nouveau nœud.

- **Sécurité d'accès**

Lors de la sélection d'un (ou plusieurs) fournisseurs pour le stockage de données dans le cloud, l'étape suivante est d'assurer l'utilisation correcte de leurs services. Le mode d'accès et de partage de données peut généralement avoir un impact très important sur leur sécurité [12]. Quelques précautions pour réduire les risques sont :

a- Authentification : L**'**utilisation des mots de passe longs et complexes pour l'authentification. Ceci évitera que des pirates accèdent aux données en devinant le mot de passe. Utiliser un fournisseur qui offre des mécanismes d'authentification à double facteur pour plus de sécurité ;

b- Partage: Le cloud rend le partage d'information très simple, il ne faut pas partager trop d'information par erreur. Le meilleur moyen d'éviter les erreurs est de ne rien partager par défaut;

c- Paramétrage: Il faut comprendre les paramètres de sécurité offerts par le fournisseur de cloud. Il ne faut pas accorder un control total à certains individus car ils peuvent partager les informations;

d- Antivirus: Il faut assurer que tous PC ayant accès aux données par l'intermédiaire de cloud doté d'un antivirus avec mis à jour ;

e- Chiffrement: plusieurs questions qui se posent :

- Comment le fournisseur de cloud chiffre-t-il les données ?
- Les clés de chiffrement sont-elles sous le contrôle du fournisseur ou sous notre contrôle ?

Une approche plus sécurisé est de chiffrer les données sur PC avant de les stocker sur le cloud. De cette façon, les données sont protégées, même si le fournisseur de cloud était compromis ;

f- Sauvegardes: Même si le fournisseur de cloud sauvegarde les données, mieux vaut, sauvegarder nous-mêmes nos données ;

g- Lecture des conditions d'utilisation, ou la licence d'utilisateur avant de contractualiser un service. Evaluer des fournisseurs alternatifs, si des conditions du contrat semblent incompréhensibles.

1.9 Centres de données

Un centre de données est organisé en armoires pouvant accueillir des éléments (switch, routeur, firewall, etc…) dans des emplacements de taille normalisée comme c'est présenté sur la figure ci-dessous. Il existe également des tiroirs coulissants contenant écran plat, clavier et souris etc... [13].

Figure 1. 5. Armoires des éléments réseaux d'un centre de données

Un centre de données est un ensemble informatique composé de serveurs, et permettant le stockage de données en un lieu sûr. Les premiers centres de données avaient pour objectif d'offrir un centre d'hébergement et de traitement des données hyper sensibles à de grandes entreprises internationales, d'un niveau de sécurité très élevé. Au fil du temps, la virtualisation des serveurs est positionné comme étant une solution économique. Les missions principales du centre sont d'offrir une bonne connexion réseau (internet, intranet, etc…) et une haute disponibilité du système d'information.

Son avantage principal est bien évidemment la qualité des infrastructures et le niveau de sécurité : (serveur performant, connexion internet haut, débit d'investissement nul,

pas de frais d'installation, pas de frais de maintenance, utilisation sur mesure, gain de place, sécurité maximale …) [14].

❖ **Sécurité et performances des centres de données**

La sécurité globale qu'offre un centre de données est articulée autour de différents axes. Elle ne se limite pas aux composants électroniques qui pourraient être défaillants, mais elle englobe l'énergie électrique, les moyens permettant de lutter contre les incendies, la sauvegarde sur plusieurs disques durs. La majorité des centres de données proposent des garanties relatives à la sécurité des serveurs :

- Sécurité de l'accès physique grâce à un contrôle d'accès (badge, carte magnétique, éventuellement biométrie) et un système de vidéosurveillance relié à un service permanent de gardiennage. La figure suivante illustre le verrouillage des armoires par un système de cadenas et parfois équipées de mécanismes de détection d'intrusion [13] ;

Figure 1. 6. Système de verrouillage des armoires

- Sécurité contre les incendies grâce à des systèmes de détection d'incendie par analyse de particules ; couplés à un système d'extinction d'incendie par gaz, comme c'est affiché sur la figure suivante ;

Figure 1. 7. Système de détection et d'extinction d'incendie dans un centre de données

- Redondance des alimentations électriques, des infrastructures (routeurs, climatisation, etc…) et des liens de connexion à internet et présence d'onduleurs, voire des groupes électrogènes de plus, un bloc d'alimentation d'urgence ainsi qu'une unité de secours [5] ;
- Garantie de la qualité de service (QoS) ainsi que du temps de rétablissement du service en cas de dysfonctionnement (GTR : Garantie de Temps de Rétablissement) ;
- Intervention par téléphone pour demander le redémarrage d'un serveur à distance ;
- Service de surveillance du trafic. Il s'agit la plupart du temps d'un système permettant de représenter graphiquement la charge du trafic sur les liens réseaux de plus des gardes de sécurité continuellement présents ;
- Climatisation précise et stable, comme c'est démontré sur la figure ci-dessous ;

Figure 1. 7. Climatisation de centre de données

1.10 Avantages et Inconvénients d'un cloud computing

- **Avantages**

On résume les avantages d'un cloud computing dans les points suivants :

- La préservation du contexte quand on change de terminal. Exemple : on commence un jeu sur une console, et on continue à jouer sur un téléphone mobile ;
- La fourniture d'une solution informatique peut être assurée dans un délai très court [11] ;
- le partage d'applications et de données est favorisé;
- Le stockage et l'hébergement des données sont assurés via une infrastructure externalisée ce qui permet aux utilisateurs de bénéficier des services en ligne ;

- L’évolution de la conservation des données en les déplaçant d’un disque dur à internet [15] ;
- l'informatique dans le nuage est plus économique grâce à son évolutivité. En effet, le coût est fonction de la durée de l'utilisation du service rendu et ne nécessite aucun investissement préalable (homme ou machine). L'élasticité du nuage permet de fournir des services évolutifs et donc de supporter les montées de charges ;
- La fiabilité des services basée sur des infrastructures performantes possédant des méthodes efficaces face aux pannes ;
- La mobilité : l’utilisateur peut à tout moment et à partir de n’importe quel appareil se connecter à ses applications. (Il peut y accéder à partir de n’importe quel type d’appareil à condition que celui-ci soit doté d’un navigateur) ;
- La souplesse pour l'entreprise : la simplicité de la résolution des problèmes de la gestion informatique.

- **Inconvénients**

Les inconvénients qu’on peut rencontrer sont les suivants :

- Les entreprises perdent le contrôle de leurs données ainsi que du cycle de vie des applications ;
- Le client d'un service de cloud computing devient dépendant de la qualité du réseau pour accéder à ce service. Aucun fournisseur de service cloud ne peut garantir une disponibilité de 100 % [16] ;
- Les clients ne disposent pas des garanties pour la récupération des données en cas de perte.

1.11 Conclusion

Face au phénomène médiatique que représente le cloud computing actuellement, on a effectué une définition pratique de cette technologie qui permet aux entreprises de disposer d'infrastructures directement en ligne sur internet avec un gain économique et une large disponibilité. On peut conclure sur le fait qu'il s'agit d’une simple évolution de la vision informatique actuelle, mais une réelle révolution dans ses usages futurs. L’essor d’une nouvelle technologie ne va pas sans ses risques qu’il faudra traiter. Même si le cloud peut se montrer menaçant, il reste un outil pratique qui mérite notre attention.

Chapitre 2 Généralités sur la cryptographie

2.1 Introduction

La cryptographie prend de plus en plus de place dans la société actuelle, nécessitent des systèmes de protection sûrs et rapides. Ce qui était réservé aux armées et aux gouvernements entre peu à peu dans la vie quotidienne.

La cryptographie a pour but de protéger nos données en les transformant en textes indéchiffrables pour ceux qui ne doivent pas y avoir accès. Deux grands types de cryptographie existent : la cryptographie symétrique et la cryptographie asymétrique, qui utilise une clé secrète connue du seul utilisateur, et une clé publique accessible à tous. En effet, le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages c'est-à-dire de les rendre impénétrables sans une action spécifique.

L'objectif de ce chapitre est de présenter brièvement la cryptographie. On va dans un premier temps présenter ses notions de base, son évolution et les services attendus de la cryptographie. Puis, on va voir les différents schémas de chiffrement ainsi que la notion de sécurité, on terminera par une conclusion.

2.2 Définitions et Concepts

La cryptologie est la science du secret. Elle se divise en deux branches : la cryptographie pour chiffrer, et la cryptanalyse pour trouver le message clair sans connaitre la clé [17]. La cryptographie est composée de 2 mots : crypto qui signifie (cacher) et graphie qui signifie (écrire). L'objet fondamental d'un système cryptographique est de permettre à deux entités ou personnes usuellement désignées par Alice et Bob, de communiquer via un canal non sécurisé de façon qu'un adversaire

Oscar, ne puisse comprendre ce qui se « dit ». Ce canal peut être une ligne téléphonique ou un réseau informatique.

L'information que Alice veut transmettre à Bob est dite texte clair. Alice crypte le texte clair, en utilisant une clé prédéterminée, pour obtenir le texte chiffré qui sera transmis via le canal. Un cryptogramme représente le texte écrit en caractères secrets. Oscar intercepte le texte chiffré mais il ne peut pas l'exploiter car il lui est incompréhensible. Bob qui possède la clé de déchiffrement peut obtenir le texte clair.

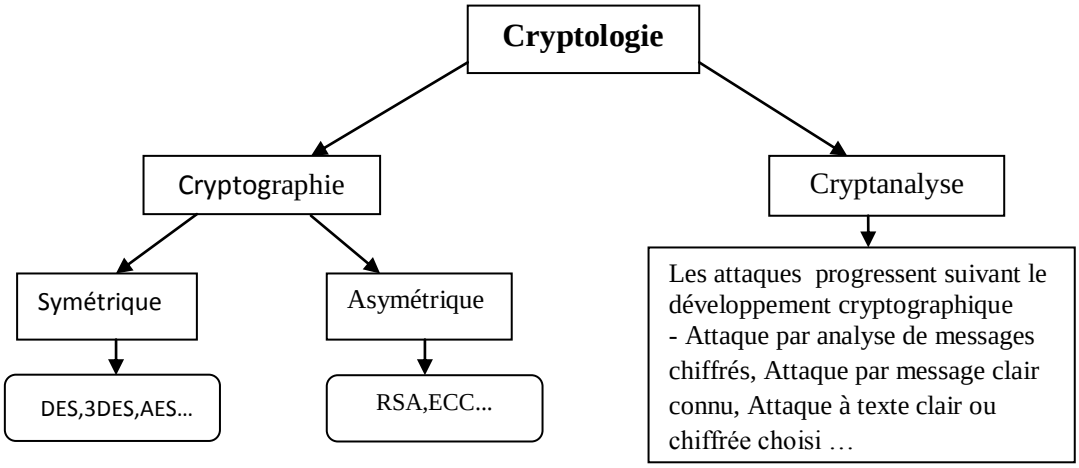


Figure 2. 1. Schéma explicite de la cryptologie

2.3 Objectifs de la cryptographie

La cryptographie a pour objectif de garantir :

- **La confidentialité** : c'est-à-dire transformer un texte clair en un texte chiffré, sans erreur, de manière à ce que seul l'expéditeur et le destinataire puissent lire le message clair ;
- **L'authentification**: identifier l'expéditeur du message de façon efficace pour prévenir toute usurpation d'identité ;
- **L'intégrité**: le destinataire doit être sûr que le message n'a pas été altéré durant la transmission;
- **La non- répudiation**: un expéditeur ne doit pas réfuter l'envoi d'un message.

2.4 Les cryptosystèmes

Les cryptosystèmes peuvent être partagés principalement en deux catégories à savoir : la cryptographie à clé secrète dite aussi symétrique et la cryptographie à clé publique ou asymétrique.

2.4.1 Cryptographie à clé privé (symétrique)

La cryptographie à clé privées, appelée aussi cryptographie symétrique est utilisée depuis déjà plusieurs siècles. C'est l'approche la plus authentique du chiffrement de données. La clé servant à chiffrer les données peut être facilement déterminée si l'on connaît la clé servant à déchiffrer et vice-versa. Dans la plupart des systèmes symétriques, le grand avantage est la simplicité des calculs qui permet de crypter et décrypter des messages très rapidement en utilisant des opérations simples.

Les algorithmes de chiffrement symétrique sont de deux types [17] :

- **Cryptosystème par flots** : le cryptage des messages se fait caractère par caractère ou bit à bit : la taille de la clé est donc égale à la taille du message ;
- **Cryptosystème par blocs** : Dans ce mode de cryptage, le texte clair est fractionné en blocs de même longueur à l'aide d'une clé unique donc bloc de n bits cryptés en blocs de n bits.

La figure suivante schématise le chiffrement symétrique :

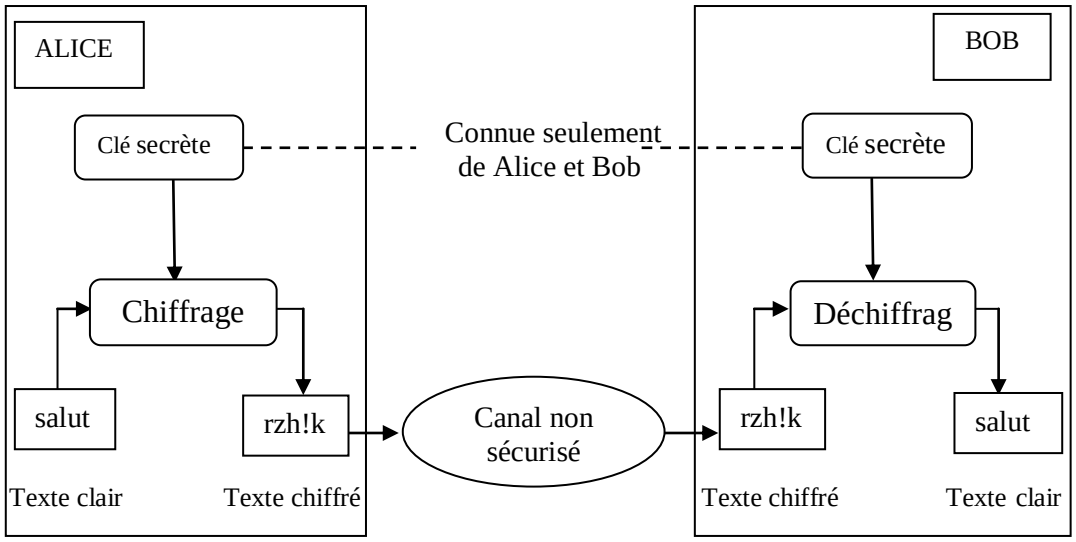


Figure 2. 2. Principe de chiffrement symétrique

De très nombreux protocoles utilisent la cryptographie symétrique :

a- Le standard de cryptage DES

Le standard de cryptage DES (Data Encryption Standard) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé, du fait de sa lenteur à l'exécution permettant une attaque systématique en un temps raisonnable [18]. Quand il est encore utilisé c'est généralement en 3DES, ce qui ne fait rien pour améliorer ses performances.

Les grandes lignes de l'algorithme sont les suivantes :

- Fractionnement du texte en blocs de 64 bits (8 octets) ;
- Permutation initiale des blocs ;
- Découpage des blocs en deux parties: gauche et droite;
- Etapes de permutation et de substitution répétées 16 fois ;
- Recollement des parties gauche et droite puis permutation initiale inverse.

b- Le standard de cryptage 3DES

Le standard de cryptage 3DES (Triple Data Encryption Standard) permet d'augmenter la sécurité du DES.

c- Le standard de cryptage AES

Le standard de cryptage AES (Advanced Encryption Standard) est comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le DES qui est devenu trop faible au regard des attaques actuelles. Les longueurs de clé de codage utilisées sont 128, 192 ou 256 bits [18].

Tous les algorithmes précédents sont symétriques en ce sens que la même clé est utilisée pour le chiffrement et le déchiffrement. Le problème essentiel de la cryptographie symétrique est la distribution des clés : pour que n personnes puissent communiquer de manière confidentielle il faut $n\ (n-1)/2$ clés.

2.4.2 Cryptographie à clé publique (asymétrique)

L'idée de base des cryptosystèmes à clés publiques a été proposée dans un article fondamental de « Diffie Hellman » en 1976. Le principe fondamental est d'utiliser des clés de chiffrement et déchiffrement différentes, non reconstructibles l'une à partir de l'autre :

- Une clé publique pour le chiffrement
- Une clé secrète pour le déchiffrement

Ce système est basé sur une fonction à sens unique, soit une fonction facile à calculer dans un sens mais très difficile à inverser sans la clé privée. Pour faire une explication enrichie, la clé publique joue le rôle d'un cadenas. Imaginons que seul Bob possède la clé (clé secrète), Alice enferme son message dans une boîte à l'aide du cadenas et l'envoie à Bob. Personne n'est en mesure de lire le message puisque seul Bob possède la clé du cadenas.

Les implémentations de tels systèmes (RSA) ont un inconvénient majeur : leur lenteur par rapport à leurs homologues à clés secrètes qui tournent eux jusqu' à près de mille fois plus vite, la figure suivante schématise le chiffrement asymétrique :

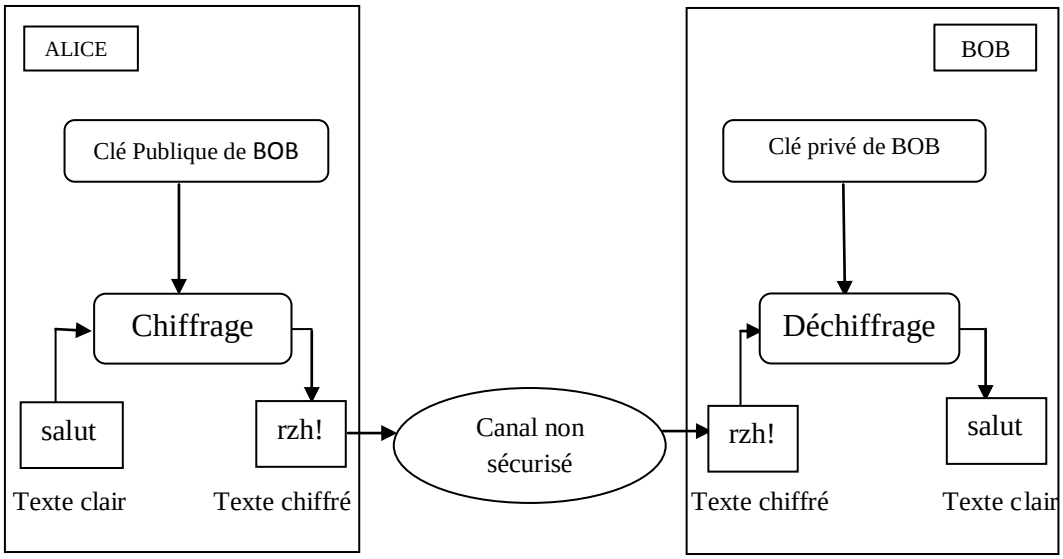


Figure 2. 3. Principe de la cryptographie asymétrique

a- Principe d'échange de clé

L'échange de clé qui repose sur le principe de « Diffie Hellman » est la première solution pratique pour le problème de la distribution des clés. En effet cette solution permet à deux entités de partager la même clé secrète sans avoir à la transmettre à travers un canal sécurisé. La sécurité de cet échange repose sur la difficulté du calcul du logarithme discret [18]. La version de base de ce protocole d'échange des clés est décrite comme suit [18] :

1- Alice et Bob se mettent d'accord sur un point P aléatoirement sur une courbe elliptique E ;
2- Alice choisit un entier a, calcule $a \times P$ et l'envoie à Bob ;
3- Bob choisit un entier b, et calcule $b \times P$ et l'envoie à Alice ;
4- Alice calcule $K = a \times (b \times P)$;
5- Bob calcule $K = b \times (a \times P)$.

Donc K est la clé secrète commune.

b- Le cryptosystème RSA

L'algorithme RSA (Rivest-Shamir-Adleman) se base sur la difficulté de factoriser de nombre élevé [17], et l'utilisation d'une clé publique pour crypter les données et une clé privée qui servira à les décrypter.

- **Génération des clés**

Pour la génération des clés on doit suivre les étapes suivantes :

Sortie : Une clé publique et une clé privée.

1: Choisir p et q deux nombres premiers distincts ;

2: Calculer $n = p \times q$;

3: Calculer produit : $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$;

4: Choisir e un entier naturel tel que e est premier avec n.

5: Calculer l'entier d tel que $d \equiv e^{-1}(mod\varphi(n))$ et inférieur (n) .

La clé publique est le couple (n, e) , la clé privée est le couple (n, d).

En pratique, les nombres premiers sont choisis suffisamment grands. Une fois les clés sont crées, si Bob veut écrire un message à Alice, il doit d'abord connaître la clé publique de Alice, qu'il lui aura donc envoyé de manière sécurisée. Puis, Bob crypte son message grâce à la clé publique de Alice, l'envoie à cet dernière qui peut le décrypter avec sa clé privée.

- **Chiffrement du message**

1 : récupérer la clé publique de Alice n, e ;

2 : représenter le message comme un entier $m \epsilon [0, n-1]$;

3 : calculer $c = m^e mod\ \varphi(n)$;

4 : envoyer c à Alice.

Pour que Alice puisse déchiffrer le message c, elle doit utiliser sa clé secrète d de la manière suivante :

- **Déchiffrement du message**

1 : recevoir le message c.

2 : calculer $m = cd\ mod\ \varphi(n)$.

2.5 Performances de cryptographie à base des courbes elliptiques

Il existe plusieurs bénéfiques lors du choix d'un système de chiffrement basé sur courbes elliptique. Les principaux critères sont :

- Attractivité : ECC nécessite moins d'espace, moins d'énergie, moins de mémoire et moins de bande passante que les autres systèmes. Cela permet de mettre en œuvre la cryptographie dans les plateformes qui sont limités, tels que les appareils sans fil, ordinateurs portables [19] ;

- Efficacité en implémentation matérielle ;
- Rapidité du calcul : L'hypothèse du logarithme discret implique quelque soit l'adversaire probabiliste, cherchant à résoudre le problème du logarithme discret, sa probabilité de succès est négligeable [20].
- La taille des clés (bits) de ECC est plus petites par rapport au RSA [21]. Le tableau suivant regroupe une comparaison de taille des clés de ces derniers :

	Taille des clés en bit			
ECC	163	256	384	512
RSA	1024	3072	7680	15360
Rapport	1:6	1:9	1:20	1:30

Tableau 2. 1. Comparaison des tailles de clés (bits)

Par exemple, l'ancienne recommandation de taille de clé RSA est de 1024 bits, pour une taille de clé ECC de 163 bits avec le même niveau de sécurité.

2.6 La cryptanalyse

Pour un cryptographe, connaitre les différentes attaques est essentiel. Le but de la cryptanalyse : trouver des moyens pour pouvoir ; dans le pire des cas parvenir à décrypter un message ; dans le meilleur trouver une partie de la clé, ou la clé entière.

On distingue quatre grandes catégories d'attaques [21]:

- **Attaque par analyse de messages chiffrés** : Oscar dispose d'un grand nombre de messages chiffrés, il essaye de trouver une méthode pour en découvrir le texte clair ou une partie de la clé ;
- **Attaque par message clair connu** : Oscar dispose d'un grand nombre de paires message clair/message chiffré, peut alors tenter de retrouver la clé ou décrypter de nouveaux messages ;
- **Attaque à texte chiffrée choisi** : Oscar intercepte l'échange des messages en les remplaçant par ces propres messages ;
- **Attaque adaptative à texte clair ou chiffrée choisi** : cas particulier de l'attaque précédente ; Oscar peut trouver le nième message en fonction de celui qui le précède.

2.7 Conclusion

On a présenté différentes méthodes de chiffrement, les attaques existantes sur les cryptosystèmes et les moyens inventés pour s'assurer de l'intégrité, de l'authentification de l'expéditeur et du destinataire d'un message. Enfin on a fait une comparaison pour choisir la méthode cryptographique, au terme de cette comparaison, il est claire que le système de chiffrement basé sur les courbes elliptiques est le plus indiqué pour la sécurité d'un cloud computing vu les contraintes imposées. Cette méthode cryptographique repose sur la théorie des courbes elliptiques qu'on va détailler dans le prochain chapitre.

Chapitre 3 Courbes Elliptiques

3.1 Introduction

La cryptographie asymétrique basée sur les courbes elliptiques est née en 1985, découverte indépendamment par V.Miller et N.Koblitz. D'une manière générale la cryptographie permet l'échange sécurisé de données entre deux entités souvent nommées Alice et Bob dans la littérature. Le développement des nouvelles technologies de télécommunication a eu pour effet de multiplier les actions nécessitant un certain niveau de sécurité. Elle permet de protéger l'accès à certaines données comme les informations bancaires, médicales, ou encore celles échangées sur le réseau internet. Ces systèmes permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels cryptosystèmes nécessitent des clés de taille beaucoup plus modeste (par exemple, une clé de 163 bits lorsque RSA utilise une clé de 1024 bits, à un niveau de sécurité équivalent) ce qui représente un avantage pour les systèmes utilisant les cartes à puces dont l'espace mémoire est très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de générations et d'échanges de clé beaucoup plus important.

Dans ce chapitre, on commence par la présentation théorique des courbes elliptiques. Puis, on aborde les notions mathématiques sur les corps finis. Et on termine par une conclusion.

3.2 Sélection de paramètres

L'implémentation d'un système ECC nécessite un nombre de sélections à différents niveaux du système de chiffrement.

- **Au niveau du corps**
  - Sélection du corps F : il peut être binaire $F_2{}^m$ ou premier F_p.
  - Choisir les algorithmes pour les opérations arithmétiques dans le corps F : l'addition (ou soustraction), la multiplication, la division (ou l'inversion).

- **Au niveau de la courbe elliptique**
  - Choisir la représentation des points : les coordonnées affines ou projectives.
  - Choisir un algorithme pour l'addition et le doublement de point.
- **Au niveau du protocole**
  - Choisir l'algorithme pour la multiplication scalaire.
  - Choisir le protocole approprié : échange de clés, chiffrement ;

3.3 Application des courbes elliptiques en cryptographie

Les courbes elliptiques ont de nombreuses applications dans des domaines très différents des mathématiques : elles interviennent ainsi en cryptologie dans le problème de la factorisation des entiers ou pour fabriquer des codes performants [17].

❖ **Courbes elliptiques sur un corps fini**

L'implémentation efficace des corps finis devient donc un point très important dans l'étude des courbes elliptiques car un grand nombre d'opérations y seront réalisées. Il existe deux grands types de corps finis, comme illustré ci- dessous.

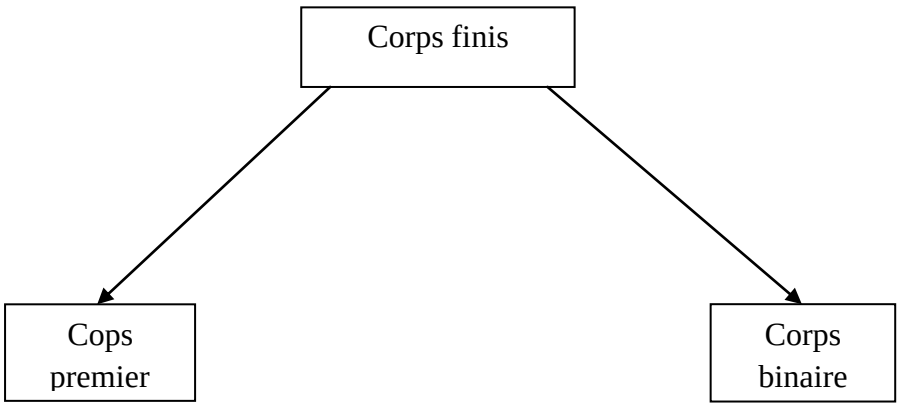


Figure 3. 1. Classification de corps finis utilisés dans le cadre des courbes elliptiques

3.4 Etude des différentes courbes elliptiques

Sur un corps fini *F*, on utilise l'équation (3.1) de Weierstrass :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (3.1)$$

Avec $a_1; a_2; a_3; a_4; a_6 \in F$ et $\Delta \neq 0$ donc E est une courbe elliptique [17], où Δ est le discriminant de la courbe calculé par les équations suivantes :

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$
$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1 a_3 \quad (3.2)$$
$$b_6 = a_3^2 + 4a_6$$
$$b_8 = -a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

On note $E(F)$ le groupe additif composé par les points de la courbe sur F et le point à l'infini ∞, l'algorithme suivant sert à étudier une courbe.

Algorithme 1 Etude d'une courbe

entrée : P, des entiers a, b.
sortie : $\boldsymbol{E}$ =courbe elliptique.
Pour $x = 0$ à $P - 1$ **faire**
$y^2 = f(x)$
si $\Delta \neq 0$ **alors**
E est une courbe elliptique
tracer E
Sinon
E n'est pas une courbe elliptique
fin si
fin pour
retourner E

La représentation de l'équation de Weierstrass sur F_p et F_{2^m} est comme suit :

a- Courbe sur F_p avec $p \neq$ de 2 ou 3

L'équation de Weierstrass devient :

$$y^2 = x^3 + ax + b$$
$$\text{avec} \quad \Delta = -16(4a^3 + 27b^2) \neq 0 \quad (3.3)$$

- L'opposé d'un point $P = (x, y) \in E(F_p)$ est le point $-P = (x, -y) \in E(F_p)$.
- Les formules d'addition et de doublement sur F_p sont les suivantes [18] :

Soit $P, Q \in E(F_p)$ ou $P = (x_1, y_1)$ *et* $Q = (x_2, y_2)$:

Si $P \neq \pm Q$ alors $P + Q = (x_3, y_3)$ avec :

$$\begin{cases} x_3 = (y_2 - y_1 / x_2 - x_1)^2 - x_1 - x_2 \\ y_3 = (y_2 - y_1 / x_2 - x_1)(x_1 - x_2) - y_1 \end{cases} \quad (3.4)$$

Si $P = Q$ alors $2P = (x_3, y_3)$ avec :

$$\begin{cases} x_3 = (3x_1^2 + a \,/\, 2y_1)^2 - 2x_1 \\ y_3 = (3x_1^2 + a/2y_1)(x_1 - x_3) - y_1 \end{cases} \quad (3.5)$$

❖ **Exemple de courbe elliptique définie sur F_p**

➢ $(E): y^2 = x^3 - 7x - 6$, tel que sa représentation est sur la figure 3.2.

- On vérifie que c'est bien une courbe elliptique en calculant le déterminant

$$\Delta = 4a^3 + 27b^2 \; mod \; p = 4(-7)^3 + 27(-6)^2 mod \; 23$$

$$-400 mod \; 23 = -377 \neq 0$$

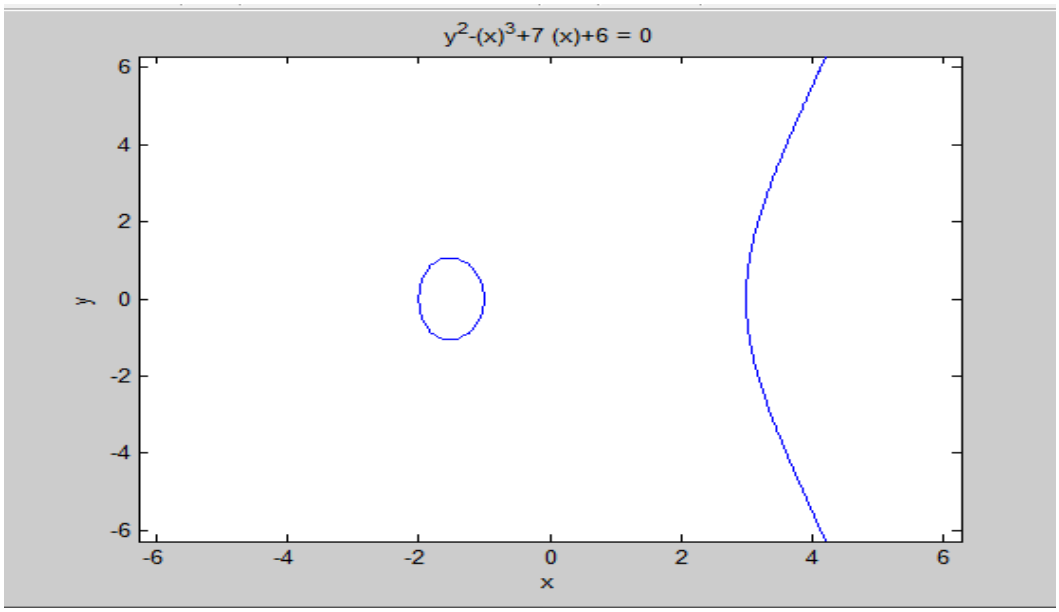


Figure 3. 2. Courbe elliptique $y^2 = x^3 - 7x - 6$ sur F_{23}

- On prend le point $P(4,7)$ et on vérifie s'il appartient à la courbe on remplaçant dans l'équation de E ;

$(7)^2 = (4)^3 - 5(4) + 5$

$49 = 64 - 20 + 5$

$49 = 49$ *d'où* $P(4,7) \in E$

- La négation des points $P\,(-4,-6), Q(17,0), R(3,9), S(0,-4)$ sont les points:

$$-P\,(-4,6), -Q(17,0), -R(3,-9), -S(0,4)$$

➢ $(E): y^2 = x^3 - 17x + 16$ définie sur F_p , sa représentation est affichée sur la figure suivante :

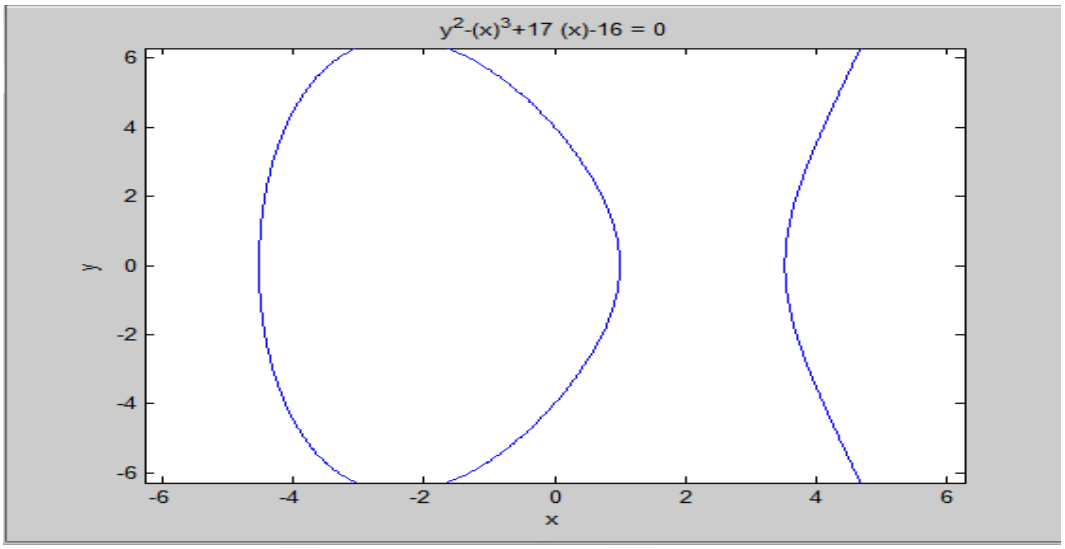


Figure 3. 3. Courbe elliptique $y^2 = x^3 - 17x + 16$ sur F_{23}

- On calcul $P + Q$ si $P = (0, -4)$ et $Q = (1,0)$

  Cas ou $P \neq Q$

$$s = \frac{(y_p - y_Q)}{(x_p - x_Q)} = \frac{(-4 - 0)}{(0 - 1)} = 4$$

$$\begin{cases} x_R = s^2 - x_p - x_Q = 16 - 0 - 1 = 15 \\ y_R = -y_P + s(x_P - x_R) = 4 + 4(0 - 15) = -56 \end{cases}$$

Alors $R = P + Q = (15, -56)$

Cas ou $P = Q = 2P$ si $P = (4,3.464)$

La formule de dédoublement:

$$s = \frac{(3x_p^2 + a)}{(2Y_P)} = \big(3 \times (4)^2 + (-17)\big)/2 \times (3.464) = 31/6.928 = 4.475$$

$$\begin{cases} x_R = s^2 - 2x_p = (4.475)^2 - 2 \times (4) = 20.022 - 8 = 12.022 \\ y_R = -y_p + s(x_p - x_R) = -3.464 + 4.475(4 - 12.022) = -3.464 - 35.898 = -39.362 \end{cases}$$

Alors $R = 2P = (12.022, -39.362)$

Remarque: comme on travaille sur un corps fini on utilise le modulo pour que nos résultats restent toujours sur le corps.

b- Courbe sur F_2^m

Dans le cas des courbes définies sur une extension de F_2^m, l'équation de Weierstrass devient [17] :

$$y^2 + xy = x^3 + ax^2 + b \tag{3.6}$$

- L'opposé d'un point $P = (x, y) \in E(F_2^m)$est le point– $P = (x, x + y) \in E(F_2^m)$.

- Les formules d'addition et de doublement sur F_2^m sont les suivantes :

Soit $P; Q \in E(F_2^m)$ ou $P = (x_1, y_1)$ et $Q = (x_2, y_2)$:

Si $P \neq Q$ alors $P + Q = (x_3, y_3)$ avec :

$$\begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \end{cases} \quad \text{tel que : } \lambda = y_1 + y_2 / x_1 + x_2 \tag{3.7}$$

Si $P = Q$ alors $2P = (x_3, y_3)$ avec :

$$\begin{cases} x_3 = \lambda^2 + \lambda + a = x_1^2 + b/x_1^2 \\ y_3 = x_1^2 \lambda x_3 + x_3 \end{cases} \quad \text{Tel que : } \lambda = x_1 + y_1 / + x_1 \tag{3.8}$$

- **Exemple de courbe elliptique définie sur F_{2^m}**

- On prend comme exemple, F_{2^4} défini à l'aide de la représentation polynomiale avec le polynôme irréductible $f(x) = x^4 + x + 1$.

On donne:

$g^0 = (0001)$ $g^1 = (0010)$ $g^2 = (0100)$ $g^3 = (1000)$ $g^4 = (0011)$ $g^5 = (0110)$

$g^6 = (1100)$ $g^7 = (1011)$ $g^8 = (0101)$ $g^9 = (1010)$ $g^{10} = (0111)$ $g^{11} = (1110)$

$g^{12} = (1111)$ $g^{13} = (1101)$ $g^{14} = (1001)$ $g^{15} = (0001)$

La figure 3.4 représente la courbe elliptique définie par : $y^2 + xy = x^3 + g^4 x^2 + 1$ *avec* $g^4 = a$ *et* $b = g^0 = 1$.

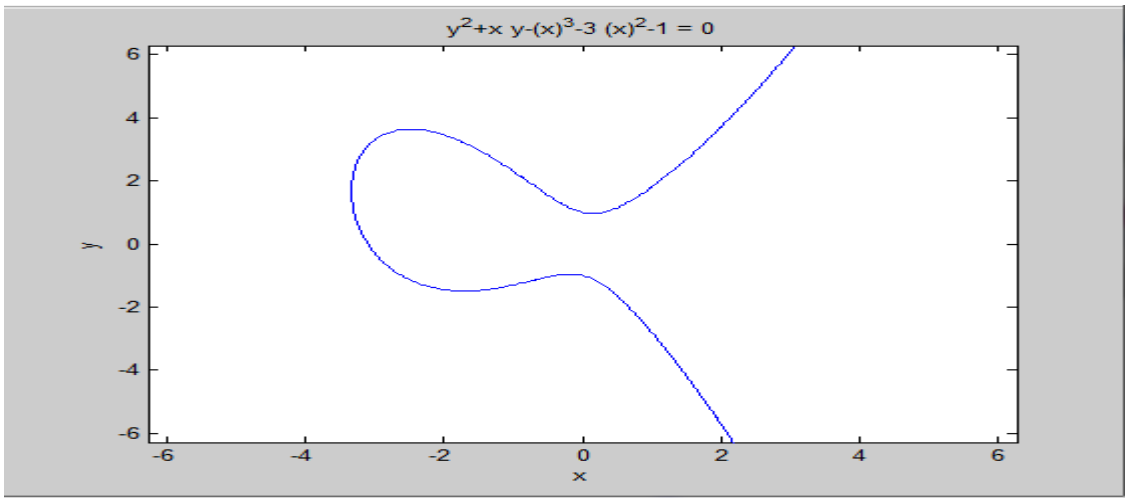


Figure 3. 4. Courbe elliptique $y^2+xy=x^3+6x^2+1$ sur F_2^4

On vérifie que Le point (g^5, g^3) satisfait cette équation sur F_{2^m}:

$y^2 + xy = x^3 + g^4 x^2 + 1$

$(g^3)^2 + g^5 g^3 = (g^5)^3 + g^4 g^{10} + 1$

$g^6 + g^8 = g^{15+} g^{14} + 1$

$(1100) + (0101) = (0001) + (1001) + (0001)$

$(1001) = (1001)$ on conclu que le point $(g5, g3)$satisfait cette équation.

- La figure 3.5 représente la courbe de l'équation : $y^2 + xy = x^3 + g^5x^2 + g^6$ définie sur F_{2^4} :

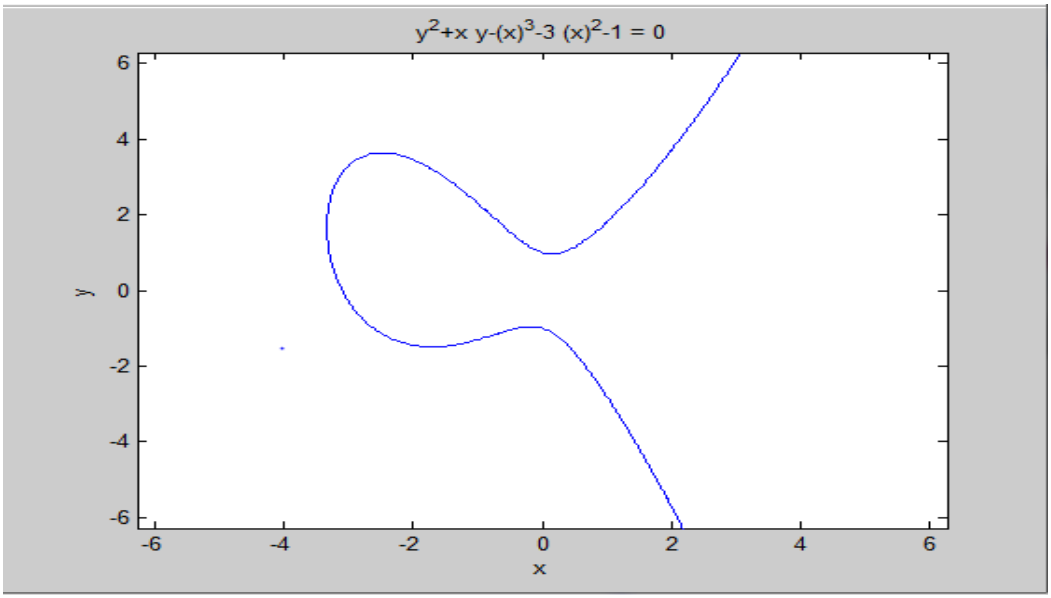


Figure 3. 5. Courbe elliptique $y^2+xy = x^3+7x^2+5$ sur $F_2{}^3$

On donne : $a = g^5, b = g^6$

$g^1 = (010)$ $g^2 = (100)$ $g^3 = (011)$ $g^4 = (110)$ $g^5 = (111)$ $g^6 = (101)$

$g^7 = (001) = 1$

On vérifie que les points $P = (g^3, g^6)$ et $Q(g^5, g^2)$ appartiennent à

$y^2 + xy = x^3 + g^2x^2 + g^6$ sur F_{2^3}

Pour $P = (g^3, g^6)$:

$(g^6)^2 + (g^3)(g^6) = (g^3)^3 + g^2(g^3)^2 + g^6$

$g^5 + g^2 = g^2 + g^1 + g^6$

$(111) + (100) = (100) + (010) + (101)$

$(011) = (011)$

$g^3 = g^3$

Pour $Q(g^5, g^2)$:

$(g^2)^2 + (g^5)(g^2) = (g^5)^3 + g^2(g^5)^2 + g^6$

$g^4 + 1 = g^1 + g^5 + g^6$

$(110) + (001) = (001) + (111) + (101)$

$(111) = (000)$: alors $Q(g^5, g^2)$ n'appartient pas à la courbe.

- On calcul l'opposé des points:

$P(g^3, g^6)$, $Q(g^5, g^2)$, $R(0, g^3)$

La négation est définie par $(x_p, x_p + y_p)$

$-P = (g^3, g^3 + g^6) = (g^3, g^4)$

$-Q = (g^1, g^1 + 0) = (g^1, g^1)$

$-R = (0, 0 + g^3) = (0, g^3)$

On calcul la somme de deux points distinct $P = (g^2, g^6)$ *et* $Q(g^5, g^5)$:

Pour $P + Q = R$:

$s = (y_P + y_Q)/(x_P + x_Q) = (g^6 + g^5)/(g^2 g^5) = g^1/g^3 = g^{-2} = g^5$

$x_R = s^2 + s + x_P + x_Q + a = g^3 + g^5 + g^2 + g^5 + g^2 = g^3$

$y_3 = s(x_P + x_R) + x_R + y_P = g^5 + (g^2 + g^3) + g^5 + g^6 = g^5 \times g^5 + g^3 + g^6$

$= g^3 + g^3 + g^6 = g^6$

Pour $P + Q = (g^3, g^6)$

On calcul le doublement : $2P$ si $P = (g^3, g^6)$:

Pour $2P = R$

$s = (y_P + y_P)/x_P = g^3 + g^4/g^3 = g^3 + g^1 = 1$

$$\begin{cases} x_R = s^2 + s + a = 1 + 1 + g^2 = g^2 \\ y_R = x_P + (s + 1) \times x_R = g^3 + 0 \times g^2 = g^3 \end{cases}$$

$2P = (g^2, g^3)$

3.5 Loi de groupe

L'ensemble des points d'une courbe elliptique, peut être muni d'une loi de groupe. Pour cela on considère une courbe elliptique défini sur un corps fini.

Soient deux points $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ d'une courbe elliptique$E$. Alors le point

$R = (x_3, y_3)$ défini par $R = P + Q \in E$.

le point R est obtenu comme suit [22]: premièrement tracer la droite qui relie les deux point P et Q, cette droite coupe la courbe en un troisième point R_1, le point R est le symétrique de R_1,par rapport à l'axe des abscisses .

- si $P \neq \pm Q$ alors $P + Q = R(x_3, y_3)$ comme c'est montré dans la figure suivante :

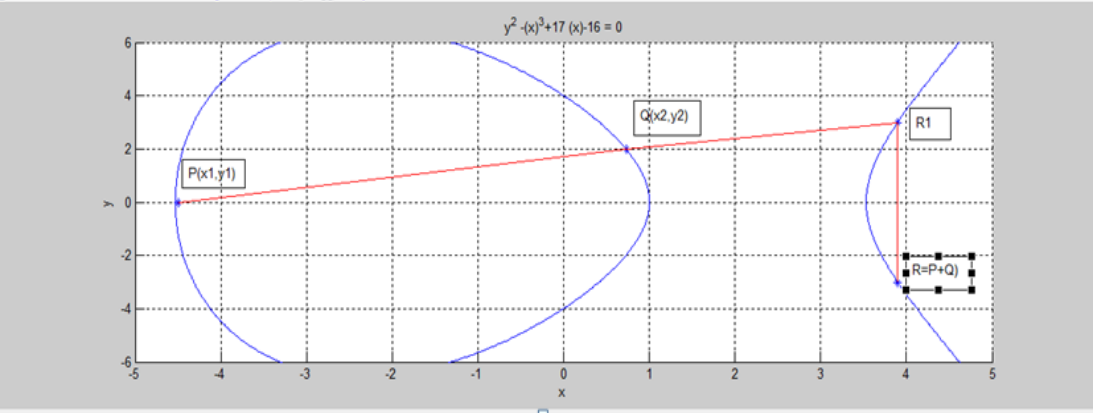


Figure 3. 6. Addition de deux points

Dans le cas où $P = Q$, on obtient R qui est le double de P comme suit : on trace la droite tangente à la courbe au point P, cette droite coupera la courbe en un deuxième point R_1, le point R est le symétrique de R_1, par rapport à l'axe des abscisses [18].

- Si $P = Q$ Alors $2P = Q = R(x_3, y_3)$ comme c'est montré dans la figure suivante :

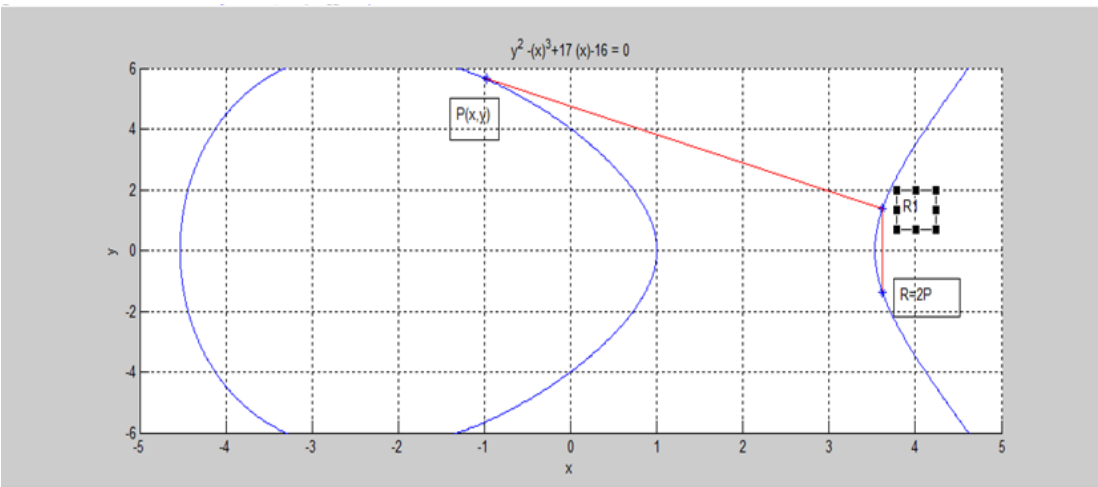


Figure 3. 7. Dédoublement de point

L'ensemble des points d'une courbe elliptique sur un corps F muni de l'opération d'addition constitue un groupe avec le point à l'infini comme élément neutre :

Si P_1 , $P_2 \epsilon\ E$

- La commutativité : $P_1 + P_2 = P_2 + P_1$;
- L'élément neutre : $P + \infty = \mathrm{P}$;
- L'inverse soit P_3le troisième point d'intersection de la droite qui relie les deux point P et ∞ avec la courbe E alors $P + \mathrm{P}_3 = \infty$ et $P = -P_3$;
- Associativité : $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

3.6 L'ordre de courbe

Le théorème ci-dessous, ne fournit qu'un encadrement du nombre de points de la courbe. Or en cryptographie, il est essentiel de connaître le nombre précis de points de la courbe elliptique manipulée [23].

- **La cardinalité**

Si p est un nombre premier, on notera dans la suite F_p un corps fini de cardinal p [23].

- **Théorème de « HASS »**

Soit p un nombre premier. Si $E(F_p)$est une courbe elliptique définie sur le corps fini F_p de cardinalité p alors la cardinalité $\#E(F_p)$ de $E(F_p)$ vérifie :

$$p + 1 - 2\sqrt{p} \leq \#E(F_P) \leq 2\sqrt{p}+p+1 \tag{3.9}$$

Le nombre de point d'une courbe E défini sur un corps F_p est dit l'ordre de E [23], il est noté$\#E(F_p)$. Le théorème de « HASS » donne les limites supérieure et inférieur de l'ordre de la courbe E.

3.7 Représentation des points et lois de groupe associées

On n'a pas encore défini formellement la cryptographie sur les courbes, mais on sait que la cryptographie asymétrique est lente en raison des tailles de nombres qu'elle utilise. De plus les éléments du corps F sont de grands nombres, c'est pour ça on entame les différents représentations des coordonnées [17], qui sont présentées sur la figure 3.8.

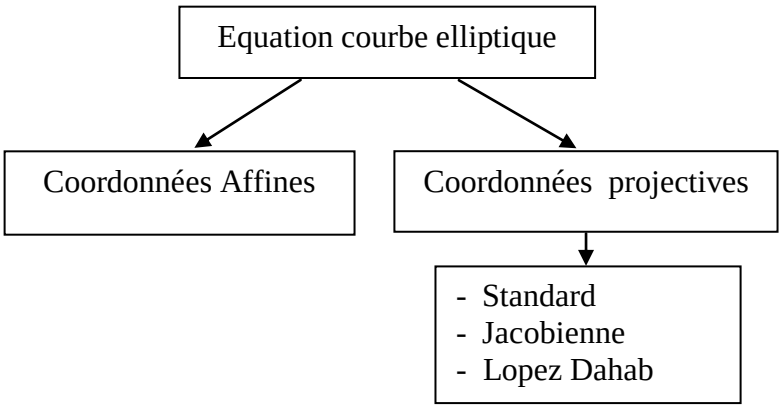


Figure 3. 8. Classification des différentes coordonnées

3.7.1 Coordonnées Affines

Soit E une courbe elliptique définie sur un corps fini F_P de l'équation suivante :

$$y^2 = x^3 + ax + b \tag{3.10}$$

Soit $P_1 = (x_1, y_1); P_2 = (x_2, y_2) \in E(F_P)$ deux points distincts de la courbe.

- L'élément neutre : pour tout point P de la courbe $P + \infty = P$;
- La commutativité : $P_1 + P_2 = P_2 + P_1$;
- L'inverse de P est $-P = (x_1, -y_1)$ on a alors : $(x, y) + (x, -y) = \infty$;
- Les formules d'addition et de doublement sont données par [22]:
  - La somme de P et Q est le point (x_3, y_3) avec :

$$\begin{cases} x_3 = \left(\frac{(y_1 + y_2)}{(x_1 + x_2)}\right)^2 + \left(\frac{(y_1 + y_2)}{(x_1 + x_2)}\right) + x_1 + x_2 + a \\ y_3 = \left(\frac{(y_1 + y_2)}{(x_1 + x_2)}\right)^3 + (x_2 + a + 1) \times \left(\frac{(y_1 + y_2)}{(x_1 + x_2)}\right) + x_1 + x_2 + a + y_1 \end{cases} \tag{3.11}$$

  - Le double de P est le point (x_3, y_3) avec :

$$\begin{cases} x_3 = (x_1 + y_1/x_1)^2 + (x_1 + y_1/x_1) + a \\ y_3 = (x_1 + y_1/x_1)^3 + (x_1 + a + 1) \times (x_1 + y_1/x_1) + a + y_1 \end{cases} \tag{3.12}$$

On remarque que ces opérations nécessitent le calcul d'inversion dans F_p qui est une opération complexe et très couteuse. Ces coordonnées sont donc très peu utilisées pour une implémentation. L'algorithme suivant permet de calculer le dédoublement de deux points en coordonnées « Affines » :

Algorithme 2 Dédoublement de point en coordonnées « Affines »

entrée : un point(x, y), en coordonnées « affines »
sortie : $Q = 2P$
  si $P = \infty$
$Q = \infty$
  fin de si
$T_1 \leftarrow y_1 + y_2$
$T_2 \leftarrow x_1 + x_2$
$x_3 \leftarrow (T_1/T_2)^2 + (T_1/T_2) + T_2 + a$
$y_3 \leftarrow (T_1/T_2)^3 + (x_2 + a + 1)(T_1/T_2) + T_2 + a$
  si $a = 1$ **alors**
$y_3 \leftarrow y_3 + T_2 + y_1$
  fin si
retourner (x_3, y_3)

L'algorithme 3 permet l'addition de deux points en coordonnées « Affines » :

Algorithme 3 Addition de deux points de coordonnées « Affines »

entrée : deux points affines $P(x_1, y_1)$ et $Q(x_2, y_2)$
sortie : $R = P + Q = (x_3, y_3)$
si $Q = \infty$
$R \leftarrow P$
fin si
si $P = \infty$ **alors**
$R \leftarrow Q$
fin si
$T_1 \leftarrow y_1/x_1 4$
$x_3 \leftarrow (x_1 + T_1)^2 + (x_1 + T_1) + a$
$y_3 \leftarrow a + y_1 + (x_1 + a + 1)(x_1 + T_1)$
si $a = 1$ **alors**
$y_3 \leftarrow y_3 + (x_1 + T_1)^3$
fin si
retourner (x_3, y_3)

3.7.2 Coordonnées projectives

Il faut trouver un moyen de remplacer les divisions, ou de ne les effectuer qu'une seule fois. La solution consiste à représenter le point $p = (x, y)$ dans un système de coordonnées projectives (X, Y, Z) telles que $(X = Z, Y = Z) = (x, y)$ vérifient l'équation de Weierstrass.

L'ensemble de tous les points projectifs est noté $P(F)$ [18]. En particulier, si $Z \neq 0$ alors $(X/Z^c, Y/Z^d, 1)$ est un point représentatif pour le point projectif (X, Y, Z) est de ce fait, il est l'unique point représentatif dont la coordonnée $Z = 1$. La forme projective d'une courbe elliptique E définie sur un corps F est obtenue en remplaçant *x* et *y* respectivement par :

$$x = X/Z^c \qquad y = Y/Z^d \tag{3.13}$$

En faisant varier les paramètres c et d, on définit plusieurs systèmes projectifs. Choisir $c = 2$ et $d = 3$ simplifie les équations sur F_p. Ces coordonnées sont appelées coordonnées « Jacobiennes ». Si on choisit $c = 1$ et $d = 2$, on obtient les coordonnées de « Lopez-Dahab ».

a- Coordonnées projectives « Standards »

Les coordonnées projectives « Standards » sont obtenues en mettant $c = d = 1$ dans l'équation (3.13), c'est à dire que le point projectif (X, Y, Z) ; $Z = 0$ correspond au point affine $X/Z, Y/Z$ avec $X; Y; Z \in F_p$.

Les lois du groupe dans ce cas sont les suivantes [22] :

- Le point à l'infini correspond à $(0,1,0)$ *;*
- L'inverse du point $P(X,Y,Z)$ est le point dans les coordonnées sont $(X,X+Y,Z)$;
- L'addition : si $P(X_1,Y_1,Z_1)$ est $Q(X_2,Y_2,Z_2)$tels que $P \neq \pm Q$

  Alors $P + Q = (X_3,Y_3,Z_3)$où :

$$\begin{cases} X_3 = BE \\ Y_3 = C(AX_1 + Y_1B)Z_2 + (A+B)E \\ Z_3 = B^3D \end{cases} \quad (3.14)$$

Avec :

$A = Y_1Z_2 + Z_1Y_2$
$B = X_1Z_2 + Z_1X_2$
$C = B^2$
$D = Z_1Z_2$
$E = (A^2 + AB + aC)D + BC$

- Dans le cas ou $P = Q$, l'addition devient alors un doublement et on a les coordonnées du point $2P(X_3,Y_3,Z_3)$ qui sont données par :

$$\begin{cases} X_3 = CE \\ Y_3 = (B+C)E + A^2 \\ Z_3 = CD \end{cases} \quad (3.15)$$

Avec :

$A = {X_1}^2$
$B = A + Y_1Z_1$
$C = X_1Z_1$
$D = C^2$
$E = (B^2 + BC + aD)$

L'algorithme 4 permet le dédoublement de point en coordonnées projectives « Standards » :

Algorithme 4 Dédoublement de point en coordonnées « Standards »

entrée : un point *(X, Y, Z)*, en coordonnées projectives « Standard »
sortie : $Q = 2P$
si $P = \infty$
$Q = \infty$
fin de si
$T_1 \leftarrow X_1 * Z_1$
$T_2 \leftarrow Y_1 Z_1$
$T_3 \leftarrow X_1^2$
$T_4 \leftarrow Y_1 {Z_1}^2$
$Z_3 \leftarrow T_1^3$
$Y_3 \leftarrow T_3^2 + T_4 + (T_3 + T_2)T_1 + aT_1^2$
si $a = 1$ **alors**
$X_3 \leftarrow T_1 Y_3$
fin si
$Y_3 \leftarrow (T_3^2 + T_2 + T_1)Y_3 + T_3^2 T_1$
retourner (X_3, Y_3, Z_3)

L'algorithme 5 permet l'addition de deux points en coordonnées « standards » :

Algorithme 5 Addition de deux points de coordonnées « Standards »

entrée : deux points projectives de « Standards » $P(X_1, Y_1, Z_1)$ et $Q(X_2, Y_2, Z_2)$
sortie : $R = P + Q(X_3, Y_3, Z_3)$
si $Q = \infty$
$R \leftarrow P$
fin si
si $P = \infty$ **alors**
$R \leftarrow Q$
fin si
$T_1 \leftarrow X_1 Z_2$
$T_2 \leftarrow Z_1 X_2$
$Y_3 \leftarrow T_1 + T_2$
$Z_3 \leftarrow (T_1 + T_2)^3 Z_1 Z_2$
$T_3 \leftarrow Y_1 Z_2$
$T_4 \leftarrow Z_1 Y_2$
$X_3 \leftarrow (T_3 + T_4)^2 + (T_3 + T_4)Y_3 + aX_3 Z_1 Z_2 + (T_1 + T_4)$
$Y_3 \leftarrow Y_3 Z_2\big((T_3 + T_2)X_1 + (T_1 + T_2)Y_1\big)$
si $a = 1$ **alors**
$Y_3 \leftarrow Y_3 + \big((T_3 + T_2) + (T_1 + T_2)\big)X_3$
fin si
$X_3 \leftarrow (T_1 + T_2)X_3$
retourner (X_3, Y_3, Z_3)

b- Coordonnées « Jacobiennes » sur F_P

En coordonnées « Jacobiennes », $c = 2$ et $d = 3$ dans l'équation 3.13, c'est à dire que le point projectif $(X, Y, Z);\ Z \neq 0$ correspond au point « affine » $(X/Z^2, Y/Z^3)$, avec $Y, Z \in F_P$.

L'équation de Weierstrass devient [22]:

$$Y^2 = X^3 + aXZ^4 + bZ^6 \tag{3.16}$$

Les lois du groupe dans ce cas sont les suivantes :

- Le point à l'infini correspond au point $(1,1,0)$
- L'inverse de (X, Y, Z) est $(X, -Y, Z)$.
- L'addition : si $P(X_1, Y_1, Z_1)$ est $Q(X_2, Y_2, Z_2)$ tels que $P \neq \pm Q$, alors

$P + \mathrm{Q} = (X_3, Y_3, Z_3)$:

$$X_3 = (Y_2 Z_1^3 - Y_1 Z_2^3)^2 - (X_1 Z_2^2 + X_2 Z_1^2)(X_2 Z_1^2 - X_1 Z_2^2)^2$$
$$Y_3 = (Y_2 Z_1^3 - Y_1 Z_2^3) - (\quad X_1 Z_2^2 + (X_2 Z_1^2 - X_1 Z_2^2)^2 - X_3) - Y_1 Z_2^3 (X_2 Z_1^2 X_1 Z_2^2)^3 \tag{3.17}$$
$$Z_3 = Z_1 Z_2 (X_2 Z_1^2 - X_1 Z_2^2)$$

- Dans le cas ou $P = Q$, l'addition devient alors un doublement et on a les coordonnées du point $2P = (X_3, Y_3, Z_3)$ qui sont données par :

$$\begin{gathered} X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1 Y_2 \\ Y_3 = (3X_1^2 + aZ_1^4)(4X_1 Y_1^2 - X_3) - 8Y_1^4 \\ Z_3 = 2Y_1 Z_1 \end{gathered} \tag{3.18}$$

L'algorithme 6 permet le dédoublement de points en coordonnées « Jacobiennes » :

Algorithme 6 Dédoublement de point en coordonnées « Jacobiennes »

entrée : un point (X, Y, Z) , en coordonnées projectives « Jacobiennes »
sortie : $Q = 2P$
si $P = \infty$
$Q = \infty$
fin de si
$T_1 \leftarrow Z_1$
$T_2 \leftarrow 2Y_1$
$Z_3 \leftarrow T_1 T_2$
$T_1 \leftarrow X_1^2$
$T_2 \leftarrow Y_1 Z_2$
$T_2 \leftarrow {Z_1}^4$
$X_3 \leftarrow (3T_1 + aT_2)^2$
$Y_3 \leftarrow 3T_1 + aT_2$
si $\boldsymbol{a = 1}$ **alors**
$X_3 \leftarrow (3T_1 + aT_2)^2$
$Y_3 \leftarrow 3T_1 + T_2$
fin si
$T_1 \leftarrow X_1$
$T_2 \leftarrow {Y_1}^2$
$X_3 \leftarrow X_3 - 8T_1 T_2$
$Y_3 \leftarrow Y_3(4T_1 T_2 - X_3) - 8T_1^2$
retourner(X_3, Y_3, Z_3)

L'algorithme 7 permet l'addition de deux points en coordonnées « Jacobiennes » :

Algorithme 7 Addition de deux points de coordonnées « Jacobiennes »

entrée : deux points projectives de « Jacobie» $P(X_1, Y_1, Z_1)$et $Q(X_2, Y_2, Z_2)$
sortie : $R = P + Q = (X_3, Y_3, Z_3)$
si $Q = \infty$
$R \leftarrow P$
fin si
si $P = \infty$ **alors**
$R \leftarrow Q$
fin si
$T_1 \leftarrow Y_2 Z_1^3$
$T_2 \leftarrow Y_1 Z_2^3$
$X_3 \leftarrow (T_1 - T_2)^2$
$Y_3 \leftarrow (T_1 - T_2)$
$T_1 \leftarrow X_1 Z_2^2$
$T_2 \leftarrow X_2 {Z_1}^2$
si $a = 1$**alors**
$X_3 \leftarrow X_3 - (T_1 + T_2)(T_2 - T_1)$
fin si
$T_3 \leftarrow X_1 Z_2^2$
$Y_3 \leftarrow Y_3 (T_1 (T_2 - T_1) - X_3)$
$Z_3 \leftarrow (T_2 - T_1) Z_1 Z_2$
$T_3 \leftarrow Y_1 Z_2^3$
$Y_3 \leftarrow Y_3 - T_3 \, (T_1 T_2)^3$
retourner (X_3, Y_3, Z_3)

c- Coordonnées de « Lopez Dahab »

Dans le cas des coordonnées de « Lopez Dahab », $c = 1$ et $d = 2$ dans l'équation 3.13, c'est-à-dire que le point projectif *(X, Y, Z); Z ≠0* correspond au point « Affine » $(X/Z^2; Y/Z^3)$.

L'équation de Weierstrass devient [22] :

$$Y^2 + XYZ = X^3 Z + aX^2 Z^2 + bZ^4 \tag{3.19}$$

Les lois du groupe pour ce type de coordonnées sont les suivantes :

- Le point à l'infini est le point $(1,0,0)$
- L'inverse de (X, Y, Z) est $(X, XZ + Y, Z)$
- L'addition : si $P(X_1, Y_1, Z_1)$est $Q(X_2, Y_2, Z_2)$ tels que$P \neq \pm Q$.

Alors $P + \mathrm{Q} = (X_3, Y_3, Z_3)$ où :

$$\begin{cases} X_3 = A(H + D) + B(C + G) \\ Y_3 = (AJ + FG)F + (J + Z_3)\, X_3 \\ Z_3 = F Z_1 Z_2 \end{cases} \tag{3.20}$$

Avec :

$A = X_1 Z_2$
$B = X_2 Z_1$
$C = A^2$
$D = B^2$
$E = A + B$
$F = C + D$
$G = Y_1 Z_2^2$
$H = Y_2 Z_1^2$
$I = G + H$
$J = IE$

Dans le cas où $= Q$, l'addition devient alors un doublement et on a les coordonnées du point $2P = (X_3, Y_3, Z_3)$qui sont données par :

$$\begin{cases} X_3 = X_1^4 + bZ_1^4 \\ Y_3 = bZ_1^4 Z_3 + X_3(aZ_3 + Y_1^2 + bZ_1^4) \\ Z_3 = Z_1^2 X_1^2 \end{cases} \quad (3.21)$$

L'algorithme 8 permet le dédoublement de points en coordonnées de « Lopez Dahab » :

Algorithme 8 Dédoublement en coordonnées « Lopez Dahab »

entrée : Un point (X, Y, Z), en coordonnées projectives de « Lopez Dahab »
sortie : $Q = 2P$
si $P = \infty$**alors**
$Q = \infty$
fin si
$T_1 \leftarrow Z_1^2$
$T_2 \leftarrow X_1^2$
$Z_3 \leftarrow T_1 T_2$
$X_3 \leftarrow T_2^2$
$T_1 \leftarrow T_1^2$
$T_2 \leftarrow T_1 b$
$X_3 \leftarrow X_3 + T_2$
$T_1 \leftarrow Y_1^2$
si $a = 1$ **alors**
$T_1 \leftarrow T_1 + Z_3$
fin si
$T_1 \leftarrow T_1 + T_2$
$Y_3 \leftarrow X_3 T_1$
$T_1 \leftarrow T_2 Z_3$
$Y_3 \leftarrow Y_3 + T_1$
retourner (X_3, Y_3, Z_3)

L'algorithme 9 permet l'addition de deux points en coordonnées « Lopez Dahab » [18] :

Algorithme 9 Addition d'un point de coordonnées « Affines » et un point de coordonnées « Lopez Dahab »

entrée : un point $P(X_1, Y_1, Z_1)$, en coordonnées projectives de « Lopez Dahab » et un point $Q(x_2,y_2)$ en coordonnées affines

sortie : $R= P+Q = (X_3, Y_3, Z_3)$

si $Q = \infty$

$R = P$

fin si

si $P =$ **alors**

$R= (x_2, y_2 ,1)$

fin si

$T_1 \leftarrow Z_1x_2$

$T_2 \leftarrow Z_1^2$

$X_3 \leftarrow X_1+T_1$

$T_3 \leftarrow T_1y_2$

$Y_3 \leftarrow Y_1+T_3$

si $X_3 = 0$ **alors**

si $Y_3= 0$

Utiliser l'algorithme précédent pour calculer $(X_3, Y_3, Z_3) = 2(x_2, y_2,1)$

fin si

retourner $R = \infty$

fin si

$Z_3 \leftarrow T_1^2$

$T_3 \leftarrow T_1Y_3$

si $a = 1$ **alors**

$T_1 \leftarrow T_1+T_2$

fin si

$T_2 \leftarrow X_3^2$

$X_3 \leftarrow T_2T_1$

$T_2 \leftarrow Y_3^2$

$X_3 \leftarrow X_3+T_3$

$T_2 \leftarrow x_2Z_3$

$T_2 \leftarrow T_2+X_3$

$T_1 \leftarrow Z_3^2$

$T_3 \leftarrow T_3+X_3$

$Y_3 \leftarrow T_3T_2$

$T_2 \leftarrow x_2+y_2$

$T_3 \leftarrow T_1T_2$

$Y_3 \leftarrow Y_3+T_3$

retourner (X_3, Y_3, Z_3)

3.8 Le coût et complexité des opérations d'addition et dédoublement

Le nombre d'opération élémentaire, addition ,multiplication et la mise au carré dans le corps F, nécessaire pour effectuer l'addition de deux points ou dédoublement de point sur une courbe elliptique E , selon les différents types de coordonnées est illustré dans le tableau suivant :

Représentation	Addition de points	Dédoublement de points
AFFINE	$2M + 1S + 8A + 1I$	$3M + 2S + 4A + 1I$
Projective Standard	$13M + 1S + 7A$	$7M + 5S + 4A$
Projective Jacobienne	$11M + 4S + 7A$	$5M + 5S + 4A$
Projective Lopez Dahab	$10M + 4S + 8A$	$5M + 5S + 4A$

Tableau 3. 1. Coût et complexité des opérations d'addition et de dédoublement

M : multiplication, S : mise au carré ; A : addition ; I : inversion dans K.

L'opération d'inversion est très couteuse, donc les coordonnées les plus efficaces sont celle de « lopez Dahab » parce que ce type de coordonnées requière au moins une multiplication et une inversion de moins par rapport aux autres coordonnées projectives.

3.9 La multiplication scalaire

Tout système cryptographique basé sur les courbes elliptiques requière une ou plusieurs multiplications scalaires sur une courbe elliptique. Cette multiplication est définie par $k \times P$, où k est un entier et P est un point de la courbe elliptique E . Cette opération est le cœur des systèmes ECC, c'est la plus lente lors de l'exécution des algorithmes de ces systèmes de chiffrement. Par conséquent, l'utilisation d'un algorithme efficace pour la multiplication scalaire représente un impact très important sur les performances de ces systèmes [17].

Calculer $k \times P$ revient à évaluer l'équation suivante:

$$Q = \underbrace{P + P + \cdots + P}_{k \text{ fois}}$$

L'addition est une addition de points dans le groupe E . Lorsque l'on parle d'addition et de doublement dans ce groupe, on parle en réalité de suites d'opérations$(+, -, \times, /, \hat{}\,2)$ sur un corps fini.

Pour réduire le temps de calcul, on peut utiliser des algorithmes très connus pour le calcul de $k \times P$ pour un k grand. On peut également améliorer le calcul pour un k petit. Il existe plusieurs méthodes de multiplication scalaire les plus utilisé sont décrit dans ce qui suit :

3.9.1 La méthode « Double and Add »

On suppose que $\#E(F_P) = nh$, où n est un entier premier et h est petit tel que $n \approx p$, les points P et Q ont un ordre n, et un entier k pris au hasard de l'intervalle $[1, n]$ [23]. La représentation binaire de k est la suivante: $k = (k_{t-1}, \dots \dots \dots k_0)$ avec $t \approx [log2(p)]$ .L'algorithme suivant est le plus simple algorithme pour le calcul de la multiplication scalaire.

Algorithme 10 « Double and Add »

Entrée : un point $P \in E$, un entier k de taille, $k = (k_{t-1}, \dots \dots k_0)$, $k_i \in \{0,1\}$

Sortie : $Q = k \times P$

$Q \leftarrow \infty$

pour i = 0 à $t - 1$ **faire**

si $k_i = 1$ **alors**

$Q \leftarrow Q + P$ // *Addition*

sinon

$P \leftarrow 2 \times P$ // *Doublement*

Fin si

Fin pour

L'algorithme 10 consiste à parcourir chaque bit de la clé [23]. A chaque étape, on va initialiser par l'élément neutre, puis, si le bit en cours est à 1, alors on ajoute le point P à ce résultat et l'on continue. Une fois le parcours est terminé, on retourne la valeur de la variable.

3.9.2 La méthode non adjacente ou « NAF »

La représentation « NAF » d'un entier peut se calculer grâce à l'algorithme 11. Dans la représentation « NAF » il n'y a pas de chiffres consécutifs différents de 0. Il nous faut deux algorithmes : un pour calculer cette nouvelle représentation (algorithme 11), un autre pour effectuer la multiplication scalaire (algorithme12) [19].

Exemple

$K = (1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1)$

$NAF(K) = (1\ 0\ \bar{1}\ 0\ 0\ 0\ 0\ 0\ \bar{1}\ 0)$

L'algorithme 11 montre la représentation « NAF » [20] :

Algorithme 11 La représentation « NAF »

Entrée :K ∈ N
Sortie : NAF(k)
$i \leftarrow 0$
tant que $K \geq 1$ **faire**
si k est impair **alors**
$K_i \leftarrow 2 - (K \ mod \ 4)$
$K \leftarrow K - K_i$
sinon
$k_i \leftarrow 0$
fin si
$K \leftarrow k/2$
$i \leftarrow i + 1$
fin tant que
retourner $(k_{i-1}, \dots \dots, k_1, k_0)$

L'algorithme 11 retourne la représentation du scalaire en base 2 où il y a un écart d'au moins un bit entre deux chiffres non nuls [20]. Une fois cette représentation calculée, on peut effectuer la multiplication scalaire grâce à l'algorithme 12.

Algorithme 12 Multiplication « NAF »

Entrée :$K \in N, P \in E(F_P)$
Sortie : $Q = KP \in E(F_P)$
Calcul de $NAF(k) = \sum_{i=0}^{i=t-1}(K_i 2^i)$
$Q \leftarrow \infty$
pour $i = t - 1$ à 0 **faire**
$Q \leftarrow 2Q$
si $k_i = 1$ **alors**
$Q \leftarrow Q + P$
Fin si
si $K_i = -1$ **alors**
$Q \leftarrow Q - P$
Fin si
Fin pour
Retourner O

Le temps d'exécution de cet algorithme est en moyenne $\approx 0{,}02 \ seconde$ [20].

3.9.3 La méthode de « Montgomery »

L'algorithme de « Montgomery » est une approche efficaces contre les attaques, sa moyenne de temps de calcul est égale à *0,02 seconde* [26], et s'appliquait uniquement à une catégorie spéciale des courbes elliptiques (les courbes de

Montgomery). L'algorithme 13 [26], représente la multiplication scalaire de « Montgomery » :

Algorithme 13 La multiplication scalaire « Montgomery » en utilisant les coordonnées « Affines »

entrée : un point P, un entier K de taille m

$k = (1, k_{m-2}, \dots \dots \dots \dots k_0), K_i[0,1]$.

sortie : $Q = k \times P$

$x_1 \leftarrow x$

$x_2 \leftarrow x + b/x^2$

pour $i = m - 2$ à 0 **faire**

$T \leftarrow x_1/x_1 + x_2$

si $K_i = 0$ **alors**

$x_2 \leftarrow x + T^2 + T$

$x_1 \leftarrow x_1^2 + b/{x_1}^2$

sinon

$x_1 \leftarrow x + T^2 + T$

$x_2 \leftarrow x_2^2 + b/x_2^2$

fin si

fin pour

$y_1 = x^{-1}(x_1 + x)[(x_1 + x)(x_2 + x) + x^2 + y]$+y

retourner $Q(x_1, y_1)$

3.10 Les opérations arithmétiques dans un corps binaire F(2^m)

L'arithmétique dans le cops $F(2^m)$ est la base de la multiplication scalaire, elle comprend l'addition (ou soustraction), multiplication, mise au carré, division et l'inversion.

3.10.1 Représentation des éléments de F(2^m)

Les éléments de $\mathrm{F}(2^m)$ sont représentés comme un vecteur binaire de dimension m en utilisant une base polynomiale :$(1, \alpha, \alpha^2, \dots \alpha^{m-1})$ ou α est la racine d'un polynôme irréductible de degré m sur $\mathrm{F}(2)$. Le corps ainsi décrit est $\mathrm{F}(2)$ [x]/f(x). Et les éléments sont des polynômes de degrés $m - 1$ au plus, modulo $P(x)$.

Exemple : Soient

– Le corps fini $F_2^4 = F_2/< X^4 + X + 1 >$

– $\alpha \in F_2^4$ tel que $F_2^4 =< \alpha >$ est racine du polynôme $X^4 + X$+1 irréductible sur F_2^4

– La courbe elliptique$E(F_2^4)$ définie par l'équation de Weierstrass

$$y^2 + xy = x^3 + \alpha^4 x^2 + 1$$

Explicitons F_2^4 en fonction de α :

Puisque α est une racine du polynôme $X^4 + X + 1$, donc $\alpha^4 + \alpha + 1 = 0$, d'où $\alpha^4 = \alpha + 1$.

Rappelons aussi que $|F_2^4|^* = 15$ donc $\alpha n = \alpha\, n\, mod(15)$.

$\alpha^5 = \alpha^4 \times \alpha = (\alpha + 1) \times \alpha = \alpha^2 + \alpha$
$\alpha^6 = \alpha^5 \times \alpha = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^6 \times \alpha = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$
$\alpha^8 = (\alpha^4)^2 = (\alpha + 1)^2 = \alpha^2 + 1$
$\alpha^9 = \alpha^8 \times \alpha = \alpha^3 + \alpha$
$\alpha^{10} = \alpha^9 \times \alpha = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^{10} \times \alpha = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^{11} \times \alpha = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha + \alpha^2 + 1 = \alpha^3 + 1$

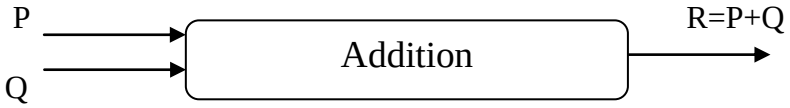
Le tableau suivant donne les correspondances entre l'écriture des éléments de F_{2^4} sous la forme d'une puissance de α, d'une combinaison linéaire d'éléments de B, ainsi que sous leur forme vectorielle [23] :

Ecriture sous forme de puissance α	Ecriture en combinaison linéaire de $\{\alpha^0, \alpha^1, \alpha^2, \alpha^3\}$	Ecriture vectorielle dans la base β
0	0	[0 0 0 0]
α^0	1	[0 0 0 1]
α^1	α	[0 0 1 0]
α^2	α^2	[0 1 0 0]
α^3	α^3	[1 0 0 0]
α^4	$\alpha + 1$	[0 0 1 1]
α^5	$\alpha^2 + \alpha$	[0 1 1 0]
α^6	$\alpha^3 + \alpha^2$	[1 1 0 0]
α^7	$\alpha^3 + \alpha + 1$	[1 0 1 1]
α	$\alpha^2 + 1$	[0 1 0 1]
α^9	$\alpha^3 + \alpha$	[1 0 1 0]
$\propto^{10}$	$\alpha^2 + \alpha + 1$	[0 1 1 1]
α^{11}	$\alpha^3 + \alpha^2 + \alpha + 1$	[1 1 1 0]
α^{12}	$\alpha^3 + \alpha^2 + \alpha$	[1 1 1 1]
α^{13}	$\alpha^3 + \alpha^2 + 1$	[1 1 0 1]
α^{14}	$\alpha^3 + 1$	[1 0 0 1]

Tableau 3. 2. Correspondances entre les différentes écritures des éléments de F_2^4

3.10.2 L'addition

L'addition de deux éléments de $F(2^m)$ est effectuée en additionnant les coefficient $mod\ 2$ [23].



Entrées: $P\ (x_1, y_1), Q\ (x_2, y_2); x_1, y_1, x_2, y_2 \in F(2^m)$
Sortie : $R\ (x_3, y_3) = P\ (x_1, y_1) + Q\ (x_2, y_2); x_3, y_3 \in F(2^m)$

Avec les coordonnées affines on a:

$$\begin{cases} x_3 = ((y_1 + y_2)/(x_1 + x_2))^2 + ((y_1 + y_2)/(x_1 + x_2)) + x_1 + x_2 + a \\ y_3 = ((y_1 + y_2)/(x_1 + x_2))^3 + (x_2 + a + 1)((y_1 + y_2)/(x_1 + x_2)) + x_1 + x_2 + a \end{cases} \quad (3.22)$$

L'addition ce n'est rien d'autre que l'opération XOR entre les coefficients de puissances égales des éléments en question comme le montre l'algorithme :

Algorithme 14 Addition dans (F_2^m)
Entrée : deux éléments $A = (a_{m-1}, a_{m-2} \dots a_0)$, $B = (b_{m-1}, b_{m-2} \dots b_0)$
Retourner : $C = A + B$
Pour m-1 to 0 **faire**
$C_i \leftarrow a_i \oplus b_i$
fin pour
retourner C

3.10.3 La multiplication

Soit *f(x)* un polynôme irréductible de degré *m* sur $F(2^m)$ de la forme [20] :

$F(x) = x^m + f_{m-1}x_{m-1} + \cdots + f_1 x + f_0$ avec $f_i \in \{0,1\}$

La multiplication de deux éléments de $GF(2^m)$ $C(x) = A(x).B(x) mod f\ (x)$ ou *:*

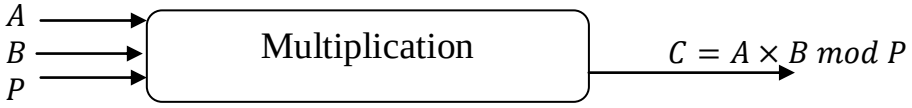
$$A(x) = \sum_0^{m-1} a_i x_i$$
$$B(x) = \sum_0^{m-1} b_i x_i$$
$$C(x) = \sum_0^{m-1} c_i x_i$$

Deux étapes sont nécessaires pour la multiplication [23] :

- la multiplication de deux polynômes de degrés $m-1$, le résultat est un polynôme de degré $2m-2$ au plus.
- la réduction modulo un polynôme irréductible, cette étapes donnera comme résultat un polynôme de degré $m-1$.

Le produit $d(x) = A(x)B(x)$ est de degré $2m - 2$, ce produit est réduit modulo un polynôme irréductible de degré m d'une manière itérative.

$$c(x) = a(x)b(x)\ mod\ f(x)$$
$$= \left(b_0 a(x) + b_1(a(x)x) + b_2(a(x)x^2) + \cdots + b_{m-1}(a(x)x^{m-1})\right) mod\ f(x)$$
$$= (b_0 a(x) + b_1(a(x)x) + b_2(a(x)x)x + \cdots + b_{m-1}(a(x)x^{m-1})x) mod\ f(x)$$



Entrées: $A(x)B(x) \in \mathrm{GF}(2^m)$, *P(x)* le polynôme irréductible
Sortie : $c(x) = A(x) \times B(x)\ mod\ P(x)$

3.10.4 La mise au carré

La mise au carré d'un élément de $\mathrm{F}(2^m)$ est plus simple que la multiplication elle peut être considéré comme une transformation linéaire.

Si $a(x) = (a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}) \in \mathrm{GF}(2^m)$ alors

$a(x)^2 = (a_0 + a_1 x + \cdots + a_{m-1}x^{2m-2})$

La représentation binaire de $a(x^2)$est obtenue en insérant de bits 0 entre les bits de la représentation binaire de $a(x)$ .cette opération est suivie d'une réduction modulo un polynôme irréductible [27]. La dernière opération n'est rien d'autre qu'une transformation définie comme suit :

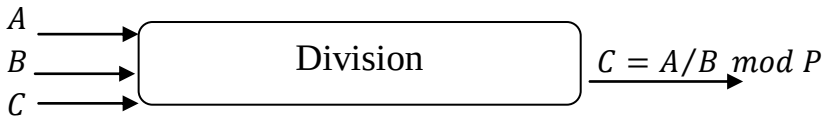
Entrées : $A(x) \in \mathrm{GF}(2^m)$, *P(x)* le polynôme irréductible
Sortie : $C(x) = A(x)^2 mod\ P(x)$

3.10.5 L'inversion ou division

L'inversion ou la division dans $\mathrm{F}(2^m)$ sont deux opérations très couteuses en terme de temps de calcul et d'espace mémoire.par conséquent le nombre de ces opérations doit être réduit au minimum [26].

Dans la méthode basée sur le théorème d'Euclide, l'opération principale est la division d'un polynôme sur x comme suit : étant donné un polynôme $p(x)$ et un polynôme irréductible $f(x)$ on a :

Entrées: $A(x) \in \mathrm{GF}(2^m)$, *P(x)* le polynôme irréductible
Sortie : $C(x) = A(x)^{-1}\ mod\ P(x)$



Entrées : $A(x), B(x) \in \mathrm{GF}(2^{\mathrm{m}})$, *P(x)* le polynôme irréductible

Sortie : $\mathrm{C(x)} = \mathrm{A(x)/B(x)\ mod P(x)}$

3.11 Protocole d'échange de clés de « Diffie Hellman » (ECDH)

Alice et Bob veulent avoir une clé en commun pour s'échanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux [28].

La méthode de « Diffie Hellman » permet justement de faire cela (en général on utilise cette méthode avec des groupes $\mathrm{F_p}^*$, mais on présente cette méthode adaptée pour les courbes elliptiques), ce protocole est présenté par les étapes suivantes :

c- Alice et Bob choisissent une courbe elliptique E définie sur un corps fini F_p, tel que le logarithme discret soit difficile à résoudre. Ils choisissent aussi un point $P \in E(F_p)$. (En général, la courbe E et le point P sont choisis de manière à ce que l'ordre p soit un grand nombre premier) ;

d- Alice choisit un nombre entier secret k_a, calcule $P_a = k_a \times P$ et envoie P_a à Bob ;

e- Bob choisit un nombre entier secret k_b , calcule $P_b = k_b \times P$ et envoie P_b à Alice ;

f- Alice calcule $k_a \times P_b = k_a \times k_b \times P$;

g- Bob calcule $k_b \times P_a = k_b \times k_a \times P$;

h- Alice et Bob utilisent une méthode quelconque connue pour extraire une clé secrète de $k_a \times k_b \times P$.

3.12 Problème du logarithme discret (DLP)

Commençons par définir ce qu'est le problème du logarithme discret dans un groupe G quelconque.

Définition : Soient G un groupe et $g \in G$. Le problème du logarithme discret dans G en base g est, pour $y \in G$ donné, de trouver un entier x tel que :

$$g^x = y$$

Dans le cas où $G = E$ est une courbe elliptique, le problème du logarithme discret en base $P \epsilon E$ est de trouver, étant donné $P \in G$, un entier x tel que :

$$Q = x \times p$$

Exemple : Dans le groupe courbe elliptique définie par : $y^2 = x^3 + 9x + 17$ sur F_{2^3}.

Quelle est le logarithme discret x de $Q = (4,5)$ à base de $P = (16,5)$ *?*

On va tenter de résoudre le problème de la façon la plus naïve possible :

$P = (16,5)$,$2P = (20,20)$, $3P = (14,14)$, $4P = (19,20)$, $5P = (13,10)$,

$6P = (7,3)$, $7P = (8,7)$, $8P = (12,17)$, $9P = (4,5)$.

On trouve que $9P = (4,5) = Q$, le logarithme discret de Q à base P est $x = 9$.

Dans l'application réelle x doit être vraiment large pour rendre la résolution du logarithme discret difficile. Revenons au protocole de « Diffie Hellman ». Les seules informations qu'un espion peut connaitre sont : la courbe E, le corps F_p et les points P, P_a, P_b . Ainsi, si l'espion veut connaitre la clé secrète commune, il doit résoudre le problème suivant :

- **Problème de « Diffie Hellman » (PDH)**

  Connaissant P, P_a, P_b des points de $E(F_p)$, peut-on trouver $k_a \times k_b \times P$?

Si l'espion peut résoudre le problème du logarithme discret sur $E(F_p)$ alors il peut résoudre le problème de « Diffie Hellman » [28]. Actuellement, on ne connait pas de moyen de trouver $k_a \times k_b \times P$ sans d'abord résoudre le problème du logarithme discret. Si quelqu'un qu'on appelle Oscar, espionne leurs communications et intercepte les points P_a et P_b, le problème du logarithme discret garantit qu'il ne sera pas en mesure de déterminer les entiers a et *b*. Il ne pourra donc pas reconstituer la clé $k_a \times k_b \times P$ commune à Alice et Bob [23].

3.13 Chiffrement « El-Gamal »

Alice veut envoyer un message secret à Bob. Tout d'abord, Bob fabrique une clé publique de la manière suivante. Il choisit une courbe elliptique E définie sur un corps fini F_p de telle manière que le problème du logarithme discret soit plus difficile à résoudre sur $E(F_p)$. Il choisit aussi un point P sur E tel que l'ordre de P soit un grand nombre premier. Il choisit un nombre entier secret k_b et calcule $B = k_b \times P$. La courbe E, le corps fini F_p et les points P et B sont la clé publique de Bob. La clé secrète de Bob est k_b. Pour envoyer le message, Alice fait comme suit [23]:

1. Elle télécharge la clé publique de Bob.
2. Elle transforme son message en un point $M \in E(F_p)$.
3. Elle choisit un nombre entier secret $k_a$et calcule $M_1 = k_a \times P$.

4. Elle calcule $M_2 = M + k_a \times B$.

5. Elle envoie M_1 et M_2 à Bob.

Bob déchiffre le message en calculant

$M = M_2 - k_b \times M_1$

On a cette égalité parce que

$$\begin{aligned} M_2 - k_b \times M_1 &= (M + k_a \times B) - k_b \times (k_a \times P) \\ &= M + k_a(k_b \times P) - k_b \times k_a \times P \\ &= M \end{aligned}$$

3.14 Conclusion

Dans ce chapitre, on a présenté l'application des courbes elliptiques dans la cryptographie qui se base sur la multiplication scalaire, et sa sécurité repose sur le problème de logarithme discret ; problème mathématique difficile à résoudre à condition de bien choisir les paramètres de la courbe. Le choix pertinent d'un système de coordonnées (projectives ou affines) permet d'avoir un gain de temps. Finalement, on a proposés des protocoles d'échange de clé suivi d'un chiffrement El-Gamal garantissant la sécurité contre différents types d'attaques, dans le prochain chapitre on s'intéresse à l'implémentation de ces protocoles.

Chapitre 4 Implémentation et Résultats

4.1 Introduction

Le cloud computing est déjà adopté par des millions d'utilisateurs, de plus en plus d'entreprises, se tournent également vers l'informatique en nuage pour des besoins informatiques variés qui leur apporte souplesse et plus d'économie. L'échange sur le réseau pose la question de la protection de la vie privé. D'où on s'intéresse dans le cadre de ce chapitre aux protocoles d'échange de clé et de chiffrement EL-Gamal. De même, une étude détaillée sur les différents types de coordonnées et méthodes de multiplication scalaire pour l'optimisation de ces derniers en termes de coût et de simplicité de calcul. Le choix des paramètres est important pour poursuivre les étapes de déroulement du travail.

4.2 Langage utilisé

MATLAB (matrix laboratoire) est un outil de calcul numérique et c'est aussi l'un des langages de programmation les plus faciles pour l'écriture de programmes mathématiques, développé par The Math Works. Il est largement utilisé dans tous les domaines des mathématiques appliquées, de l'enseignement et de la recherche dans les universités et dans l'industrie, ce logiciel est construit autour de vecteurs et matrices. Cela rend le logiciel particulièrement utile pour l'algèbre linéaire, mais MATLAB est également un excellent outil pour résoudre des équations algébriques et différentielles et pour l'intégration numérique. Il dispose d'outils graphiques puissants et peut produire des photos en 2D et en 3D [29]. C'est aussi est l'un des langages de programmation les plus faciles pour l'écriture de programmes mathématiques. MATLAB a aussi des boîtes à outils utiles pour le traitement du signal, traitement d'image, optimisation, etc…

4.3 Sécurité d'un mail

Le cloud computing, technologie de confiance utilisée par des millions d'utilisateurs, l'exemple le plus courant étant l'utilisation d'une boite de messagerie e-mail. Les e-mails peuvent contenir des données confidentielles ou personnelles, pour conserver ces données on doit assurer un niveau de sécurité efficace. Il existe plusieurs critères de protection on s'intéresse particulièrement à la cryptographie basée sur les courbes elliptiques.

Chiffrer un e-mail c'est non seulement protéger la confidentialité de l'information, mais c'est aussi une garantie pour l'expéditeur que seul le destinataire pourra le lire, Cela fonctionne avec d'une part une clé secrète commune qu'elle doit être échangé entre deux entités, qui veulent communiquer pour chiffrer l'e-mail. Par contre pour le déchiffrer il faut une clé privée qu'il faut garder secrète. Ce système de double clé est donc une méthode de chiffrement asymétrique. Pour avoir le texte en clair il faut déchiffrer chacun de son coté avec sa propre clé.

4.4 Sélection des paramètres

4.4.1 Choix d'une équation de Weierstrass

L'équation de Weierstrass d'une courbe peut s'écrire différemment, et plus simplement, grâce à un changement de variables. L'équation obtenue, dite équation simplifiée, est très utile en pratique. Une courbe elliptique E sur le corps fini F_p est un ensemble de points (x, y) vérifiant l'équation simplifiée de Weierstrass.

Sur un corps fini F l'équation de Weierstrass (3.1) prend la forme de l'équation (3.3) :

$$y^2 = x^3 + ax + b$$

- **Le choix de l'équation de Weierstrass**

On considère dans notre étude 3 cas :

- **1ier cas** : on choisi $y^2 = x^3 + 10x + 5$ définie sur F_{17} tel que:

$$\begin{cases} a = 10 \\ b = 5 \end{cases}$$

  - **Vérification de l'équation**

    Pour vérifier si cette équation représente une courbe elliptique, il faut que le discriminant de l'équation Δ soit différent de 0. Pour cela on doit calculer $\Delta = -16(4a^3 + 27b^2) mod\ p \neq 0$, en utilisant l'algorithme1 (cité dans le chapitre 3).

On trouve $\Delta = 4(10)^3 + 27(5)^2 mod\ 17 = 4675\ mod\ 17 = 0$, comme c'est montré sur la figure ci-dessous.

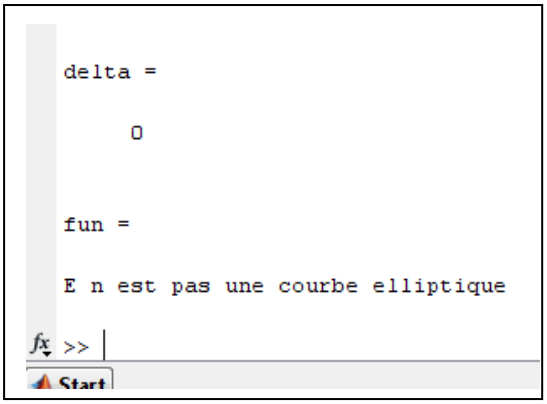


Figure 4. 1. Vérification de $y^2=x^3 + 10x + 5$ sur F_{17}

Par conséquent, cette équation ne représente pas une courbe elliptique car $\Delta = 0$, sa représentation est affichée sur la figure suivante:

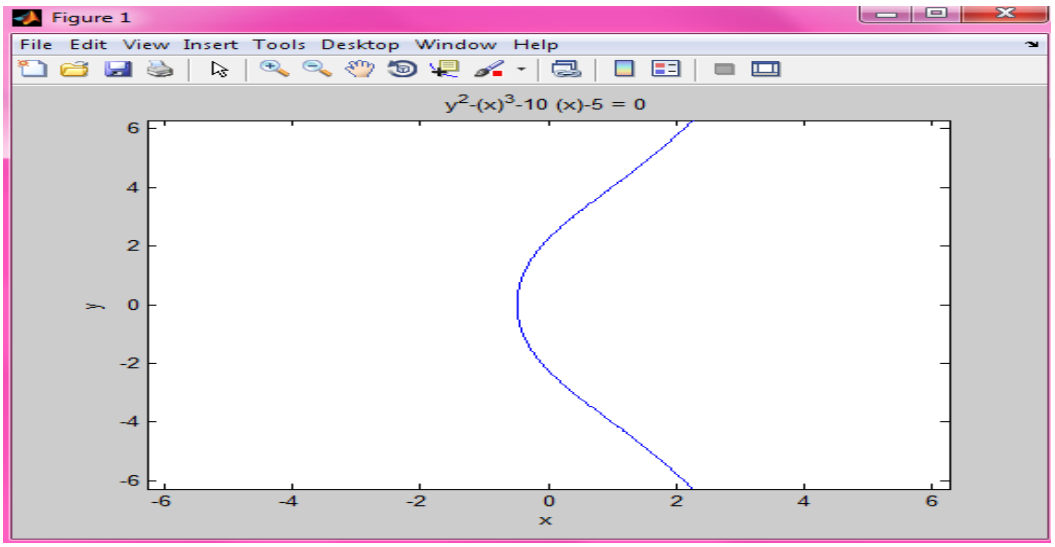


Figure 4. 2. Représentation de l'équation $y^2=x^3 + 10x + 5$

- **2^{eme} cas:** on choisie une équation : $\boldsymbol{y^2 = x^3 - x}$ définie sur $\boldsymbol{F_{23}}$, tel que :

$$\begin{cases} a = -1 \\ b = 0 \end{cases}$$

  - **<u>Vérification de l'équation</u>**

    On applique le même principe comme le 1^{ier} cas, il faut que le discriminant de l'équation Δ soit différent *de* 0.

    On trouve $\Delta = -4\ mod\ 23 = 19 \neq 0$ ce qui est assuré sur la figure ci-dessous, donc cette équation représente bien une courbe elliptique.

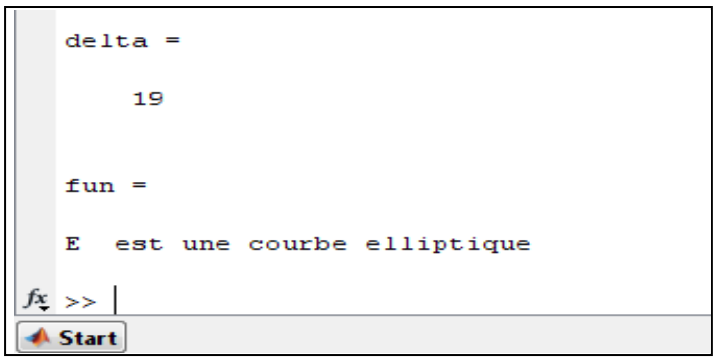


Figure 4. 3. Vérification de $y^2 = x^3 - x$ sur F_{23}

La figure suivante nous donne l'allure de cette courbe elliptique.

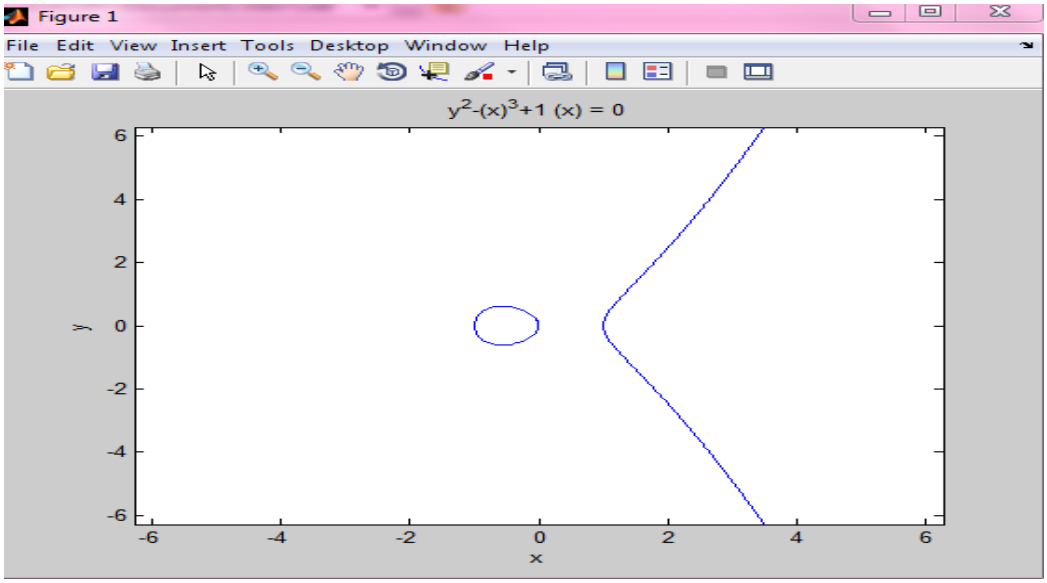


Figure 4. 4. Représentation de l'équation : $y^2 = x^3 - x$ sur F_{23}

- **3eme cas : on** choisi une équation $y^2 = x^3 - 5x + 4$ définie sur le corps fini F_{23}, tel que :

$$\begin{cases} a = -5 \\ b = 4 \end{cases}$$

  - **<u>Vérification de l'équation</u>**

    On calcule Δ et on trouve $\Delta = -68 \; mod \; 23 = 1 \neq 0$ ce qui est prouvé par la figure 4.5, donc cette équation représente une courbe elliptique.

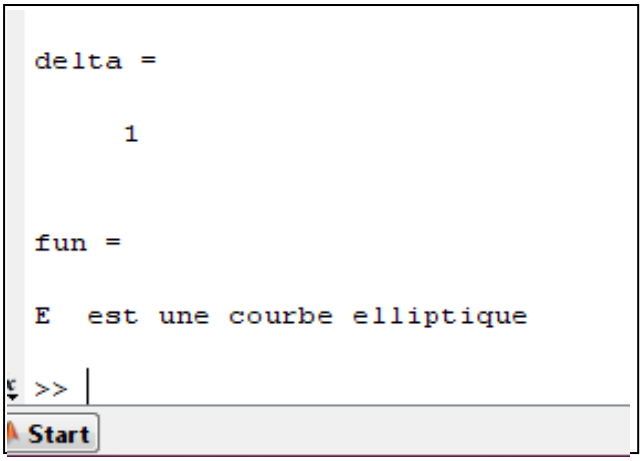


Figure 4. 5. Vérification de $y^2=x^3-5x+4$ sur F_{23}

La figure suivante nous donne l'allure de cette courbe elliptique.

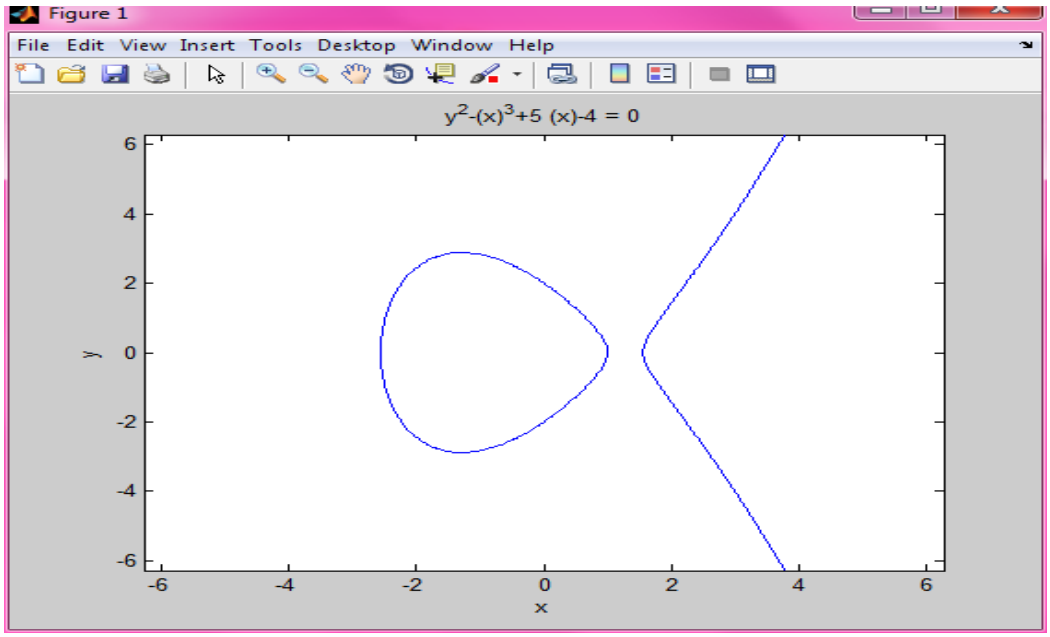


Figure 4. 6. Représentation de l'équation $y^2=x^3-5x+4$ sur F_{23}

Interprétation

On a étudié trois équations différentes pour voir si elles représentent des courbes elliptiques, on a trouvé les résultats suivants :

- Dans le 1^{ier} cas : $\Delta = 0$ donc l'équation ne représente pas une courbe elliptique ;
- Dans le 2^{eme} et le 3^{eme} cas : $\Delta \neq 0$, ces deux équations représentent des courbes elliptiques.

On choisie l'équation $y^2 = x^3 - 5x + 4$ définie sur F_{23} pour la suite de notre travail.

4.4.2 Extraction des points de la courbe

La courbe elliptique se compose d'un nombre fini de points correspondant, avec un point à l'infini ∞. Les points d'une courbe elliptique sont donc des couples (x, y), avec x et y réels qui vérifient l'équation $y^2 = x^3 + ax + b$. On tire ces points grâce à l'organigramme 2 (annexe B).

- On commence par diviser l'équation en deux parties :
    - partie droite $(EG = y^2)$
    - partie gauche $(ED = x^3 - 5x + 4)$
- On vérifie que $EG = ED$

Deux cas se posent :

- **Pour p un petit nombre premier : $p = 23$**

  Vérification du point $P(x, y)$

  Cette équation est satisfaite pour $x = 2, y = 5$.

  $$y^2 \ mod \ p = (x^3 - 5x + 4) \ mod \ p \qquad (*)$$
  $$5^2 \ mod \ 23 = (2^3 - 10 + 4) \ mod \ 23$$
  $$25 \ mod \ 23 = 2 \ mod \ 23$$
  $$2 = 2$$

En utilisant $(*)$ on obtient le tableau ci-dessous :

x	$Ed = (x^3 - 5x + 4) \ mod \ p$	y	$Eg = y^2 \ mod \ p$
0	4	0	0
1	0	1	1
2	2	2	4
3	16	3	9
4	2	4	16
5	12	5	2
6	6	6	13
7	13	7	3
8	16	8	18
9	21	9	12
10	11	10	8
11	15	11	6
12	16	12	6
13	20	13	8
14	10	14	12
15	15	15	18
16	18	16	3
17	2	17	13
18	19	18	2
19	6	19	16
20	15	20	9
21	6	21	4
22	8	22	1

Tableau 4. 1. Calcul des points de la courbe sur F_{23}

Remarque : pour extraire les points de la courbe :

- A chaque fois la vérification que $Ed = Eg$ et on prend leurs position (x, y)

Les points qui appartiennent à la courbe sont :

(1,0) (2,5) (2,18) (3,4) (3,19) (4,5) (4,18) (5,9) (5,14) (6,11) (6,12) (7,6) (7,17) (8,4) (8,19) (12,4) (12,19) (16,8) (16,15) (17,5) (17,18) (19,11) (19,12) (21,11) (21,12) (22,10) (22,13).

On applique le théorème de « Hass » de l'équation (3.9) pour avoir l'intervalle des limites supérieurs et inférieurs du nombre de point, on obtient les résultats suivants :

$$p + 1 - 2\sqrt{23} \leq \#E(F_{23}) \leq 2\sqrt{23} + 23 + 1$$

$$|14| \leq \#E(F\_23) \leq |33|$$

D'après nos calculs on a trouvé 27 solutions qui appartiennent à l'intervalle [14,33]

Remarque : on prend la valeur absolue car le nombre de points doit être entier.

La figure suivante représente les points de la courbe sur F_{23} :

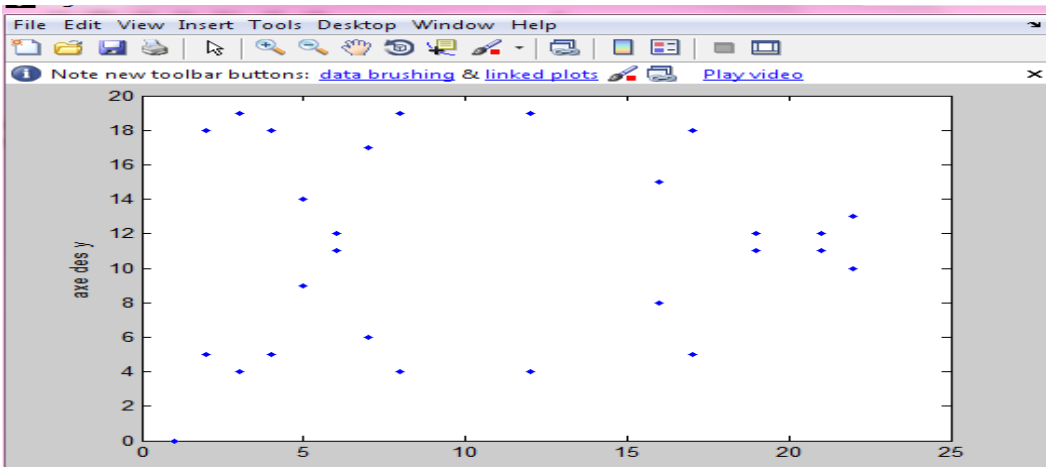


Figure 4. 7. Représentation des points de la courbe sur F_{23}

- **Pour p un grand nombre premier : $p = 71$**

  Vérification d'un point : Cette équation est satisfaite pour $x = 9, y = 7$.

  $y^2 \ mod \ p \ = \ (x^3 - 5x + 4) \ mod \ p \qquad (*)$

  $7^2 \ mod \ 71 \ = \ (9^3 - 45 + 4) \ mod \ 71$

  $49 \ mod \ 71 = \ 688 \ mod \ 71$

  $49 = \ 49$

Pour extraire les points de la courbe on applique le même principe qu'on a utilisé précédemment donc, à chaque fois on vérifie que $Ed = Eg$ et on prend leurs positions (x, y).

Les points qui appartiennent à la courbe sont :

(0,2)(1,0)(2,12)(2,59)(3,4)(3,67)(4,30)(4,41)(6,30)(6,41)(8,11)(8,60)(9,7)(9,64)
(11,12)(11,59)(13,19)(13,52)(15,31)(15,40)(17,2)(17,69)(21,1)(21,70)(23,25)
(23,46)(24,17) (24,54) (27,13) (27,58) (28,27) (28,44) (29,26) (29,45) (30,4)(70,47)
(30,67) (38,4)(38,67) (43,29) (43,42) (45,33) (45,38) (47,28) (47,43) (49,20) (49,51)
(54,2) (54,69) (58,12) (58,59) (59,18) (59,53) (60,19) (60,52) (61,30) (61,41)
(62,32)(62,39)(63,10)(63,61)(69,19)(69,52)(70,24).

On applique le théorème de « Hass » de l'équation (3.9) pour avoir l'intervalle des limites supérieurs et inférieurs du nombre de point, on obtient les résultats suivants :

$$p + 1 - 2\sqrt{71} \leq \#E(F_{71}) \leq 2\sqrt{71} + 71 + 1$$

$$|55| \leq \#E(F_{71}) \leq |88|$$

D'après nos calculs on a trouvé 66 solutions qui appartiennent à l'intervalle [55,88]

La figure suivante représente les points de la courbe sur F_{71} :

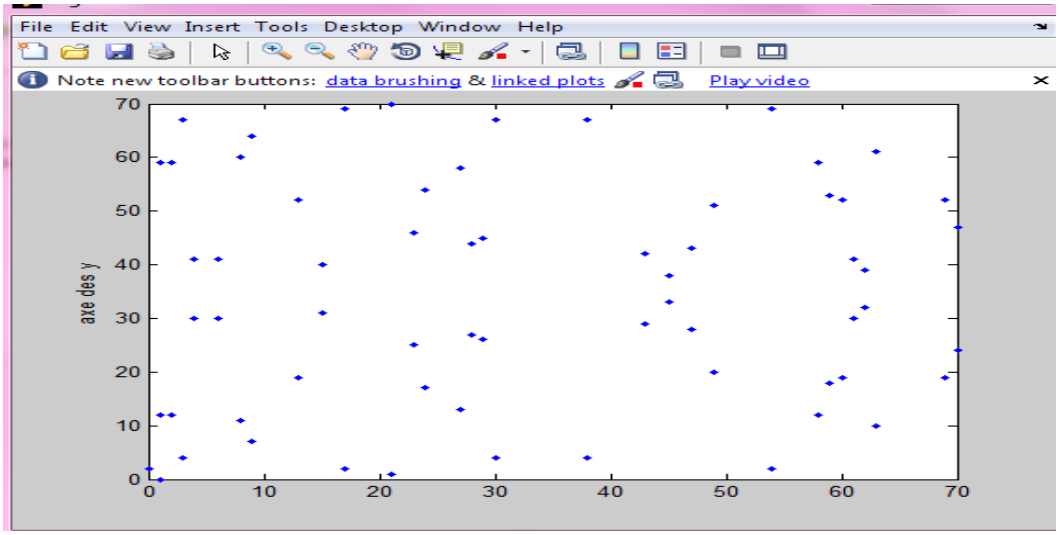


Figure 4. 8. Représentation des points de la courbe sur F_{71}

Interprétation

On a prit deux cas pour étudier l'impact de p sur le nombre de points on a obtenu :

- Pour $p = 23$ on a obtenu 27 solutions (points) ;
- Pour $p = 71$ le nombre de solution augmente jusqu'à 66 solutions.

4.4.3 Etude de différentes coordonnées

L'ensemble des points d'une courbe elliptique, et le point à l'infini forment un groupe. L'efficacité du calcul des opérations de groupe, l'addition et le doublement de points, est essentielle. La complexité de ces calculs varie en fonction de la représentation des points de la courbe choisie. Dans cette étape, on traite les différentes coordonnées sur des corps finis.

L'unité arithmétique et logique pour l'ECC doit être performante: temps d'exécution court, sécurité face à d'éventuelles attaques théoriques et physiques. On doit trouver le meilleur compromis performances/sécurité.

- **Temps d'exécution : complexité**

Dans cette partie, on aborde les notions de temps de calcul, de complexité et d'efficacité d'un algorithme. Il s'agit en pratique de pouvoir évaluer la durée (en unités de temps) nécessaire à l'exécution d'un algorithme. La capacité mémoire (ou complexité en espace) que peut nécessiter un algorithme n'est pas prise en considération, même si elle reste un paramètre important. Deux types de représentation de points existent: affine et projective, on va évaluer les performances de chacune en fonction du temps de calcul ainsi que la complexité. On choisit deux points de la courbe ($P(19,11)$, $Q = (6,11)$) pour implémenter les algorithmes d'addition et dédoublement :

- **Dédoublement du point P en coordonnées « Affines »**

On implémente l'algorithme 2 (cité dans le chapitre 3), dont l'exécution du programme correspondant donne les résultats affichés sur la figure suivante :

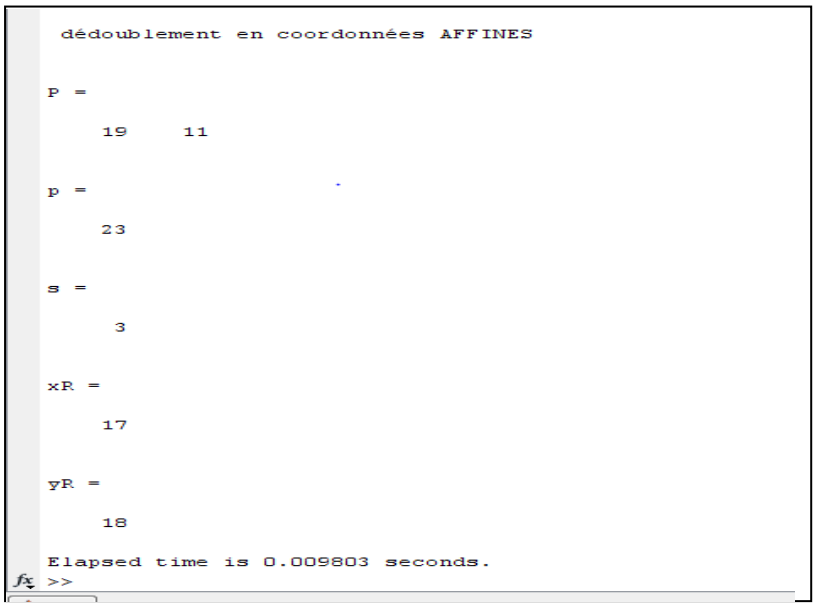


Figure 4. 9. Temps de calcul du dédoublement « Affine »

- **Addition des points P et Q en coordonnées « Affines »**

Après l'implémentation de l'algorithme 3 (cité dans le chapitre 3) et son exécution, on trouve les résultats présentés dans la figure suivante :

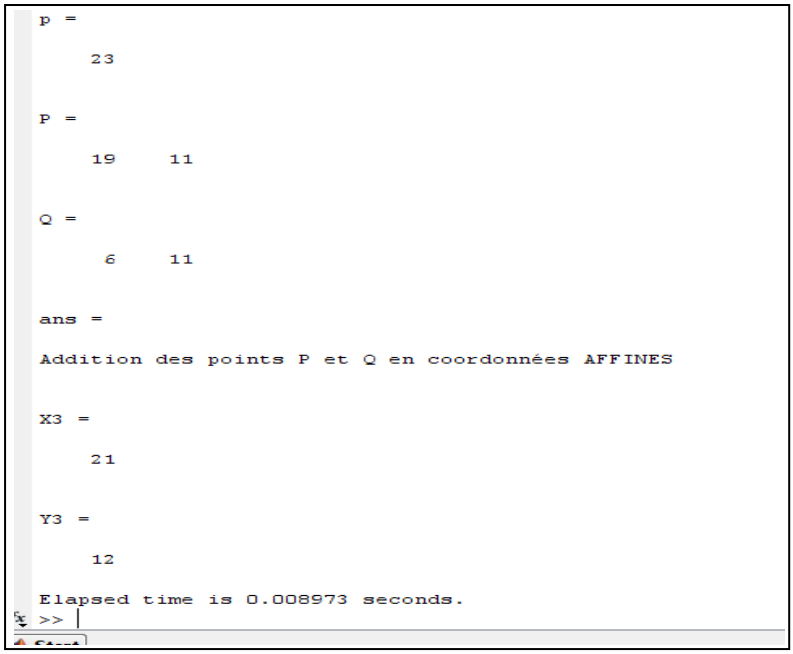


Figure 4. 10. Temps de calcul d'addition « Affine »

- **Dédoublement du point *P* avec $z = 1$ en coordonnées « Jacobiennes »**

On implémente l'algorithme 6 (cité dans le chapitre 3) après exécution de son programme, on trouve les résultats affichés sur la figure suivante :

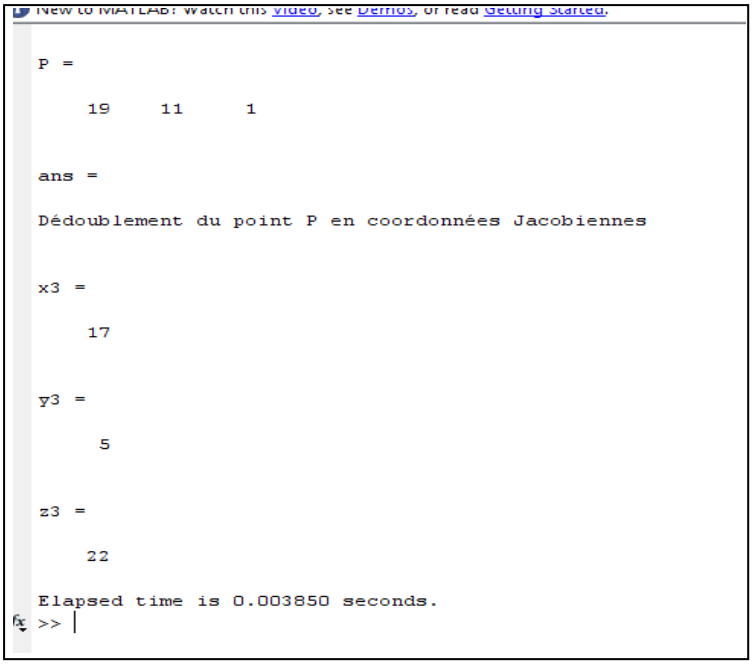


Figure 4. 11. Temps de calcul du dédoublement « Jacobie »

- **Addition des points *P* et Q avec $z_1 = z_2 = 1$ en coordonnées « Jacobiennes »**

On implémente l'algorithme 7 (cité dans le chapitre 3), dont l'exécution de son programme correspondant, on trouve les résultats affichés dans la figure suivante :

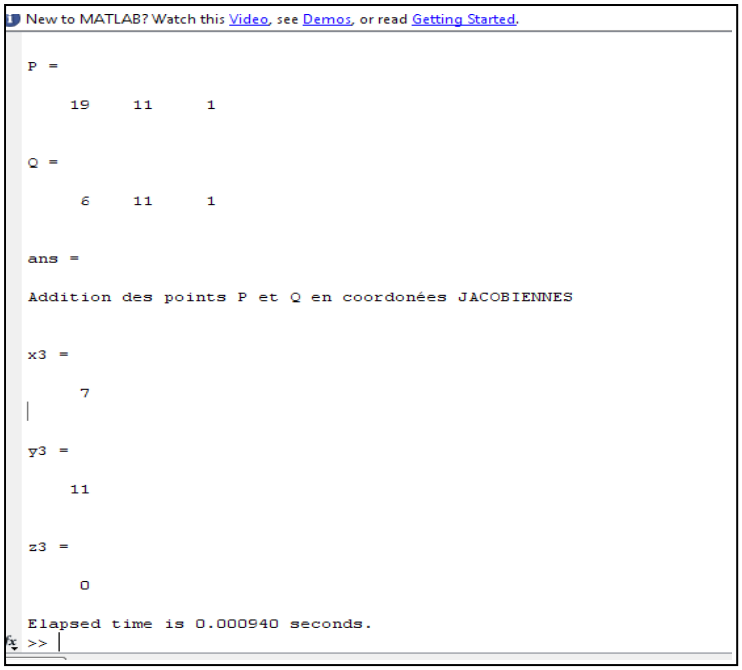


Figure 4. 12. Temps de calcul d'addition « Jacobie »

- **Dédoublement du point P avec $z = 1$ en coordonnées « Standards »**

On implémente l'algorithme 4 (cité dans le chapitre 3), les résultats trouvés sont présentés dans la figure 4.13 :

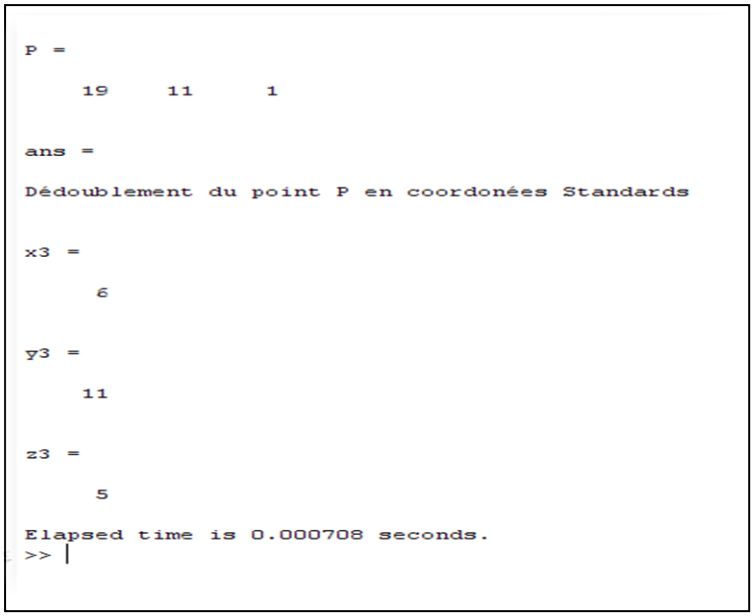


Figure 4. 13. Temps de calcul du dédoublement « Standard »

- **Addition des points P et Q avec $z_1 = z_2 = 1$ en coordonnées « Standards »**

On implémente l'algorithme 5 (cité dans le chapitre 3) et on trouve les résultats suivants :

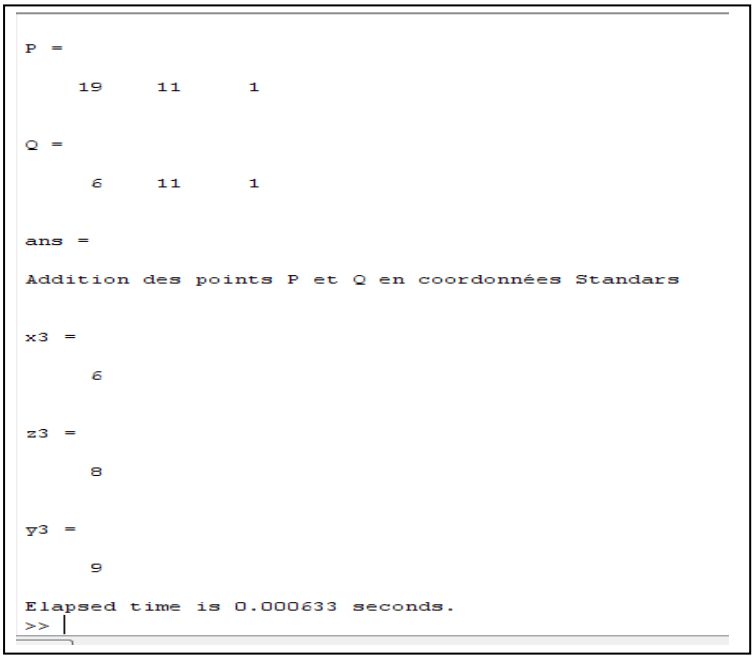


Figure 4. 14. Temps de calcul d'addition « Standard »

- **Dédoublement du point P avec $z = 1$ en coordonnées « Lopez Dahab »**

On implémente l'algorithme 8 (cité dans le chapitre 3) et on obtient les résultats suivants :

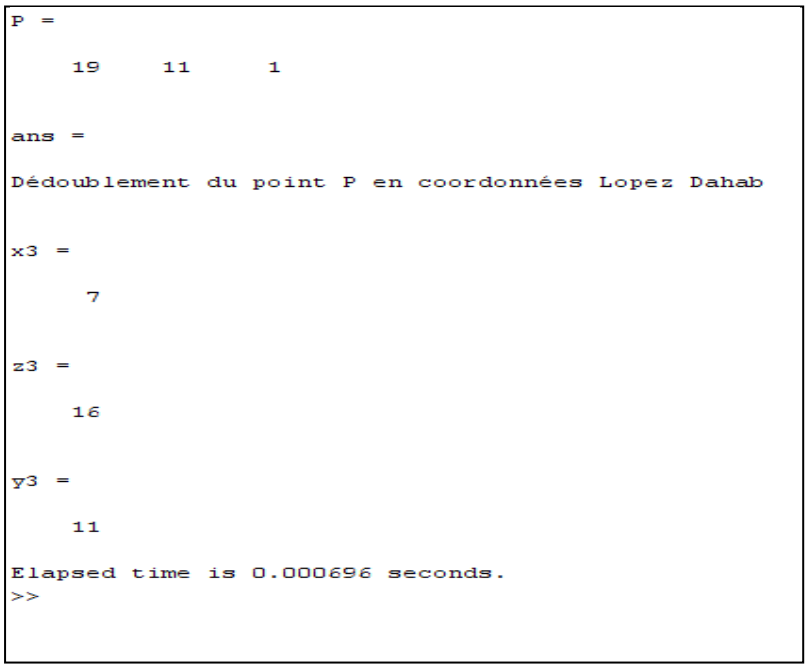


Figure 4. 15. Temps de calcul du dédoublement « Lopez Dahab »

- **Addition des points P et Q avec $z_1 = z_2 = 1$ en coordonnées « Lopez Dahab »**

On implémente l'algorithme 9 et on obtient les résultats affichés dans la figure suivante :

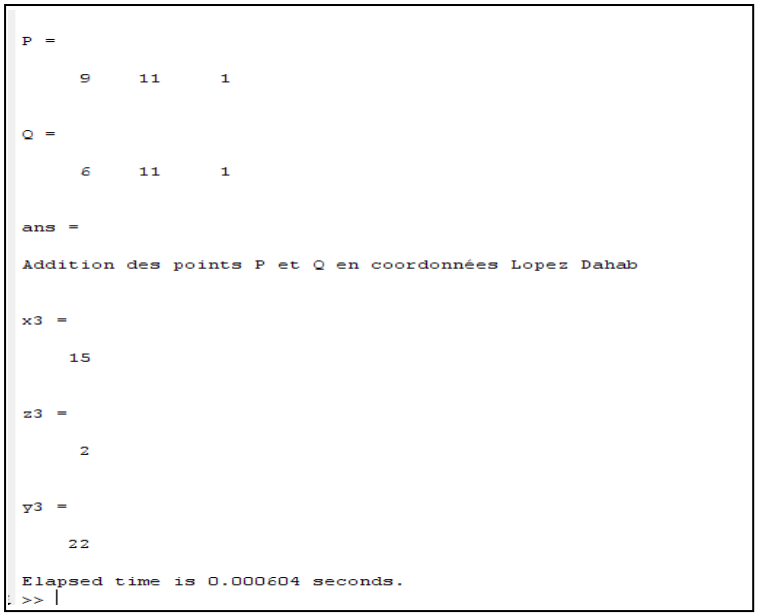


Figure 4. 16. Temps de calcul d'addition « Lopez Dahab »

Le temps de calcul de l'addition et du dédoublement des différentes coordonnées est regroupé dans le tableau 4.2. L'histogramme correspondant est illustré sur la figure 4.17.

Coordonnée	Temps de calcul (seconde)	
	Addition	Dédoublement
Affine	0.00897	0.00980
Jacobie	0.00094	0.00385
Standard	0.000633	0.000708
Lopez Dahab	0.000604	0.000696

Tableau 4. 2. Temps de calcul de l'addition et dédoublement pour différentes coordonnées

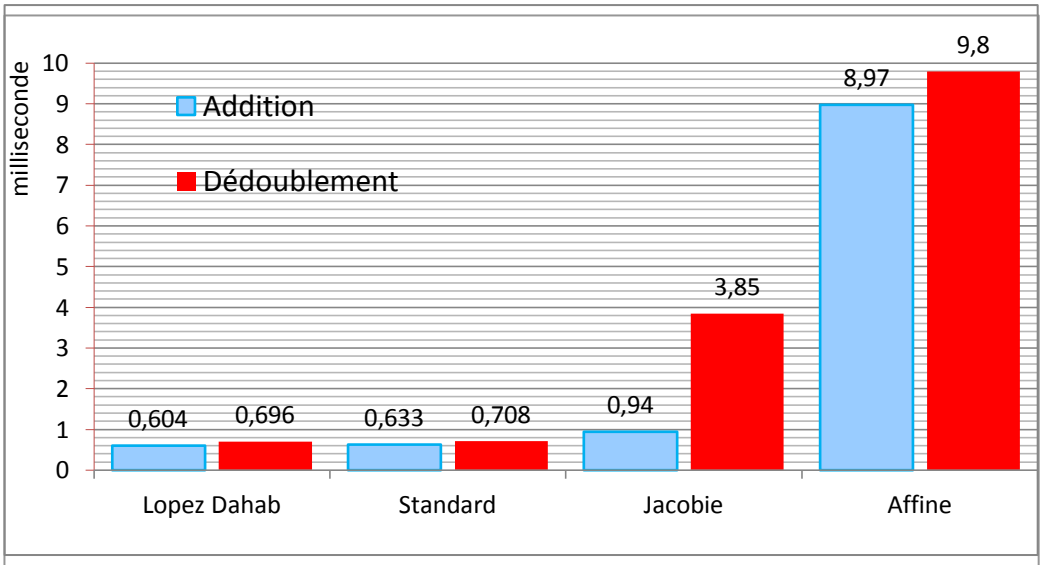


Figure 4. 17. Comparaison de temps de calcul

Interprétation

L'histogramme de la figure 4.17 montre une variation du temps de calcul, des différentes coordonnées. D'après l'étude du tableau 3.1 (coût et complexité des opérations) cité dans le chapitre 3 et du tableau 4.3 (Temps de calcul de l'addition et dédoublement pour les différentes coordonnées), on en déduit que les coordonnées « Lopez Dahab » sont plus efficaces, car ce type de coordonnées requière au moins une multiplication de moins par rapport aux autres coordonnées, d'où on va poursuivre notre application.

4.4.4 Etude de différentes méthodes de multiplication scalaire

Dans cette étape on étudie plusieurs méthodes de multiplication scalaire sur une courbe elliptique. Leur complexité est donnée en terme de nombre moyen d'addition de points (A) et de doublement de points (D).

On a vue dans le chapitre précédent, (par exemple dans le cas de l'échange de clé) que la principale opération lors d'un protocole cryptographique à base des courbes elliptiques est le calcul de la multiplication scalaire. Le but de cette étude est de faire une mise au point sur les différentes méthodes de multiplication en terme de temps de calcul et de complexité.

La première difficulté se présente pour $k > 2$. Il faut choisir la meilleure chaine d'additions. Plusieurs méthodes sont possibles :

- ✓ utiliser un des algorithmes de multiplication présentés dans le chapitre précédent ;

- ✓ tenter de trouver à la main les meilleures chaines ;
- ✓ tester plusieurs chaines et garder la meilleure.

La recherche d'une chaine d'addition optimale est difficile en raison du nombre de décompositions possibles, mais on peut néanmoins choisir les chaines les plus prometteuses. Donc pour calculer $k \times P$ il faut évaluer l'équation suivante:

$$Q = \underbrace{P + P + \ \dots\dots\dots\dots + P}_{k \text{ fois}}$$

Pour notre application on entame quatre cas, avec :

$k = 9,\ P = (6{,}11)$, $z = 1$ et $p = 23$.

- **1^{ier} cas : « Variant_1 »**

On implémente la chaine d'addition « Variant_1 » suivante, qui se base sur les coordonnées « Lopez Dahab », tel que le nombre de doublement $>$ nombre d'addition. $Q = 2P + 2P + 2P + 2P + P$. On obtient les résultats suivants :

```
p =

     6    11     1


ans =

Multiplication scalaire variant 1 en coordonnées Lopez Dahab


q =

     3    15     6

Elapsed time is 0.000833 seconds.
>>
```

Figure 4. 18. Résultat de multiplication scalaire « Variant_1 »

- **2eme cas : « variant_2 »**

On implémente la chaine d'addition « Variant_2 » suivante, qui se base sur les coordonnées « Lopez Dahab », tel que le nombre de doublement $<$ nombre d'addition. $Q = 2P + P + P + P + P + P + P + P$. On obtient les résultats suivants :

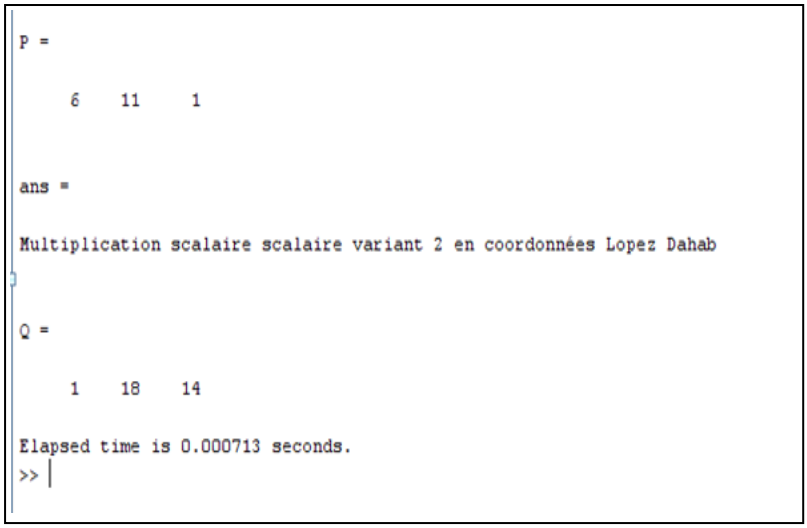


Figure 4. 19. Résultat de multiplication scalaire « Variant_2 »

- **3eme cas : « variant_3 »**

On implémente la chaine d'addition « Variant_3 » suivante, qui se base sur les coordonnées « Lopez Dahab », tel que le nombre de doublement = nombre d'addition. $Q = 2P + P + 2P + P + 2P + P$. On obtient les résultats suivants :

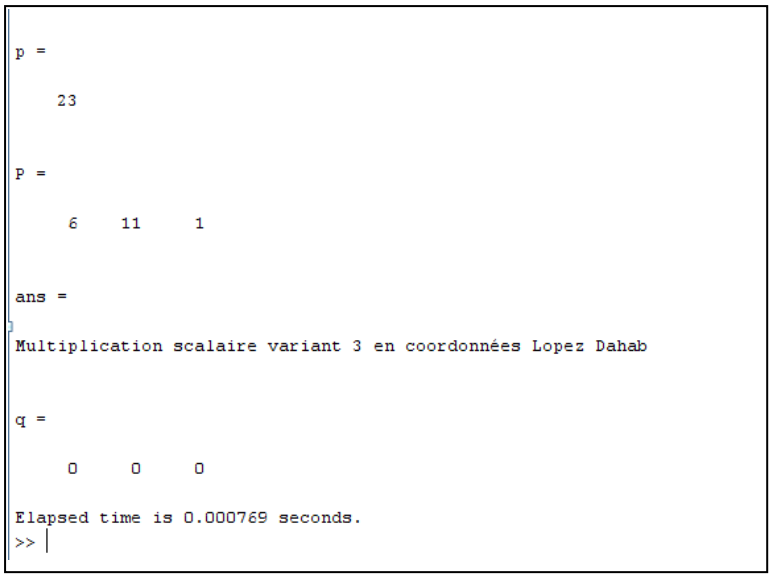


Figure 4. 20. Résultat de multiplication scalaire « Variant_3 »

- **4eme cas : « Double and Add »**

On implémente l'algorithme 10 (cité dans le chapitre 3) en coordonnées « Lopez Dahab ». On obtient les résultats suivants (figure 4.21) :

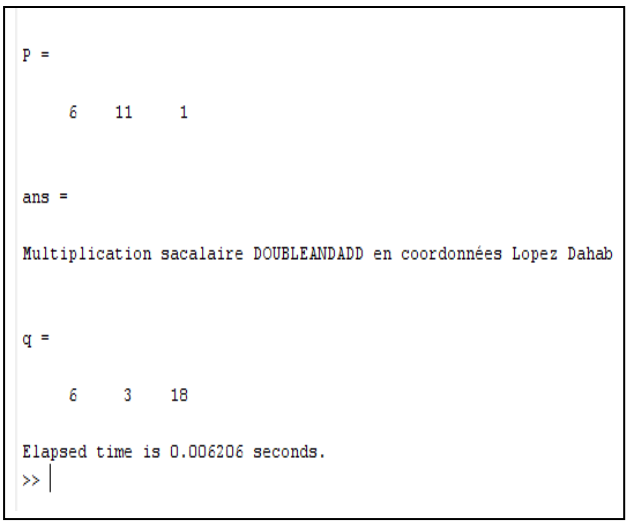


Figure 4. 21. Résultat de multiplication scalaire « Double and add »

Le tableau suivant regroupe le temps de calcul de chaque méthode.

Multiplication scalaire	Temps de calcul (s)
« Variant_1 »	0.000838
« Variant_2 »	0.000713
« Variant_3 »	0.000769
« Double and Add »	0,006206

Tableau 4. 3. Temps de calcul des différentes méthodes de multiplication

L'histogramme ci-dessous, illustre les performances de chaque méthode de multiplication scalaire en terme de temps de calcul, suivant le tableau précédent et l'étude théorique (la méthode NAF, Montgomery- chapitre 3).

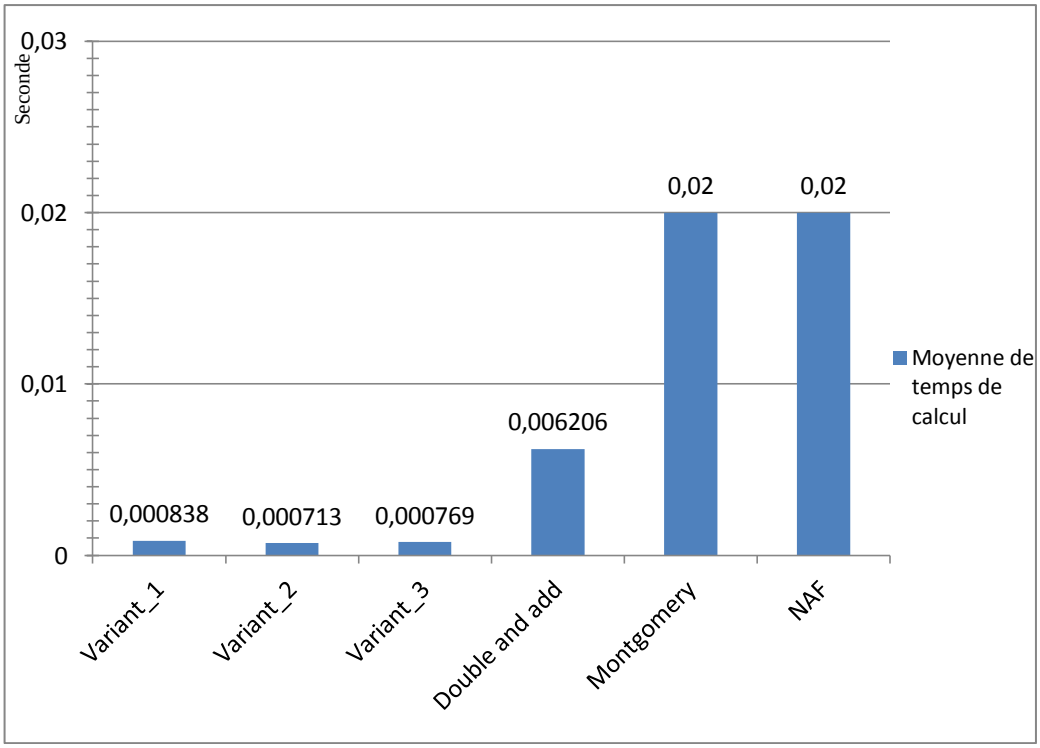


Figure 4. 22. Temps de calcul de multiplication scalaire

Interprétation

L'optimisation de la multiplication scalaire selon ces méthodes, permet d'obtenir de meilleurs coûts avec des formules simplifiées. Pour la suite de notre travail on s'appuie sur ces résultats, on prend en compte la combinaison entre le quatrième et le deuxième cas, car la méthode « Double and add » offre une simplicité de calcul. De plus, une grande résistance face aux attaques. La méthode « Variant_2 », diminue le temps de calcul.

4.5 Echange de clé

En général, lorsqu'on utilise le chiffrement, deux parties (Alice et Bob) communiquent sur un canal non sécurisé. Alice et Bob veulent s'assurer que leur communication reste incompréhensible pour toute personne qui pourrait écouter. De plus, comme Alice et Bob se trouvent dans des endroits distants, Alice doit être certaine que les informations qu'elle reçoit de Bob n'ont pas été modifiées par quiconque lors de la transmission. En outre, elle doit s'assurer que les informations proviennent bien de Bob et non pas d'une personne se faisant passer pour lui.

Pour réaliser l'échange de clé entre Alice et Bob on doit suivre le protocole suivant :

- ✓ Alice et Bob choisissent sur une courbe elliptique E un corps fini F_p sur laquelle le problème du logarithme discret est difficile à résoudre ;
- ✓ Alice et Bob se mettent d'accord sur le point P qui appartenant à la courbe elliptique qui n'est rien d'autre qu'une clé publique : $P(P_x, P_y)$ trouvé ci dessus, et puisque notre choix s'y porté sur les coordonnées de « Lopez Dahab », et cela à cause du temps d'exécution donc $P(P_x, P_y, 1)$;
- ✓ Alice choisit un entier k_a secrètement et se sera sa clé privée « secrète » ;
- ✓ Bob choisit un entier $k_b$secrètement, et se sera sa clé privée « secrète » ;
- ✓ Alice calcule $P_a = P \times k_a$ et l'envoie à Bob ;
- ✓ Et Bob calcule $P_b = P \times k_b$ et l'envoie à Alice.

Une fois que les deux acteurs du scénario ont calculés P_a et P_b , ils vont refaire les calculs suivants :

- ✓ Alice reçoit P_b et calcule $k_a \times P_b$
- ✓ Bob reçoit P_a et calcule $k_{b\times}P_a$

Alors, Alice et Bob partagent le secret commun.

Le principe de l'échange de clé est schématisé sur la figure suivante :

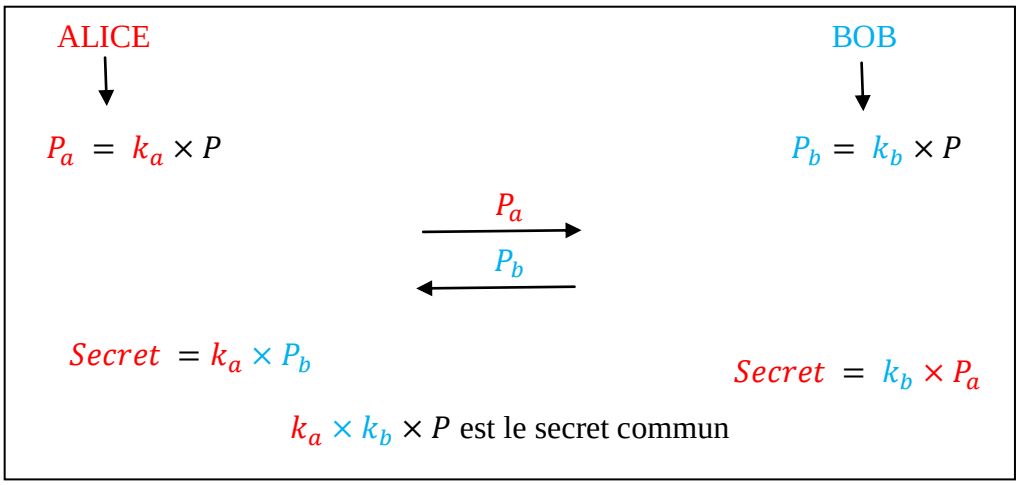


Figure 4. 23. Principe d'échange de clé

- **Pour $p = 23$**

Les paramètres sont définis comme suit :

- On prend un point $P(2,5)$ parmi les 27 solutions trouvées auparavant et le $z = 1$;
- La clé secrète d'Alice est l'entier $k_a = 9$;
- La clé secrète de Bob est l'entier $k_b = 5$.

Après l'implémentation d'organigramme 3 (voir annexe B) on obtient les résultats suivants :

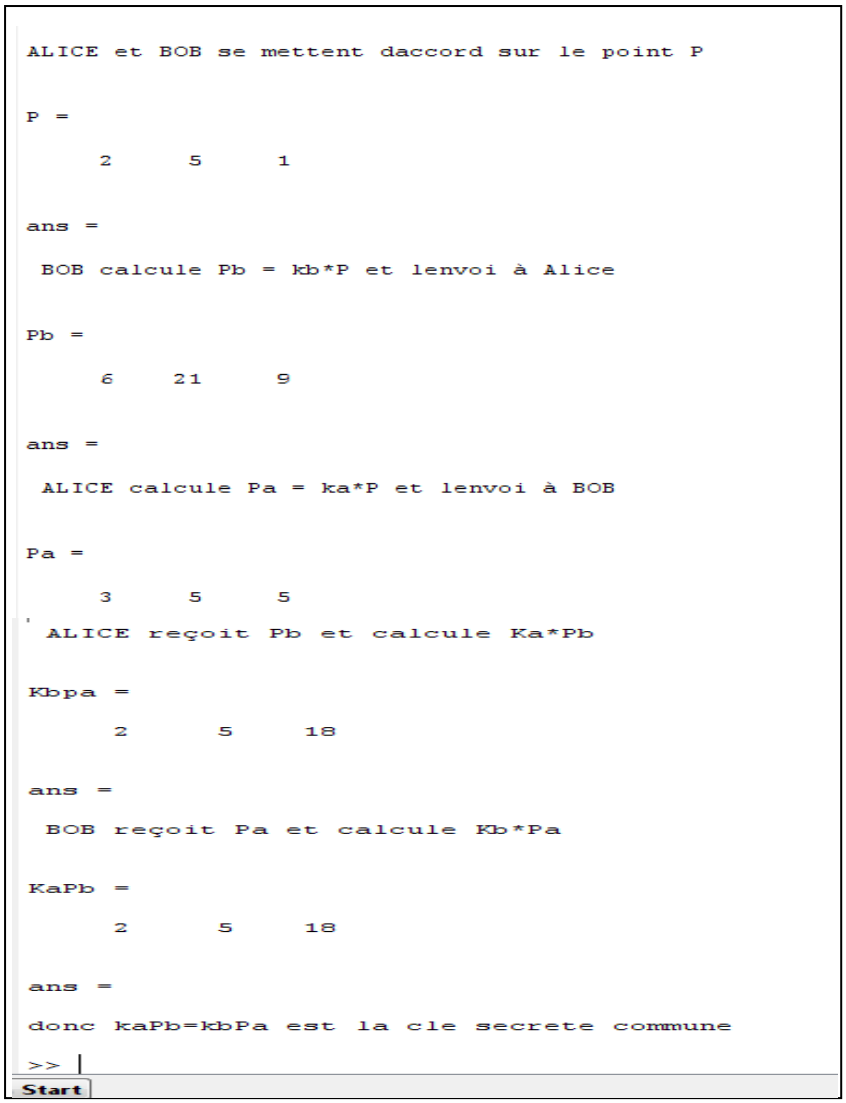


Figure 4. 24. Obtention de la clé secrète commune sur F_{23}

- **Pour $p = 71$**

Les paramètres sont définis comme suit :

- On prend un point $P(9,7)$ parmi les 66 solutions trouvés auparavant et le $z = 1$;
- La clé secrète d'Alice est l'entier $k_a = 9$;
- La clé secrète de Bob est l'entier $k_b = 5$.

Après l'implémentation d'organigramme 3 (annexe B), on obtient les résultats suivants :

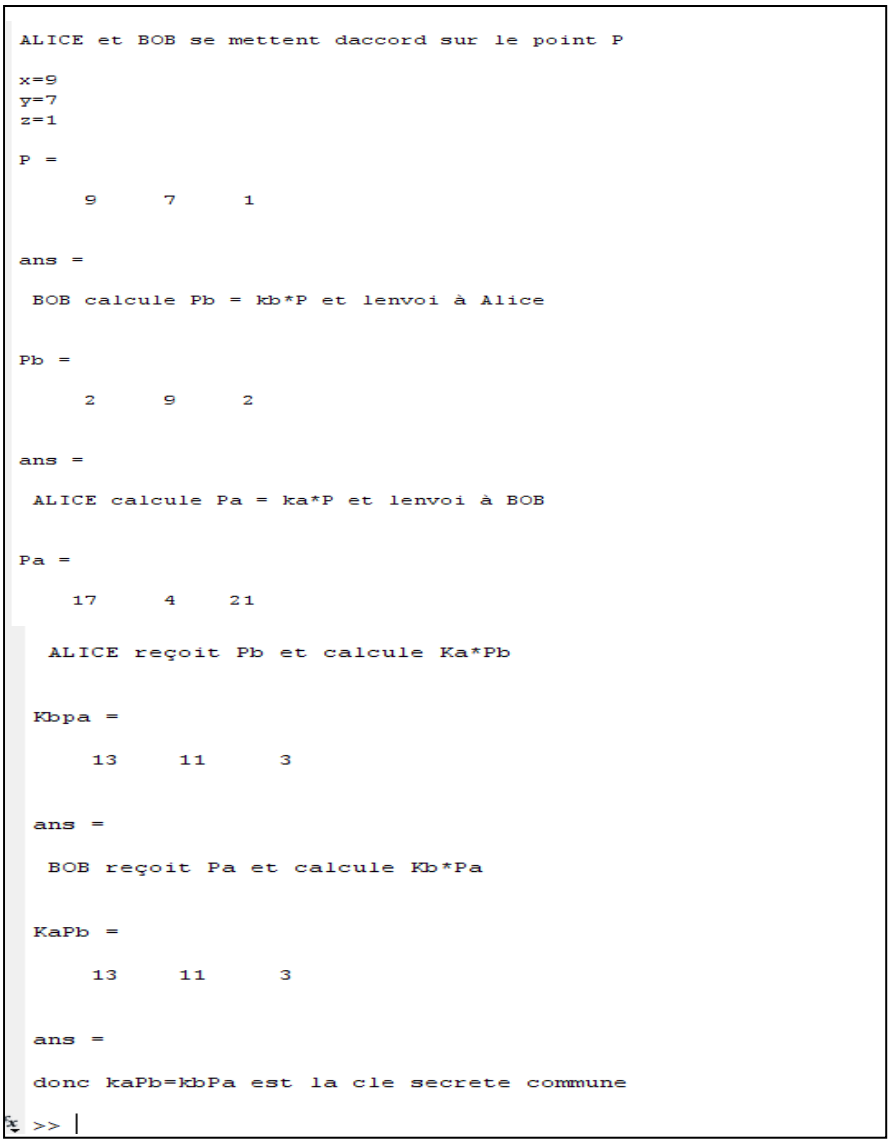


Figure 4. 25. Obtention de la clé secrète commune sur F_{71}

Interprétation

- $k_a \times k_b \times P$ sert à chiffrer le message ;
- k_a est la clé de déchiffrement d'Alice ;
- k_b est la clé de déchiffrement de Bob.

Malgré que P, P_a, P_b sont connus par le publique, la détermination des clés privées k_a, k_b est difficile à découvrir, ça revient à résoudre le problème du logarithme discret.

4.6 Chiffrement et déchiffrement « EL- Gamal »

La sécurité de ce système est basée sur le problème du logarithme discret. En effet, les quantités $k_b \times P$ et $k_a \times P$ peuvent être interceptées, mais il est très difficile de calculerk_a, k_b ou même $k_b \times k_a \times P$ (PDH).

Le principe de chiffrement « El-Gamal » est présenté sur la figure suivante :

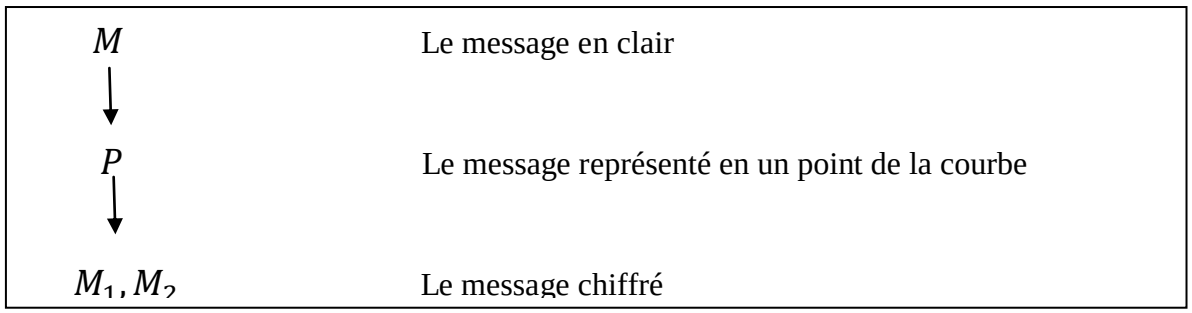


Figure 4. 26. Principe de chiffrement « EL Gamal »

- **1^{ier} cas : $p = 23$**

le message qu'on veut le chiffrer est : $MOT\ DE\ PASSE: 210586ZN$, après l'exécution de l'organigramme 4 (annexe B), on arrive aux résultats présentés dans le tableau ci-dessous. Pour la première ligne de tableau on obtient les résultats suivants :

```
Message =

     1     0     1


ans =

le message chiffre est représente par M1 et M2


M1 =

    14    21    11


M2 =

     9    12     3
```

Figure 4. 27. Résultat d'un chiffrement d'un message

Le même principe est appliqué pour les points restants, telle que les résultats sont mentionnés dans le tableau suivant :

Message	Points sur la courbe	Message chiffré		$k_a \times (k_b \times P)$
		$M_1 = k_a \times P$	$M_2 = M + k_a \times (k_b \times P)$	
M	(1,0,1)	(14,21,11)	(9,12,3)	(8,12,2)
O	(2,5,1)	(1,17,22)	(12,10,14)	(10,5,13)
T	(2,18,1)	(0,13,22)	(2,18,1)	(0,0,0)
ESPACE	(8,19,1)	(13,6,21)	(17,12,19)	(9,16,18)
D	(17,5,1)	(3,19,21)	(18,3,3)	$(1, 21, 2)$
E	(3,19,1)	(4,11,14)	(16,15,10)	(13,19,9)
ESPACE	(8,19,1)	(13,6,21)	(17,12,19)	(9,16,18)
P	(4,5,1)	(3,9,14)	(10,4,19)	(6,22,18)
A	(4,18,1)	(10,20,18)	(15,13,13)	(11,18,12)
S	(5,9,1)	(8,13,6)	(8,4,10)	(3,18,9)
S	(5,9,1)	(8,13,6)	(8,4,10)	(3,18,9)
E	(3,19,1)	(4,11,14)	(16,15,10)	(13,19,9)
:	(12,4,1)	(9,1,3)	(9,13,5)	(20,9,4)
2	(5,14,1)	(5,1,17)	(19,12,4)	(14,21,3)
1	(6,11,1)	(6,3,18)	(2,4,5)	(19,16,4)
0	(6,12,1)	(18,0,4)	(2,3,10)	(19,14,9)
5	(7,6,1)	(4,18,17)	(8,8, 1)	(1,2,0)
8	(7,17,1)	(22,13,4)	(12,21,19)	(5,4,18)
6	(8,4,1)	(21,22,21)	(3,22,17)	(18,18,16)
Z	(12,19,1)	(16,18,11)	(13,20,3)	(1,1,2)
N	(16,8,1)	(10,5,12)	(22,11,19)	(6,3,18)

Tableau 4. 4. Résultats de chiffrement « EL-Gamal » sur F_{23}

La question qui se pose ici est : Est ce qu'on peut chiffrer avec n'importe quel point ? La réponse est affichée dans la figure suivante :

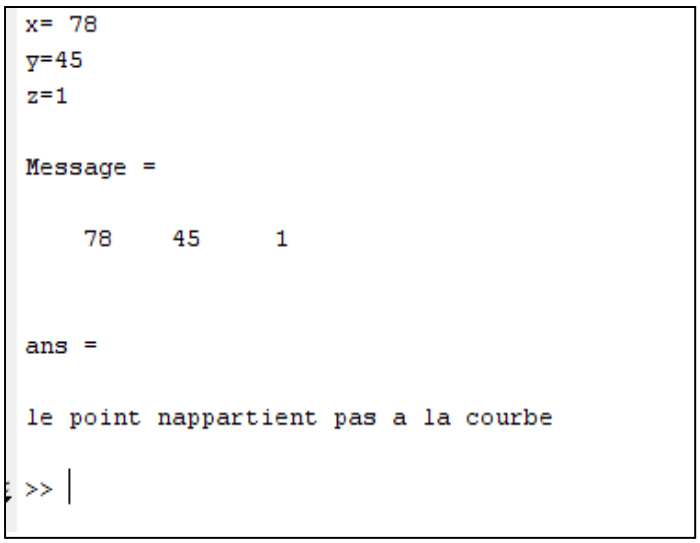


Figure 4. 28. Vérification d'un point

Pour le déchiffrement Bob doit calculer : $M = M_2 - K_b \times M_1$(organigramme 5, annexe B) .Pour la première lettre de tableau, on calcule :

$M = (1,0,1) = (9,12,3) - 5 \times (14,21,11) = (1,0,1) = M$, les résultats de l'exemple précédent sont affichés sur la figure suivante :

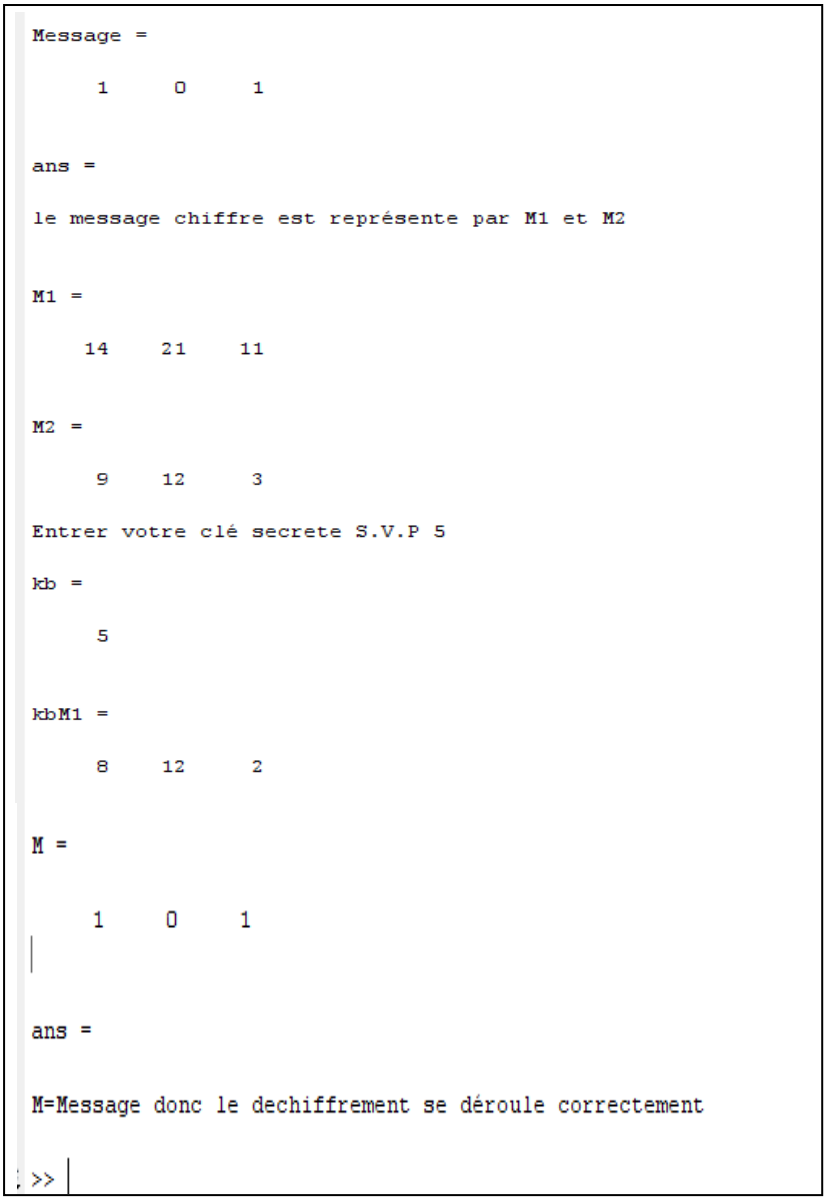


Figure 4. 29. Résultat de déchiffrement d'un message

Le même principe est appliqué pour les points restants, les résultats sont consignés dans le tableau suivant :

$M_1 = k_a \times p$	$M_2 = M + k_a \times (k_b \times P)$	$k_a \times (k_b \times P)$	$M = M_2 - k_b \times M_1$	Message
(14,21,11)	(9,12,3)	(8,12,2)	(1,0,1)	M
(1,17,22)	(12,10,14)	(10,5,13)	(2,5,1)	O
(0,13,22)	(2,18,1)	(0,0,0)	(2,18,1)	T
(13,6,21)	(17,12,19)	(9,16,18)	(8,19,1)	$ESPACE$
(3,19,21)	(18,3,3)	(1, 21, 2)	(17,5,1)	D
(4,11,14)	(16,15,10)	(13,19,9)	(3,19,1)	E
(13,6,21)	(17,12,19)	(9,16,18)	(8,19,1)	$ESPACE$
(3,9,14)	(10,4,19)	(6,22,18)	(4,5,1)	P
(10,20,18)	(15,13,13)	(11,18,12)	(4,18,1)	A
(8,13,6)	(8,4,10)	(3,18,9)	(5,9,1)	S
(8,13,6)	(8,4,10)	(3,18,9)	(5,9,1)	S
(4,11,14)	(16,15,10)	(13,19,9)	(3,19,1)	E
(9,1,3)	(9,13,5)	(20,9,4)	(12,4,1)	:
(5,1,17)	(19,12,4)	(14,21,3)	(5,14,1)	2
(6,3,18)	(2,4,5)	(19,16,4)	(6,11,1)	1
(18,0,4)	(2,3,10)	(19,14,9)	(6,12,1)	0
(4,18,17)	(8,8, 1)	(1,2,0)	(7,6,1)	5
(22,13,4)	(12,21,19)	(5,4,18)	(7,17,1)	8
(21,22,21)	(3,22,17)	(18,18,16)	(8,4,1)	6
(16,18,11)	(13,20,3)	(1,1,2)	(12,19,1)	Z
(10,5,12)	(22,11,19)	(6,3,18)	(16,8,1)	N

Tableau 4. 5. Résultats de déchiffrement « El-Gamal »

La question qui se pose ici : Est-ce que un espion peut déchiffrer le message ?

La réponse est affichée dans la figure suivante :

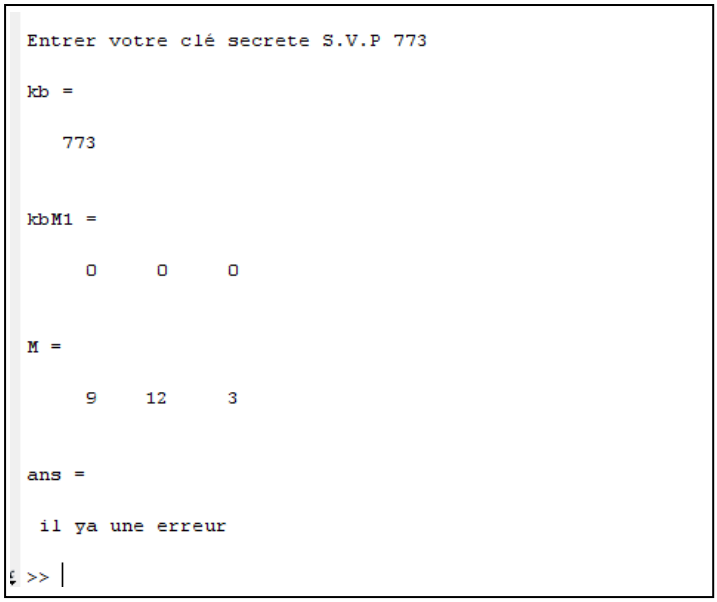


Figure 4. 30. L'intervention de l'espion

- **2eme cas : $p = 71$**

Le texte qu'on veut le chiffrer est :

Le Conseil des ministres s'est réuni, mercredi, sous la présidence de M. Abdelaziz Bouteflika, président de la République, voici le communiqué rendu suite à cette réunion :

« Le président de la République, Monsieur Abdelaziz Bouteflika, a présidé ce mercredi 12 safar 1434 H, correspondant au 26 décembre 2012, une réunion du Conseil des ministres.

Le Conseil des ministres a entamé ses travaux par l'examen et l'adoption d'un projet de loi fixant les règles applicables aux activités de la poste, des télécommunications et à celles liées aux technologies de l'information et de la communication.

Les nouvelles dispositions visent à consacrer la démocratisation de l'accès aux services de la poste, des télécommunications et des nouvelles technologies. Intervenant à ce propos, le Chef de l'Etat a appelé le Gouvernement à poursuivre les efforts déployés en vue d'arrimer notre pays à la nouvelle économie fondée sur l'utilisation accrue des technologies de l'information et de la communication. Cette dynamique devra s'articuler particulièrement sur la promotion de l'accès à l'internet à haut et à très haut débit au profit des citoyens et des entités économiques ainsi que le niveau de sécurité avec des méthodes supérieurs comme l'empreinte de l'œil».

Si on compte combien de lettre alphabétique et combien de chiffre plus les points de ponctuation on trouve :

- 10 lettres majuscule : L, C, M, A, B, R, H, I, E,G ;
- 28 lettres minuscule : a, b, c, d, e, f, j, h, i, g, k, l, m, n, o, p, q, r, s, t, u, v, x, y, z, à, é, è ;
- 6 chiffres : 0, 1, 2, 3, 4, 6 ;
- Les points de ponctuations : **« : » , ′ .**
- Espace

Donc le texte contient 10 lettres majuscule, 28 lettres minuscule, 6 chiffres, les ponctuations et l'espace qu'on va les chiffrés suite à l'exécution de l'organigramme 4. On arrive aux résultats du tableau ci-dessous.

Message	Les points sur la courbe	Message Chiffré		$k_a \times (k_b \times P)$
		$M_1 = k_a \times P$	$M_2 = M + k_a \times (k_b \times P)$	
L	(1,0,1)	(44,60,18)	(0,2,1)	(0,0,0)
M	(0,2,1)	(0,0,0)	(8,32,26)	(7,32,25)
A	(2,12,1)	(0,52,32)	(2,12,1)	(0,0,0)
B	(2,59,1)	(2,30,31)	(41,61,39)	(39,2,38)
R	(3,4,1)	(40,22,23)	(41,18,59)	(38,14,58)
H	(3,67,1)	(22,46,45)	(21,3,25)	(18,7,24)
C	(4,30,1)	(69,32,69)	(60,49,6)	(56,19,5)
I	(4,41,1)	(1,36,55)	(10,2,2)	(6,32,1)
E	(6,30,1)	(51,16,2)	(66,45,10)	(60,15,9)
G	(6,41,1)	(10,51,5)	(46,41,10)	(40,0,9)
a	(8,11,1)	(10,44,19)	(2,4,25)	(65,64,24)
b	(8,60,1)	(25,61,1)	(26,13,38)	(18,24,37)
c	(9,7,1)	(56,4,57)	(27,25,21)	(18,18,20)
d	(9,64,1)	(65,30,27)	(18,9,11)	(9,16,10)
e	(11,12,1)	(69,66,13)	(68,53,6)	(57,41,5)
f	(11,59,1)	(43,0,41)	(21,10,37)	(10,22,36)
j	(13,19,1)	(31,46,39)	(59,68,44)	(46,49,43)
h	(13,52,1)	(18,16,68)	(35,13,37)	(22,32,36)
i	(15,31,1)	(64,68,47)	(5,15,51)	(61,55,50)
g	(15,40,1)	(57,13,7)	(32,19,4)	(17,50,3)

k	(17,2,1)	(59,37,17)	(3,5,17)	(57,3,16)
l	(17,69,1)	(13,0,32)	(16,33,44)	(70,35,43)
m	(21,1,1)	(2,10,17)	(0,46,49)	(50,45,48)
n	(21,70,1)	(68,0,1)	(13,31,33)	(63,32,32)
o	(23,25,1)	(49,0,25)	(56,5,7)	(33,51,6)
p	(24,54,1)	(61,0,44)	(53,8,49)	(29,25,48)
q	(27,13,1)	(7,66,26)	(7,3,38)	(51,61,37)
r	(27,58,1)	(2,21,35)	(36,41,38)	(9,54,37)
s	(28,27,1)	(22,0,42)	(34,49,2)	(6,22,1)
t	(28,44,1)	(52,5,24)	(21,30,61)	(64,57,60)
u	(60,52,1)	(10,2,70)	(58,44,9)	(69,63,8)
v	(29,45,1)	(35,52,9)	(67,58,37)	(38,13,36)
x	(3,04,1)	(58,44,65)	(32,61,19)	(2,57,18)
y	(70,47,1)	(15,51,46)	(14,45,33)	(15,69,32)
z	(30,67,1)	(55,17,46)	(31,33,7)	(1,37,6)
é	(3,84,1)	(64,62,1)	(26,43,9)	(59,39,8)
è	(38,67,1)	(1,0,3)	(65,15,55)	(27,19,54)
à	(43,29,1)	(36,0,32)	(2,24,6)	(30,66,5)
0	(43,42,1)	(1,0,46)	(27,18,11)	(55,47,10)
1	(45,33,1)	(38,0,31)	(44,39,39)	(70,6,38)
2	(45,38,1)	(24,0,28)	(35,51,5)	(61,13,4)
3	(47,28,1)	(56,44,11)	(70,24,2)	(23,67,1)
4	(47,43,1)	(68,0,20)	(38,13,46)	(62,41,45)
6	(49,20,1)	(3,0,6)	(25,51,9)	(47,31,8)
.	(49,51,1)	(23,18,55)	(52,52,26)	(3,1,25)
:	(5,42,1)	(3,23,59)	(64,31,38)	(10,29,37)
,	(54,69,1)	(39,0,4)	(27,24,26)	(44,26,25)
′	(58,12,1)	(8,44,25)	(11,37,5)	(24,25,4)
«	(58,59,1)	(53,0,54)	(1,7,2)	(14,19,1)
»	(5,918,1)	(43,0,39)	(6,10,38)	(18,63,37)
$ESPACE$	(59,53,1)	(59,0,42)	(2,41,39)	(14,59,38)

Tableau 4. 6. Résultats de chiffrement sur F_{71}

Afin de déchiffrer Bob doit calculer : $M = M_2 - k_b \times M_1$. Pour la première lettre de tableau, on calcule :

$$M = (1,0,1) = ((0,2,1)) - 5 \times (44,60,18) = (1,0,1) = M$$

Le même principe est appliqué dans le tableau suivant :

$M_1 = k_a \times P$	$M_2 = M + k_a \times (k_b \times P)$	$k_a \times (k_b \times P)$	$M = M_2 - k_b \times M_1$	Message
(44,60,18)	(0,2,1)	(0,0,0)	(1,0,1)	L
(0,0,0)	(8,32,26)	(7,32,25)	(0,2,1)	M
(0,52,32)	(2,12,1)	(0,0,0)	(2,12,1)	A
(2,30,31)	(41,61,39)	(39,2,38)	(2,59,1)	B
(40,22,23)	(41,18,59)	(38,14,58)	(3,4,1)	R
(22,46,45)	(21,3,25)	(18,7,24)	(3,67,1)	H
(69,32,69)	(60,49,6)	(56,19,5)	(4,30,1)	C
(1,36,55)	(10,2,2)	(6,32,1)	(4,41,1)	I
(51,16,2)	(66,45,10)	(60,15,9)	(6,30,1)	E
(10,51,5)	(46,41,10)	(40,0,9)	(6,41,1)	G
(10,44,19)	(2,4,25)	(65,64,24)	(8,11,1)	a
(25,61,1)	(26,13,38)	(18,24,37)	(8,60,1)	b
(56,4,57)	(27,25,21)	(18,18,20)	(9,7,1)	c
(65,30,27)	(18,9,11)	(9,16,10)	(9,64,1)	d
(69,66,13)	(68,53,6)	(57,41,5)	(11,12,1)	e
(43,0,41)	(21,10,37)	(10,22,36)	(11,59,1)	f
(31,46,39)	(59,68,44)	(46,49,43)	(13,19,1)	j
(18,16,68)	(35,13,37)	(22,32,36)	(13,52,1)	h
(64,68,47)	(5,15,51)	(61,55,50)	(15,31,1)	i
(57,13,7)	(32,19,4)	(17,50,3)	(15,40,1)	g
(59,37,17)	(3,5,17)	(57,3,16)	(17,2,1)	k
(13,0,32)	(16,33,44)	(70,35,43)	(17,69,1)	l
(2,10,17)	(0,46,49)	(50,45,48)	(21,1,1)	m
(68,0,1)	(13,31,33)	(63,32,32)	(21,70,1)	n
(49,0,25)	(56,5,7)	(33,51,6)	(23,25,1)	o
(61,0,44)	(53,8,49)	(29,25,48)	(24,54,1)	p
(7,66,26)	(7,3,38)	(51,61,37)	(27,13,1)	q

(2,21,35)	(36,41,38)	(9,54,37)	(27,58,1)	r
(22,0,42)	(34,49,2)	(6,22,1)	(28,27,1)	s
(52,5,24)	(21,30,61)	(64,57,60)	(28,44,1)	t
(10,2,70)	(58,44,9)	(69,63,8)	(60,52,1)	u
(35,52,9)	(67,58,37)	(38,13,36)	(29,45,1)	v
(58,44,65)	(32,61,19)	(2,57,18)	(3,04,1)	x
(15,51,46)	(14,45,33)	(15,69,32)	(70,47,1)	y
(55,17,46)	(31,33,7)	(1,37,6)	(30,67,1)	z
(64,62,1)	(26,43,9)	(59,39,8)	(3,84,1)	é
(1,0,3)	(65,15,55)	(27,19,54)	(38,67,1)	è
(36,0,32)	(2,24,6)	(30,66,5)	(43,29,1)	à
(1,0,46)	(27,18,11)	(55,47,10)	(43,42,1)	0
(38,0,31)	(44,39,39)	(70,6,38)	(45,33,1)	1
(24,0,28)	(35,51,5)	(61,13,4)	(45,38,1)	2
(56,44,11)	(70,24,2)	(23,67,1)	(47,28,1)	3
(68,0,20)	(38,13,46)	(62,41,45)	(47,43,1)	4
(3,0,6)	(25,51,9)	(47,31,8)	(49,20,1)	6
(23,18,55)	(52,52,26)	(3,1,25)	(49,51,1)	.
(3,23,59)	(64,31,38)	(10,29,37)	(5,42,1)	:
(39,0,4)	(27,24,26)	(44,26,25)	(54,69,1)	,
(8,44,25)	(11,37,5)	(24,25,4)	(58,12,1)	′
(53,0,54)	(1,7,2)	(14,19,1)	(58,59,1)	«
(43,0,39)	(6,10,38)	(18,63,37)	(5,918,1)	»
(59,0,42)	(2,41,39)	(14,59,38)	(59,53,1)	$ESPACE$

Tableau 4. 7. Résultats de déchiffrement sur F_{71}

4.7 Conclusion

Dans ce chapitre, on a entamé le problème de l'implantation d'échange de clé et le chiffrement sur les courbes elliptiques définies sur des corps premiers. On a abordé ce problème aussi bien au niveau des algorithmes de multiplication scalaire. L'inconvénient est qu'il est très difficile de trouver des chaînes efficaces, c'est-à-dire courtes, dans un temps raisonnable. Affin de contourner ce problème, on a proposé d'étudier une classe de chaînes d'additions variée. L'implémentation d'un ECC en utilisant les coordonnées « Lopez Dahab » présente une amélioration par rapport à l'utilisation des autres coordonnées. La cryptographie proposée par courbes elliptiques est aussi dite cryptographie « puissante ». Il faudra beaucoup de temps pour casser un seul e-mail. La sécurité proposée reste donc très confortable.

Conclusion générale

Le modèle cloud computing propose à moindre coût plus de choix, de flexibilité et d'efficacité opérationnelle aux entreprises, aux institutions gouvernementales et aux particuliers. Pour tirer pleinement parti de tous ces avantages, des garanties fiables doivent être apportées en matière de confidentialité et de sécurité des données en ligne. La cryptographie est en évolution continue afin de pouvoir répondre aux besoins de sécurisation. En effet, les cryptosystèmes se doivent d'être performants face à des attaques de plus en plus nombreuses. Les algorithmes asymétriques sur les courbes elliptiques présentent de nombreux avantages par rapport à la cryptographie habituelle, vu que le cryptosystèmes basé sur les courbes elliptiques permet d'obtenir un niveau de sécurité élevé pour une taille de clé moindre, ceci les rend très attractifs pour les applications qui nécessitent des ressources très limitées (mémoire, puissance, bande passante...) telles que la téléphonie mobile ou communication satellitaire etc...

L'ensemble des informations rassemblées et analysées au travers notre étude sont présentés dans ce qui suit :

Au chapitre 1, à partir de l'étude portée montre que le cloud est un modèle pratique, il permet un accès via le réseau à une multitude de services à la demande telle que la disponibilité, une préservation du contexte lorsque on change de terminal et le stockage en ligne qui offre un gain économique. Malgré tout ses avantages, il présente des failles de sécurité.

Au chapitre 2, on a examiné les différents cryptosystèmes traditionnels face au système de cryptage à base de courbes elliptiques afin d'en tirer la meilleur méthode en terme de performances au niveau de la sécurité et l'efficacité.

Au chapitre 3, on a étudié les diverses représentations des coordonnées et les différentes méthodes de multiplication scalaire, coût et complexité et on a entamé la méthode « El-Gamal » à base de courbes elliptiques.

Au chapitre 4, on a montré que même si les cryptosystèmes basés sur les courbes elliptiques présentent un haut niveau de sécurité, pour une longueur de clé minime, une

bonne optimisation des algorithmes les rend encore plus performants. Cependant, on a constaté que la combinaison de la méthode du produit scalaire « Double and Add » et « variant_2 » offre une meilleur efficacité en terme de coût et de complexité grâce à la difficulté du problème de logarithme discret. Le chiffrement « El-Gamal » qui repose sur le principe d'échange de clé de « Diffie Hellman » nous a permet de réaliser un cryptage jugé efficace.

D'après ce travail, on peut envisager que l'intérêt particulier que la cryptographie par les courbes elliptiques s'explique essentiellement par leur niveau de sécurité très élevé, contrairement aux autres systèmes existants, aucune attaque à temps sous exponentiel n'est connue à ce jour contre les ECC, sauf en des cas particuliers rares et bien identifiés.

Annexe A

Rappel des notions mathématiques

Définition1 : Groupe

- Pour tous éléments Q, P et R de E, l'égalité ;
  $(Q \times P) \times R = Q \times (P \times R)$ est vraie → associative
- $P + (-P) = O \epsilon E$ L'élément symétrique de la courbe E ;
- $P + Q = Q + P \rightarrow$ commutative ;
- P lui-même l'élément neutre.

Définition 2 : Anneau

Soit E un ensemble muni de deux lois de composition internes,

Notées $+$ et $\times$, $(E; +; \times)$ est appelé anneau si :

- $(E; +)$ est un groupe commutatif ;
- $\times$ est distributive sur la loi $+$ et est associative ;
- E admet un élément neutre pour $\times$.

Si la loi est commutative, alors $(E; +; \times)$ est un anneau commutatif.

Définition 3 : corps fini

Un ensemble F muni de deux lois de composition internes est appelé corps si :

- $(F; +; \times)$ est un anneau ;
- L'élément neutre de la loi $+$ est différent de l' élément neutre de la loi $\times$;
- Tout élément non nul de F admet un symétrique pour $\times$.

Un corps est dit fini si l'ensemble F est fini.

Définition 4 : Extension de corps

Soit F un corps, L est une extension du corps F si L est un corps et F est inclus dans L.

On note F_q les extensions du corps F_p ou $q = p\hat{}\alpha$ avec $\alpha \epsilon N^*$ et p premier.

On considère deux cas : les corps F_p ou $p \geq 3$ et les extensions de corps binaire $F\ 2^m, m \epsilon N$. Pour un corps quelconque, on utilise la notation F. Enfin, si on considère un corps fini et ses extensions, on écrira F_q.

Définition 5 : Modulo

On désigne par modulo l'opération de calcul du reste de la division euclidienne. On écrira a mod n pour représenter le reste de la division de a par n. Un modulo équivaut donc à la différence entre "a" et la multiplication de la valeur tronquée du quotient de "a" par "n". C'est à dire : $a \, mod \, n = a - [a/n] \times n$.

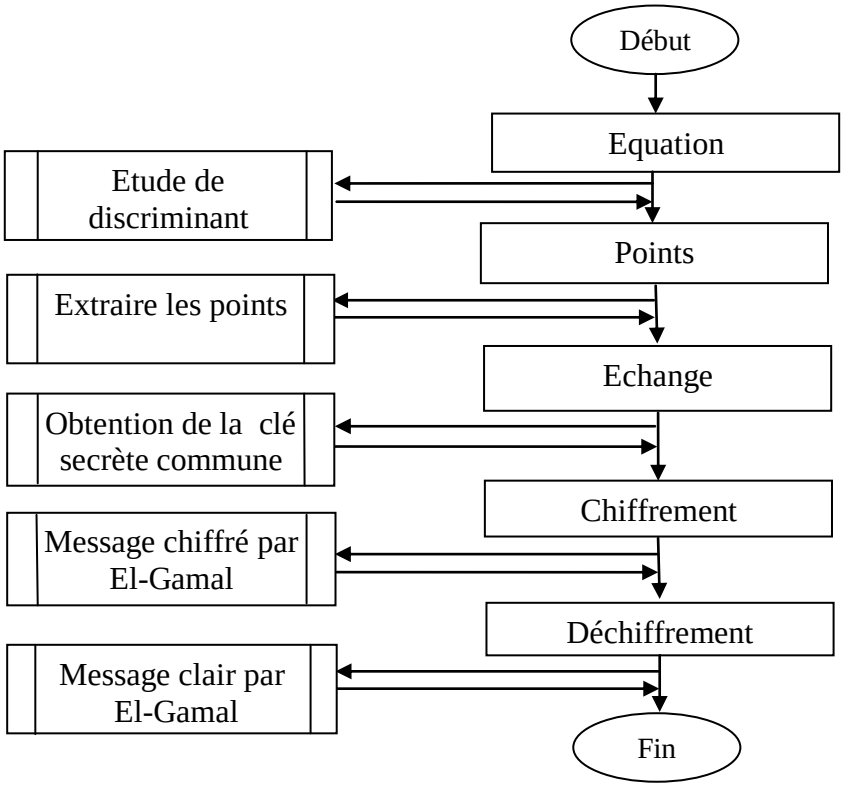
Définition 6 : Cardinal

La cardinalité est une notion de taille pour les ensembles. Lorsqu'un ensemble est fini, c'est-à-dire si ses éléments peuvent être listés par une suite finie, son cardinal est la longueur de cette suite.

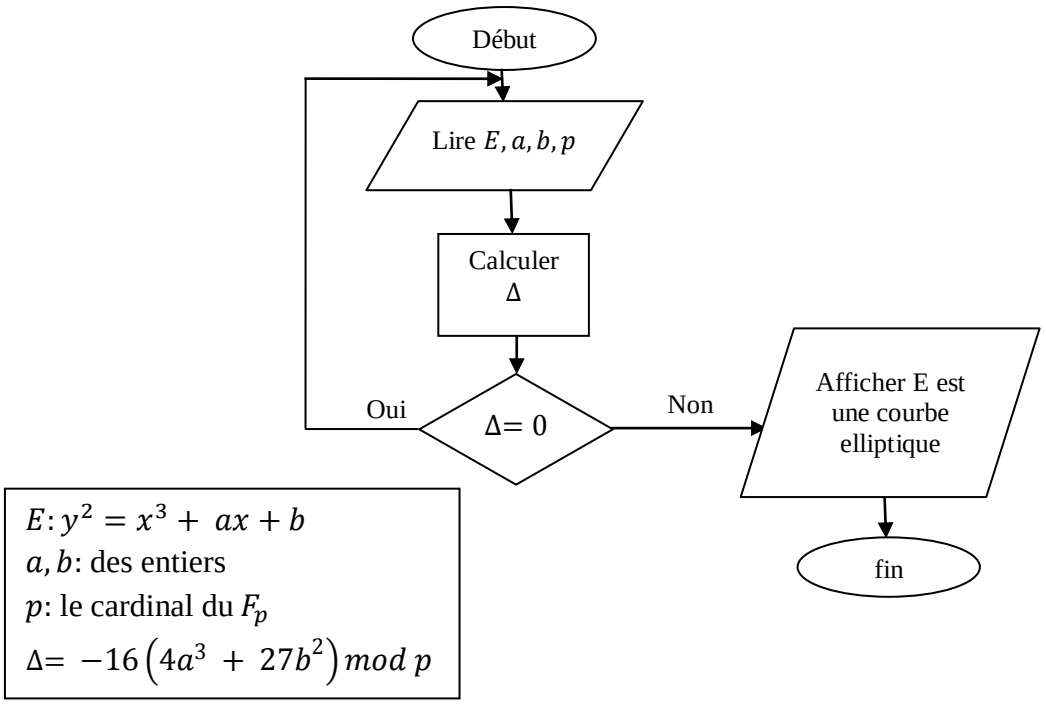
Annexe B

Les organigrammes implémentés

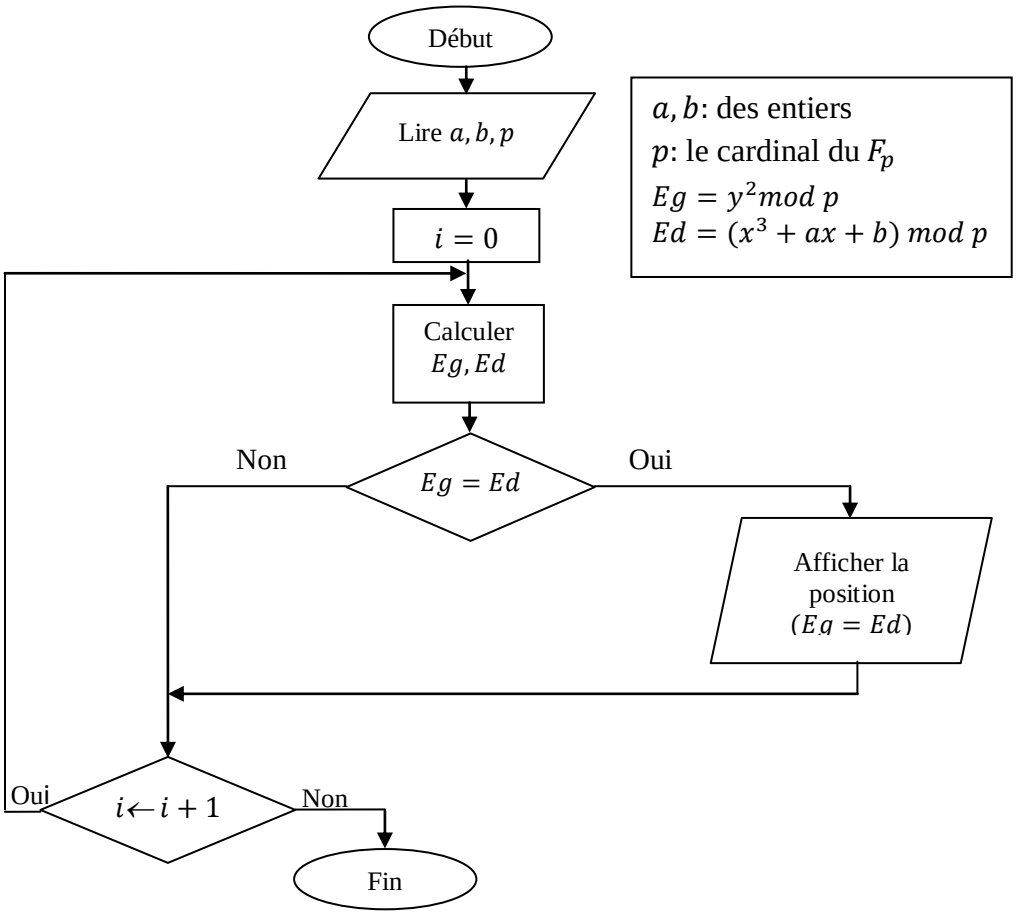
Organigramme principal de cryptographie à base de courbe elliptique



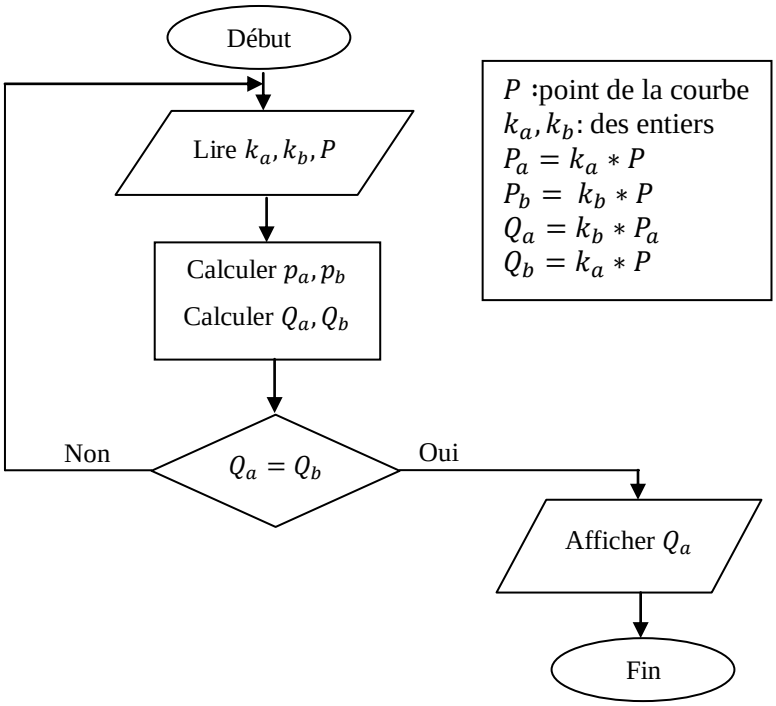
Organigramme 1 Etude de discriminant



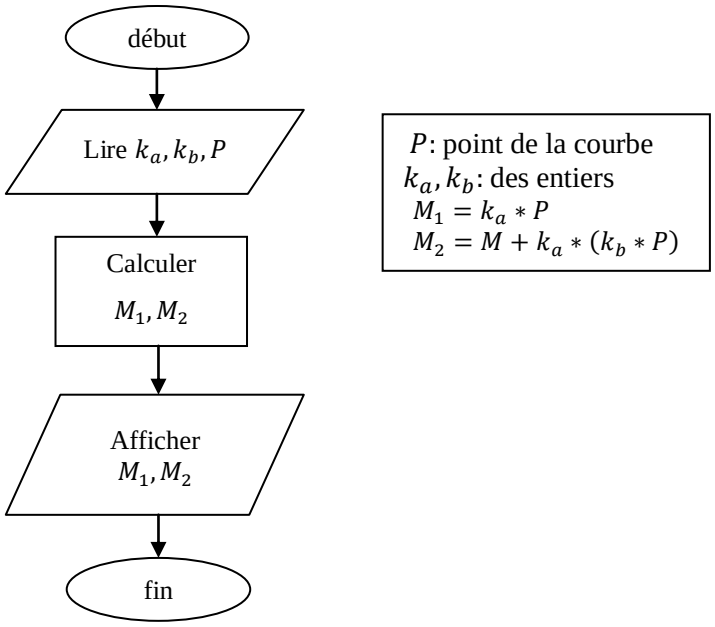
Organigramme 2 Extraire des points



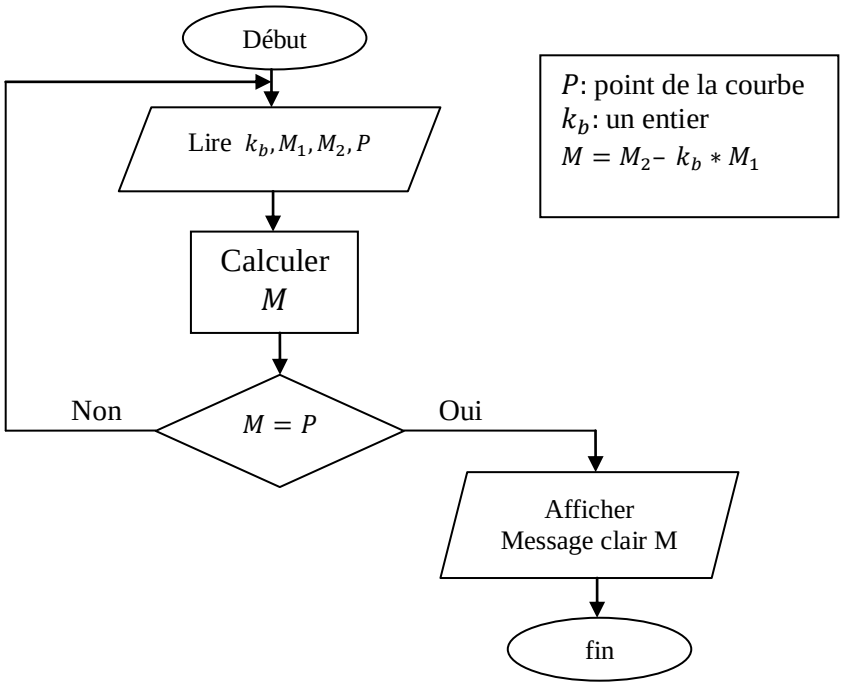
Organigramme 3 Obtention de la clé secrète commune



Organigramme 4 Message chiffré par « El-Gamal »



Organigramme 5 : Message clair par « El-Gamal »



Bibliographie

[1] Phillipe Hedde, « sécurité du cloud computing », Livre blanc, Syntec numérique, 2012.

[2] Allan Lefort, « Administration des systèmes réseaux et applications à base de logiciel libre », thèse de master, Université de Nancy, 2012.

[3] Mavridis Ioannis, "Towards new acces control models for cloud computing systems", university of Macedonia, departement of Applied Informatics, Greece.

[4] Eric Berthelot, « Le Cloud Computing, Quel impact organisationnel pour les équipes informatiques des systèmes d'information », Thèse de master, Management des Systèmes d'information et de Communication, Université du Québec à Montréal, Canada, Année universitaire 2010 – 2011.

[5] Goolmann.D, "Computer security", Interdisciplinary Reviews, 2010.

[6] Peter Sempolinski, Douglas Thain, "A comparison and critique of open nebula and eucalyptus", Proceeding of the 2010 IEEE second international conferance on cloud computing ,technology and science Washington, USA, 2010.

[7] Stefan Husemann, « Les enjeux du cloud computing en entreprise – Intégration dans le cloud », Thèse de master, Université de Fribourg-département d'informatique, Suisse, 2010.

[8] Point de vue de Microsoft, « La sécurité du cloud computing », janvier 2010.

[9] Meriam Mehdjoub, « Etude et expérimentation du cloud computing pour le monitoring des applications orientées services », Thèse de master, Ecole nationale d'ingénieurs de Sfax, Tunisie, 2011.

[10] Christian Baun, Marcel Kunze, Jens Nimis, Stefan Tai, "Cloud computing-web-Based dynamic IT services", Karlsruhe institue of technology (KIT), Germany,2011.

[11] Daniel Catteddu, Giles Hogben, "Risks and recommandations for information security", Article ENISA – European Network and Information Security Agency.

[12] ISO/IEC Information technology, "Security méthodes – Information security risks management", Annex E : Information security assessment approches, 2008.

[13] Nicolai James, "Data centers turn to out sourcing to meet capacity needs", Article Co.com, 10 mai 2011.

[14] Jew Jonathan, "BICSI Datacenter standard, Ressource for today's datacenter operators and designer", New maguasine, juin 2010.

[15] Nicolas Roberge, « les avantages du cloud computing », Article evoila.com, 2010.

[16] Jonathan Faure, Jean François Knoepfli, Mthieu Rivoalen, « Cloud computing-comment avoir la tête dans les nuages », Mémoire de licence, Ecole supérieure de génie informatique, Paris.

[17] Thomas Izard, « Optimisation de la multiplication pour de petits scalaires », Thèse de master, Laboratoire d'informatique de robotique et de micro-électronique, Académie de Montpellier-Sciences et techniques du Languedoc, France, 2008.

[18] M. Mouchini Toufik, « Implémentation d'un processeur basé sur les courbes elliptiques convenable pour les étiquettes RFID », Thèse de magister, Ecole militaire polytechniques Alger, Algérie, 2013.

[19] Nabil Ghanmi, « Etude et implémentation matériel de signature numérique à base des courbes elliptiques (ECDSA) », Thèse de master, Laboratoire d'électronique et des technologies de l'information- Ecole national des ingénieurs de Sfax, Tunisie, septembre 2011.

[20] Amandine Jambert, « Outils cryptographiques pour la protection des contenus et de la vie privée des utilisateurs », Thèse de doctorat de l'université Bordeaux1, France, mars 2011.

[21] Robert Rollan, « Emergence de la cryptographie elliptique », Institut de mathématiques de Luminy- Marseille, France, novembre 2007.

[22] Hagler Michael, « Courbes elliptiquesvet cryptographie », Article, février 2006.

[23] Stéphane Ballet, Alexis Bonecaze, « Courbes elliptiques-Application à la cryptographie », Cours de Cryptographie Avancée, Ecole d'ingénieur de Luminy, Marseille, France, 2011-2012.

[24] Julien Franq, « Conception et sécurisation d'unités arithmétiques hautes performances pour courbe elliptique », Thèse de doctorat d'informatique, Ecole national des mines-Montpelier, France, décembre 2009.

[25] Naveed shoaib, “A portable and improved implementation of the Diffie Hellman protocol for wireless sensor networks”, Master of Science in the Mathematics Program, Youngstown state university, United States, Aout 2009

[26] Sylvain Duquesne, « Multiplication scalaire de Montgomery pour les courbes de genre 2 », université de Montpelier 2, Institue de mathématiques et de modélisation, France, 20 mars 2008.

[27] A.Chillali, « Exemple de courbe elliptique et cryptographie », Faculté des sciences et techniques, Fès, Maroc, 2012.

[28] Vincent Verneuil, « Courbes elliptique et attaques par canaux auxiliaires »,Article de ESIEA, Aout 2009.

[29] Lynch, Stephen, « des systèmes dynamiques avec des applications à l'aide de MATLAB », 2004.