République Algérienne Démocratique et Populaire
Ministère de L'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master Recherche

Option : Réseaux et Systèmes Distribués

Thème

L'authentification à base d'empreinte digitale dans les réseaux à faibles ressources

Réalisé par :

Mlle AIT ABDELMALEK Wassila
Mlle MANSOURI Abla

Devant le jury composé de :

Président :	M.	ABBACHE Bournane
Examinatrice :	Mme	ALOUI Soraya
Examinatrice :	Mme	YESSAD Nawel
Encadreur :	M.	OMAR Mawloud
Co-Encadreur :	M.	MOHAMMEDI Mohamed

Promotion 2014/2015

Remerciements

Louange à **Allah** le tout-puissant, le Miséricordieux. Louange à **Allah** qui nous a aidé à voir l'aboutissement de cette thèse.

À vous, docteur **OMAR Mawloud**.
Maître de Conférences A
Chef de Département d'Informatique
Chef de l'équipe " Réseaux pour les Applications Médicales "
Laboratoire d'Informatique Médicale - LIMED
Pour nous avoir fait l'honneur d'accepter de diriger cette thèse.
Pour l'intérêt que vous avez bien voulu porter à ce travail.
Pour vos précieux conseils et votre disponibilité.
Veuillez trouver ici l'expression de notre sincère reconnaissance et les plus profonds respects.

À Monsieur **MOHAMMEDI Mohammed**.
Doctorant au Laboratoire d'Informatique Médicale - LIMED de Bejaia
Vous nous avez fait l'honneur de diriger ce travail en faisant toujours preuve de gentillesse, de disponibilité et de patience. On a eu la chance d'être formé à vos côtés.
Soyez sûre de notre respect le plus sincère et de toutes nos reconnaissances.

Au président de jury, ***M*** **ABBACHE bournnane**.
Pour l'honneur que vous nous faites en acceptant d'être membre du jury. Avec toute notre estime et tous nos profonds respects.

Au membre de jury, M^{me} **ALLOUI Soraya**.
Pour l'honneur que vous nous faites par votre présence dans ce jury.
Pour vos chaleureux encouragements.
Recevez nos très sincères remerciements.

Au membre de jury, M^{lle} **YESSAD Nawel**.
Pour l'honneur que vous nous faites, d'avoir accepté d'être notre examinatrice pour nous faire apprendre de votre critique et remarques.
Recevez nos très sincères remerciements.

À tout le personnel de l'université de Abderrahmane Mira " Targa ouzemour " de Bejaia, tous les enseignants du département d'informatique qu'ont côtoyé pendant notre formation qui par leur apprentissage, leurs conseils et leur expérience, nous ont permis d'en arriver là.

On tient aussi à exprimer notre gratitude particulière à Mr **OUZEGGANE Radouane** et Mme **TAMAZOUZTE Kahina** qui nous ont comblé de leur soutien.
À tous ceux qui de près ou de loin ont contribué au bon déroulement de cette étude.

Abla et Wassila

Dédicace

JE DEDIE CE MODESTE TRAVAIL A :

Mon exemple éternel, mon soutien moral et source de joie et de bonheur, celle qui s'est toujours sacrifié pour me voir réussir, que dieu te protège
À **Maman** que j'adore.

À la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ; À toi **mon père**.

À mes deux yeux, mes deux frères, **Mohammed el Amine** et **Abderrahim** pour leurs conseils, leur aide morale et leur simple présence à mes côtés.

À ma grande sœur **Zineb** qui n'a jamais cesser de m'aider de toutes manières, à ma petite sœur **Noor el yakine** à qui je souhaite toute la réussite et le bonheur, à mes deux charmantes princesses, mes deux nièces, **Ines** et **riheb**.

Je n'oublie jamais de dédier ce travail aux personnes qui m'ont toujours aidé dans mes choix professionnels et encouragé dans ma carrière d'étude, à **Billel**, **Hakim**, **Aicha** et **Nadjet**, pour leur aide et leurs conseils. A ma chère **Lalla** qui ne m'a jamais oublié avec ses prières à tous mes oncles et tantes, cousins et cousines et à mes deux familles **Mansouri** et **Terrai**.

À mes chers camarades et amies **Houda** et **Mouna** : merci pour tous les moments heureux et difficiles partagés, vous avez été mes sœurs de cœur durant toutes ces années.
À mes collègues d'étude et aimables amis.

J'accorde une place à part dans mes dédicaces à mon binôme **Wassila**, qui par son dynamisme et sa bonne humeur a su égayer la gestion des " aléas " inhérents aux projets de recherche.

Abla

Dédicace

JE DEDIE CE MODESTE TRAVAIL A :

À la plus belle créature que Dieu a créée sur terre, à cette source de tendresse, de patience et de générosité qui m'ont comblé de leur soutien et m'ont vouée un amour inconditionnel. Vous êtes pour moi un exemple de courage et de sacrifice continu. Je vous aime **MAMAN** et **PAPA**.

À mes très chères deux petites sœurs : **Karima** et **Tinhinane** pour leurs compréhensions, leurs soutiens et leurs tendresses....
À mon unique frère : **Aimad** pour son soutien moral.
À mes tantes Sabiha et Farida.
Je n'oublie jamais mes meilleurs amis : **Samira**, **Malika**, **Wissam**, **Mina**, **Ali** et **Boualem**.
À toute la famille **Ait Abdelmalek** et **Kara** ; cousins et cousines, oncles et tantes.

J'accorde une place à part dans ces remerciements à ma binôme **Abla**, qui par son dynamisme et sa bonne humeur a su égayer la gestion des " aléas "inhérents aux projets de recherche.
À tous ceux qui ont su m'apporter aide et soutien aux moments propices, je dédie ce modeste travail.
À toute la promotion d'Informatique Recherche 2014/2015.

Wassila

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

API	**A**pplication **P**rogramming **I**nterface
BANet	**B**ody **A**rea **N**etwork
EC	**E**lliptic **C**urve
ECC	**E**lliptic **C**urve **C**ryptography
ECDSA	**E**lliptic **C**uvre **D**igital **S**ignature **A**lgorithm
EER	**E**qual **E**rror **R**ate
EAR	**E**qual **A**cceptance **R**ate
ERR	**E**qual **R**ejection **R**ate
ID	**ID**entifiant
JCA	**J**ava **C**ryptography **A**rchitecture
NA	**N**on **A**bordé
PDA	**P**ersonal **D**igital **A**ssistant
PIN	**P**ersonal **I**dentification **N**umber
PKI	**P**ublic **K**ey **I**nfrastructure
PRNG	**P**seudo **R**andom **N**umbers **G**enerator
RSA	**R**ivest **S**hamir **A**dleman
WSNs	**W**ireless **S**ensor **N**etworks
XOR	**eX**clusive **OR**

Introduction Générale

La sécurité des systèmes informatiques est devenue une préoccupation majeure [26] [68]. De nos jours, on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance : l'e-commerce, les opérations bancaires basés sur l'identification du demandeur, la protection civile, les crimes et tout récemment la lutte contre les fraudes sociales, etc. [25][44]. Devant la croissance exponentielle des communications tant physiques que virtuelles et les risques que cela peut représenter, la vérification automatique des personnes représente un marché gigantesque plébiscité par des besoins de sécurité de plus en plus accrue [26]. Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans un monde qui devient de plus en plus interconnecté.

Il existe traditionnellement deux manières d'identifier un individu [26]. La première méthode est basée sur une connaissance a priori (knowledge-based) de la personne telle que, par exemple, la connaissance de son code PIN (Personal Identification Number) qui permet d'activer un téléphone portable tandis que la seconde est basée sur la possession d'un objet (token-based). Il peut s'agir d'une pièce d'identité, d'une clé ou d'un badge [60] [61] [68]. Cependant, chacune de ces méthodes a ses propres faiblesses. Dans la première, le mot de passe peut être oublié ou deviné par une autre entité. Dans la seconde, le badge (ou la pièce d'identité ou la clé) peut être perdu ou volé. En outre, les mots de passe ne peuvent pas fournir des fonctions d'authentifications vitales comme la non-répudiation et la détection d'inscriptions multiples. Par conséquent, il devient de plus en plus évident que ces mécanismes ne soient pas suffisants pour déterminer d'une manière fiable l'identité d'une personne.

La biométrie ou mesure (metron) du vivant (bios) est, d'après l'encyclopédie Larousse [1] l'étude statistique des dimensions et de la croissance des êtres vivants [51]. La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques qui doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. Elle s'agit d'un domaine à très fort potentiel, en ce sens qu'elle est rattachée à la structure de la personne, elle peut être morphologique (Iris, voix, etc.), biologique (le sang, l'odeur, etc.) ou comportementale (dynamique de frappe, signature, etc.).

La reconnaissance d'empreintes digitales est une technique biométrique morphologique. Elle est connue comme la technique la plus ancienne. Les empreintes digitales sont des signatures que nous laissons derrière à chaque fois que nous touchons un objet. Elles se basent sur l'extraction et l'analyse des points caractéristiques particuliers. Elles sont uniques et immuables, elles ne se modifient pas au cours du temps (sauf par accident comme une brûlure par exemple) et la probabilité de trouver deux empreintes digitales similaires est de l'ordre de 10^{-24}. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches mais pas semblables. Elles sont composées de terminaisons en crêtes, soit le point où la crête s'arrête, et de bifurcations, soit le point où la crête se divise en deux. Le noyau est le point intérieur, situé en général au milieu de l'empreinte [50]. Il sert souvent de point de repère pour situer les autres minuties. Cette technique présente pourtant un défaut : la propreté ou l'humidité de la main nuisent à la qualité de la mesure et peuvent générer de faux rejets [60]. Elle est utilisée par les institutions financières pour leurs employés et leurs clients. Il se retrouve également dans les magasins, les hôpitaux, les écoles, les aéroports, les cartes d'identité, les passeports, les permis de conduire et de nombreuses autres applications. L'unicité, la révocabilité de cette technique a provoqué sa large utilisation dans le domaine de la sécurité pour déterminer des systèmes d'authentification fiables et sûrs. A cause de sa grande taille et les longs traitements qu'elle nécessite, le développement d'une nouvelle technique qui remédie à ses faiblesses est l'objet principal de ce présent travail.

Les systèmes cryptographiques basés sur les courbes elliptiques permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels crypto-systèmes utilisent

1. http ://www.larousse.fr/encyclopédie/

des clés de taille beaucoup plus modeste, ce qui représente un avantage pour les systèmes utilisant des dispositifs à faibles ressources et 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 génération et d'échange de clés beaucoup plus rapide [11] [69].

Notre travail entre dans le cadre de l'authentification des utilisateurs dans les réseaux à faibles ressources, basé sur l'empreinte digitale et les courbes elliptiques. Notre travail offre, principalement une étude synthétique des travaux de recherche qu'ont été fait, de proposer un nouveau protocole d'authentification basé sur l'empreinte digitale pour résoudre les problèmes liés à l'authentification classique en utilisant les courbes elliptiques qui pallie le problèmes d'espace mémoire requis par les données biométriques utilisées dans les approches proposées. Le reste de ce mémoire est structuré comme suit. Le premier chapitre est consacré aux notions élémentaires sur les courbes elliptiques. Dans le second chapitre, nous présentons un état de l'art sur les protocoles d'authentification proposés ainsi qu'une étude critique. Le troisième chapitre est consacré aux détails de notre protocole. Dans le quatrième et dernier chapitre, nous évaluons les performances de notre protocole à travers l'implémentation d'un prototype sous Java. Enfin, nous cloturons ce mémoire par une conclusion générale résumant les points essentiels de notre travail ainsi que des perspectives.

Chapitre 1

Notions élémentaires sur la cryptoraphie à base de courbes elliptiques

1.1 Introduction

La cryptographie est l'art de transmettre des données (texte, image, vidéo,) secrètes. L'un de ses aspects essentiels est de trouver un moyen de chiffrement ou de signature aussi difficile à déjouer que possible pour les éventuelles " intrus ". Les notions élémentaires sur les courbes elliptiques et leur adaptation à la cryptographie et une vue globale sur les différents algorithmes conçus dans la cryptographie à courbes elliptiques ECC (Elliptic Curve cryptography) sont présentées dans ce chapitre.

1.2 Définition

Une courbe elliptique peut être définie comme une courbe projective lisse [1] [21] [27] de degré 3, dans le plan projectif muni d'un point d'origine. L'ensemble des points est alors muni d'une structure de groupe [58] [39] [75]. Mathématiquement, une courbe elliptique est définie par une équation de la forme $y^2 = x^3 + ax^2 + b$ [46] [62]. La figure 1.1 présente un exemple d'une courbe elliptique $E_p(a,b)$ de l'équation $y^2 = x^3 + x$.

1. Lisse : c'est-à-dire qu'aucun point de la courbe n'annule toutes les équations aux dérivées partielles, donc un système n'admet pas de solutions

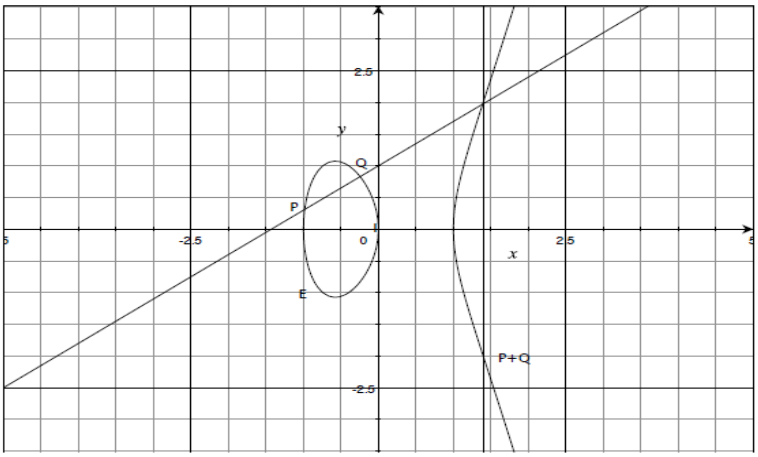

FIGURE 1.1 – Exemple de courbe elliptique $y^2 = x^3 + x$ [62].

Pour l'utiliser dans la cryptographie, on se place dans le corps Z/pZ. La courbe $E_p(a,b)$ est dite courbe elliptiques si et seulement si elle est définie par un triplé d'entiers (a,b,p) et vérifie les conditions suivantes tels que :

◇ P est premier.

◇ $0 < |a| < p$.

◇ $0 < |b| < p$.

◇ $4a^3 + 27b^2 \bmod p \neq 0$.

La courbe elliptique $E_p(a,b)$ est l'ensemble des points (x,y) tels que : $y^2 mod p = (x^3 + ax^2 + b) mod p$.

1.3 La cryptographie à base de courbes elliptiques (ECC)

La cryptographie est un domaine de mathématique a pour objet la transformation d'une donnée brute à une donnée secrète [4] [6] [11]. Les courbes elliptiques sont l'outil qui renforce cette sécurité de raison d'utiliser des clés cryptographiques à la fois légères et difficiles à détourner [58][69]. Les courbes elliptiques sont utilisées dans la cryptographie :

- Dans les algorithmes de factorisation d'entiers ;
- Pour l'échange des clés générées par l'algorithme de Diffie Hellman ;
- Pour la conception de systèmes à clés publiques (le chiffrement et la signature) ;

– Pour la conception des générateurs de nombres pseudo aléatoires.

Dans ce qui suit, nous nous intéressons aux algorithmes que fournit la cryptographie à courbe elliptique ă savoir : la génération de paire de clés, le chiffrement/déchiffrement et la signature/vérification.

1.3.1 Générations des paramètres avec ECC

Les paramètres géométriques utilisés dans la cryptographie à courbe elliptique (courbe, point de base, les paires de clés, etc.) sont générés de manière automatique. D'abord, on choisit une courbe $E_p(a,b)$ dans un corps fini ensuite un entier k très grand qui sert comme une clé privée. Deux points $A = (x_A, y_A)$ et $B = (x_B, y_B)$ sont choisis sur la courbe $E_p(a,b)$ et l'intersection de la droite reliant ces deux points avec $E_p(a,b)$ est le point de base P de la courbe. Enfin, la multiplication du point de base P et la clé privée k donne la clé publique Q [6][13][22]. L'algorithme de génération de clés est présenté à travers l'algorithme 1.

Algorithm 2 Algorithme de génération des clés

Entrées : Un entier k.
Sorties : La clé publique.
1 : Choisir une courbe elliptique $E_p(a,b)$ et un entier $k \in [1, n-1]$.
2 : Choisir deux points a et b et calculer P.
3 : Calculer $Q = kP$.
4 : retourner la clé publique Q et la clé privée k.

1.3.2 Le chiffrement et le déchiffrement avec ECC

Les opérations de chiffrement/déchiffrement classiques (exemple : RSA) sont efficaces pour la sécurité des données mais aussi couteuses en matière d'espace mémoire et de temps d'exécution. Le chiffrement/déchiffrement avec les courbes elliptiques fournit le même niveau de sécurité avec élimination de la majorité de ces problèmes [42].

1.3.2.1 Algorithme de chiffrement

Pour chiffrer, il faudra encoder tout d'abord le message clair M comme un point A_M de coordonnées (x_M, y_M). Nous utilisons la clé privée k_A de l'expéditeur et la clé publique $k_B P$ du destinataire, en additiont le point k_A avec le résultat de la multiplication k_A avec $k_B P$ (l'opération de l'addition et de multiplication propre aux courbes elliptiques) [49][11]. Les détails de ce processus sont présentés dans l'algorithme 2 :

Algorithm 3 : Chiffrement avec ECC
Entrées : Un message M.
Sorties : Une paire (M', Q).
1 : Calculer $M' = M + k_A\ (k_B P\ )$.
2 : retourner le message chiffré est le couple (M', Q).

1.3.2.2 Algorithme de déchiffrement

Pour déchiffrer, on calcule $k_B Q$ et on soustrait $k_B(k_A P)$ de M', et on obtient à la fin M [23][6]. Les détails de ce processus sont présentés dans l'algorithme 3

Algorithm 4 : Déchiffrement avec ECC
Entrées : Une paire (M',Q).
Sorties : Un message M.
1 : Calculer $k_B\ Q = k_B\ (\ k_A\ P)$.
2 : Calculer $M = [M + k_A\ (\ k_B\ P\ )]$ - $[\ k_B\ (\ k_A\ P]$.
3 : Retourner le message en claire M.

1.3.3 La signature numérique et sa vérification avec ECC

Nous présentons l'algorithme de signature digitale et de vérification sur des courbes elliptiques ECDSA (Elliptic Curve Digital Signature Algorithm)[6].

1.3.3.1 Signature

Le couple (r, s) est le résultat de l'application du processus de signature avec ECC sur un message en clair M en utilisant la clé privée du singataire. L'algorithme 4 explique les étapes suivies dans le processus de signature numérique [11] [22] [58].

Algorithm 5 Signature
Entrées : Un message $M \in N$
Sorties : Une signature du message M.
1 : Choisir un nombre entier $k \in]1, n-1[$.
2 : Calculer un point $k_P = (x_1, y_1)$ et $r = x_1$ (mod n).
3 : Si $r = 0$, aller à l'étape 1.
4 : Calculer k^{-1} (mod n).
5 : Calculer $s = k^{-1}(H(M) + xr)$.
6 : Retourner la signature du message M est le couple (r, s).

1.3.3.2 Vérification

La vérification de la signature numérique avec ECC se fait avec la clé publique du signataire [13][66][72]. Le principe de vérification est présenté dans l'algorithme 5.

Algorithm 6 : Vérification de la signatire avec ECC

Entrées : La signature (r,s).
Sorties : Vérification de la signature.
1 : Vérifier que r, $s \in [1,n-1]$.
2 : Calculer $w = s^{-1}(modn)$ et $H(M)$.
3 : Calculer $u_1 = H(M)\ w(modn)$ et $u_2 = rw(modn)$.
4 : Calculer $u_1\ P + u_2\ Q = (x_0, y_0)$ et $v = x_0(modn)$.
5 : Retourner la signature est acceptée si $v = r$.

1.4 Conclusion

L'utilisation des courbes elliptiques offre plusieurs avantages surtout pour les utilisateurs des réseaux à faibles ressources. Dans ce chapitre nous avons illustré des notions de base sur la cryptographie à courbes elliptiques. Le chapitre suivant sera consacré à l'état de l'art des protocoles d'authentification basé sur des données biométriques.

Chapitre 2

État de l'art sur les protocoles d'authentification biométriques

2.1 Introduction

Dans ce chapitre, nous présentons d'abord les différents critères d'évaluation des protocoles d'authentification à base de la biométrie, existant dans la littérature, en décrivant leurs principes ainsi que leurs importances pour l'évaluation. Nous consacrons par la suite le reste du chapitre à l'étude critique de ces protocoles ainsi que leur comparaison.

2.2 Critères d'évaluation des solutions

Afin de mieux comprendre la diversité des solutions que nous allons étudier dans ce chapitre traitant le problème d'authentification, nous proposons une comparaison à base d'un ensemble de critères définis ci-dessous :

2.2.1 Sécurité du système

Avoir un système d'authentification sécurisé revient à assurer : la protection des données confidentielles de ce système et que ce dernier fait face aux attaques existant dans son domaine du développement [31].

◇ **Sécurité des données :** La sécurité des données recouvre par définition tous les aspects concernés par la définition, l'obtention et la conservation de la confidentialité, la fiabilité de l'intégrité et de l'authenticité des données, [2] [10]. En effet, les garder

secrètes consiste à définir une bonne politique de sécurité, pour pouvoir à la fin protéger tous les processus d'authentification.

◇ **Vulnérabilité aux attaques :** Elle correspond aux faiblesses des protocoles aux attaques visant le processus d'authentification. Le protocole doit être muni d'un système de détection d'attaque ou de correction et d'évitement automatique ou il doit être conçu de façon fiable contre ces attaques. [44].

2.2.2 Coût du système

Le coût du système est une métrique importante pour mesurer les performances d'un protocole. Il dépend pour en être minimal de la réduction du coût de communication, le coût de calcul et de l'espace mémoire requis [15] [26].

◇ **Coût de communication :** Le coût de communication est le temps nécessaire aux changements des informations entre deux entités ou plus. Ce dernier dépond de la capacité du canal de transmission et de la taille des données transportées sur ce canal. Assurer un coût de communication minimal revient à avoir une bonne bande passante et à réduire au maximum la taille des données transportées afin de garantir un système léger et rapide [18][34].

◇ **Coût de calcul :** Le coût de calcul est généralement mesuré en temps moyen nécessaire pour chaque opération éffictuée (le temps moyen pour générer les données biométrique des individus et aussi en temps moyen de vérification qui désigne le temps moyen pour l'acquisition des données et la comparaison de ces dernières avec le modèle correspondant). Il consiste pour en être réduit l'utilisation des systèmes de calcul simples et rapides. C'est important de se baser sur ce critère pour concevoir un système souple et performant [34][40].

◇ **Mémoire requise :** C'est l'espace mémoire requis par les données nécessaires dans l'implémentation et le fonctionnement du système. La capacité de stockage du système doit être gérée d'une façon permettant de stocker un grand nombre de données et d'utilisateurs dans un espace mémoire très réduit tout en cherchant un bon compromis entre les deux. Cela permet de garder la rapidité et les performances du système malgré la croissance du nombre d'utilisateurs et leurs données enregistrées [34].

2.2.3 Fiabilité

La fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données dans une période de temps. C'est l'étude des défaillances des systèmes et la probabilité de n'avoir aucune défaillance à l'instant t [15] [26]. Ces défaillances sont partagées en trois catégories qui sont :

◇ **Taux de Faux Rejet ou FRR (False Rejection Rate)** : Est le pourcentage des transactions des utilisateurs légitimes rejetées par erreur. Ces transactions sont rejetées soit par le système de correspondance en raison de non-correspondance à tort ou bien en raison d'un échec à l'acquisition [32] [53] [61].

◇ **Taux de Fausse Acceptation ou FAR (False Acceptance Rate) :** Est la probabilité d'accepter un intrus dans le système tout en pensant qu'il s'agit d'une autre personne autorisée [8] [45] [73].

◇ **Taux d'Egalité d'Erreurs ou EER (Equal Error Rate) :** Est le taux calculé à partir des deux premiers taux d'erreur (FRR et FAR). Il constitue un point de mesure de performance courante, il correspond à la situation où FRR = FAR, c'est-à-dire le meilleur compromis entre les fausses acceptations et les faux rejets [1] [9]. la figure 2.1 présente l'évolution de taux de FAR et FRR en fonction de seuil de similitude.

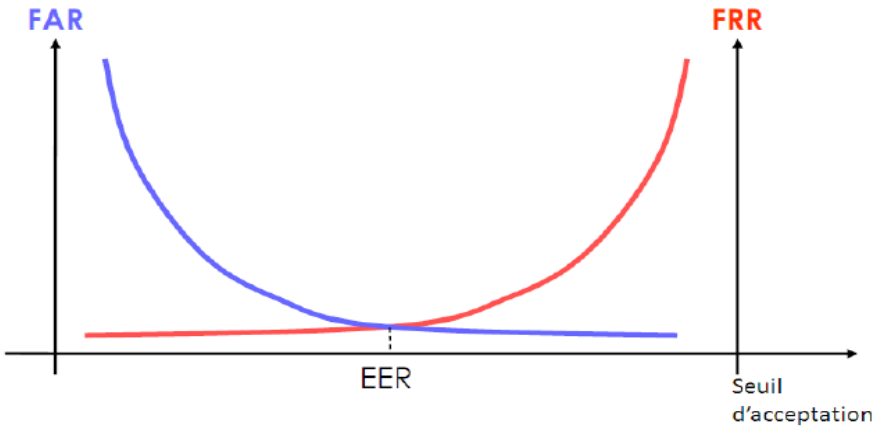

FIGURE 2.1 – Evolution de taux de FAR et FRR en fonction de seuil de similitude [1].

2.3 Classification des protocoles d'authentification biométriques dans les réseaux à faibles ressources

Nous avons classifié les protocoles d'authentification que nous allons étudier par la suite conformément à l'environnement d'application. La figure 2.2 décrit les trois classes que englobent les protocoles étudiés.

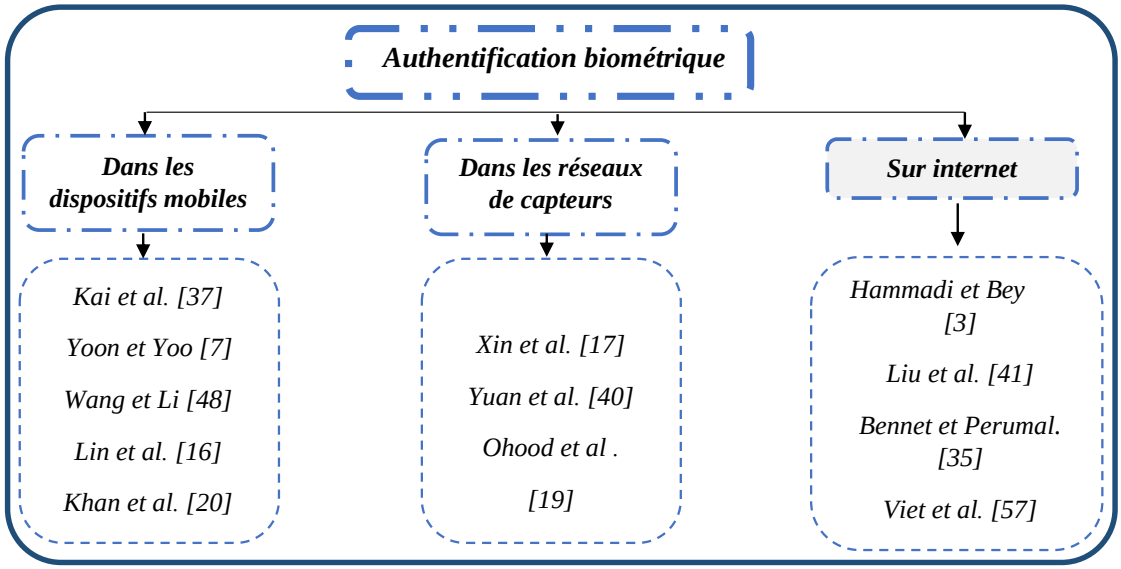

FIGURE 2.2 – Classification des protocoles d'authentification biométrique.

2.3.1 Protocoles d'authentification biométriques dans les dispositifs mobiles

Se servir d'ordinateur, de smartphone et d'autres dispositifs mobiles pour des raisons professionnelles (accédées à une entreprise, un réseau, etc.) est de plus en plus courant dans un monde extrêmement connecté. La protection des données et des communications à travers ces dispositifs doit être garantie, ce qui nécessite un système d'authentification fiable. Plusieurs solutions, que nous allons voir par la suite, ont été proposées dans ce cadre [27].

2.3.2 Protocoles d'authentification biométriques dans les réseaux de capteurs sans fil

Les réseaux de capteurs sans fil ou Wireless Sensor Networks (WSNs) sont constitués d'un ensemble de nœuds en vue de collection et de transmission de données vers un nœud puits qui les transmet à son tour au centre de traitement de données pour les analysées et ensuite prendre une décision [6][14][24][33]. Ces réseaux sont applicables sur des différents environnements (médicale, militaire, etc.), les types de données transportées sur ces réseaux sont sensibles, pour cela établir un protocole d'authentification est obligatoire pour garantir la sécurité de ces données [68] [30].

2.3.3 Protocoles d'authentification biométriques sur internet

L'explosion remarquable dans le réseau de communication Internet plus particulièrement les nouvelles applications développées sur internet (E-commerce, transaction bancaire, etc.) rend la nature des informations échangées dans ces applications très sensibles, donc pour garantir leur protection, il faut développer des systèmes d'authentification efficaces.

2.4 Étude critique de quelques protocoles d'authentification biométriques

Afin de résoudre les problèmes que souffrent les protocoles d'authentification existants, nous effectuant une analyse de chaque protocole, en se basant sur les critères d'évaluation des solutions cités auparavant.

2.4.1 Protocoles d'authentification biométriques dans les dispositifs mobiles

2.4.1.1 Fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment

Kai et al. [37], ont proposé un protocole de sécurité bio-cryptographique conçu pour l'authentification client/serveur dans un environnement mobile. Afin de manipuler les dif-

férents types d'attaques et protéger la phase d'authentification, les auteurs ont adopté différents mécanismes de sécurité à savoir : la cryptographie à courbe elliptique (ECC), l'infrastructure de clé publique (PKI) et un modèle brouillé (flou) pour sécuriser les caractéristiques biométriques qui ne sont pas seulement utilisées pour la vérification biométrique mais également pour la génération de clés bio-cryptographique.

Ce protocole assure la sécurité des données manipulées au cours du traitement car il ne stocke pas la donnée biométrique brute, il offre la sécurité contre l'attaque de force brute et celle de rejou et il assure un taux de fausses acceptations réduit. L'espace mémoire utilisé apparait réduit car il n'enregistre que les clés de petite taille, ce qui implique la réduction du coût de communication entre le serveur, le client et l'autorité de certification. Cependant ce protocole souffre de son coût de calcul élevé, son taux de faux rejets considérables et du problème de perte ou de vol de dispositif mobile qui contient toutes les informations d'authentification, il est vulnérable aussi aux attaques des canaux de transmission (interruption, interception, etc.).

2.4.1.2 A New Fingerprint Biometric Remote User Authentication Scheme Using Chaotic Hash Function on Mobile Devices

Yoon et Yoo [7], ont développé un protocole d'authentification d'utilisateur distant à base de l'empriente digitale qu'est une amélioration de protocole de Khane et al. [55] , en utilisant le dispositif mobile et la fonction de hachage chaotique.

L'utilisation de la fonction de hachage chaotique disposant d'un énorme potentiel dans la protection des actifs en raison de son comportement aléatoire et sa sensibilité aux conditions initiales a permis à ce système d'authentification d'assurer la sécurité contre les attaques de force brute, de session parallèle et les attaques d'intrus privilégié. L'espace mémoire requis dans ce protocole est minimal et il assure un taux de fausses acceptations réduit. Les faiblesses de ce protocole sont : son coût de calcul élevé, l'insécurité des données nécessaires au chiffrement de l'empreinte digitale plus le temps de communication imprévisible et les attaques de déni de service et de modification des clés. Ce protocole n'assure pas la sécurité des dispositifs mobiles.

2.4.1.3 A New Fingerprint-Based Remote User Authentication Scheme Using Mobile Devices

Wang et Li [48], ont décrit un nouveau protocole d'authentification à base d'empreinte digitale d'utilisateur à distances utilisant des dispositifs mobiles. Cette solution est une amélioration de deux autres protocoles Khan et al. [37] et Yoon et Yoo. [59], ces deux protocoles nécessitent la synchronisation d'horloge du système. Sinon, le protocole d'authentification ne fonctionnera pas correctement due à l'utilisation de paramètres d'estampillage. Pour surmonter ces problèmes des auteurs remplace les délais de temps par des nonces.

La sécurité de protocole proposé est basée sur celle des fonctions de hachage chaotique qu'a l'avantage de posséder une énorme potentielle de sécurité grâce à son comportement aléatoire et qui réduit la taille de la donnée qui implique la réduction de l'espace mémoire, les communications établies entre le serveur et l'utilisateur ont un coût réduit. Cependant ce système est vulnérable à plusieurs attaques (attaque de déni de service, attaque par rejoue, etc.). Le canal de transmission n'est pas sécurisé d'où les informations transportées sur le canal peuvent être extraites facilement, le coût de calcul est élevé à cause de grand nombre d'opérations de hachage effectuées.

2.4.1.4 Fingerprint-based user authentication scheme for home healthcare system

Lin et al. [16], ont conçu un protocole d'authentification d'utilisateur basé sur l'empreinte digitale pour les systèmes de soins et de santé à domicile pour offrir une sécurité de service et de données médicales et biologiques entre le dispositif mobile de surveillance de l'utilisateur et le serveur du système de soins et de santé à l'hôpital. Il utilise la fonction de hachage à sens unique, plus des méthodes cryptographiques et mathématiques.

Ce protocole résiste contre l'attaque d'anonymat des utilisateurs, l'attaque de falsification d'identité d'utilisateurs ou de l'agent médical, de deviner le mot de passe ou la clé secrète du serveur, l'attaque de rejou et assure la non-divulgation des informations même en cas de vol de dispositif mobile ce qui assure la sécurité des données, mais les inconvénients majeurs de ce protocole sont l'insécurité du canal de transmission publique, l'utilisation des courbes elliptiques augmente le coût de calcul et celui de communication. L'enregistrement direct de l'empreinte digitale brute nécessite un espace mémoire élevé.

L'application d'une fonction de hachage sur des données variables n'assure pas la fiabilité.

2.4.1.5 More efficient key-hash based fingerprint remote authentication scheme using mobile device

Khan et al. [20], ont présenté un système d'authentification à distance basée sur les empreintes digitales utilisant des dispositifs mobiles et une clé efficace, le protocole proposé est une amélioration de deux autres protocoles à savoir celui de Chen et al. [28] et de Truong et al. [29].

La sécurité de protocole Khan et al. [20] est héritée de celle des fonctions de hachage utilisées. Il présente une résistance aux attaques de vol, d'usurpation d'identité, de deviner le mot de passe, déni de service et il garantit l'authentification mutuelle, avec une augmentation remarquable de fonctionnalités utilisables il utilise un espace mémoire réduit, mais le problème de cette solution est le nombre de fonctions de hachage utilisé qui augmente le coût de calcul et puisque les messages transportés sur le canal sont des condensés des fonctions de hachages et le nombre de communication effectué entre les entités augmente le coût de communication de ce protocole.

2.4.2 Protocoles d'authentification biométriques dans les réseaux de capteurs sans fil

2.4.2.1 A Fingerprint-based User Authentication Protocol with One-time Password for Wireless Sensor Networks

Xin et al. [17], ont proposé un protocole d'authentification d'utilisateur basé sur l'empreinte digitale avec un mot de passe jetable pour les réseaux de capteurs sans fil. Ils ont prouvé que les protocoles de Wong et al [65], H.R. Tseng [60], x.y Liu [43], T. H. Lee [56] et d'autres sont vulnérables à de nombreuses attaques et ne sont pas pris en compte dans tous les aspects. Pour améliorer ces protocoles les auteurs ont rajouté quatre phases supplémentaires.

Les données biométriques manipulées dans les différentes phases sont sécurisées car elles sont hachées. Ce protocole résiste aux attaques (attaque de déni de service, attque de l'homme au milieu, etc.) et un coût de communication réduit vu au nombre de communication limitée. Les inconvénients de ce protocole sont la surcharge des étapes sup-

plémentaires qui diminue l'énergie des capteurs sans fil, l'espace mémoire utilisé car il enregistre toutes les données et le coût de calcul élevé dus à l'utilisation répétée des fonctions d'hachage.

2.4.2.2 A Biometric-Based User Authentication for Wireless Sensor Networks

Yuan et al. [40], ont développé un protocole d'authentification biométrique des utilisateurs conçus pour les réseaux de capteurs sans fil, la solution proposée est une amélioration de protocole de Wong et al. [48] et Watro et al. [70] qui sont vulnérables à centains types attaques (attaque de l'homme au milieu, etc.) c'est pourquoi Yuan et al. [39] tentent de surmonter certains problèmes dans leur proposition.

La sécurité du protocole proposé est basée sur celle des fonctions de hachage qui permet de réduire le coût de communication ainsi que celui de calcul ce qui ne consomme pas beaucoup d'énergie de capteur sans fil et utilise un espace mémoire réduit. Il assure aussi la sécurité contre plusieurs attaques (attaque d'usurpation d'identité, etc.), mais pas à celle de : déni de service car le protocole n'est pas compatible avec le nœud passerelle, si un message est bloqué par un intrus il ne sera pas détecté par le nœud capteur c'est pourquoi il est nécessaire d'utiliser un système de détection d'intrusion. Il est vulnérable aussi à l'attaque aux nœuds capteurs car les nœuds doivent être inviolables et déployés dans un environnement hostile, plus l'attaque d'inondation et l'attaque à clé dynamique secrète. Le protocole génère un taux de faux rejet élevé, puisque la fonction de hachage utilisée est sensible à la variabilité de l'empreinte digitale (la même personne peut ne pas s'authentifier si son empreinte subit un petit changement).

2.4.2.3 An Efficient Biometric Authentication Protocol for Wireless Sensor Networks

Ohood et al. [19], ont montré que leur protocole d'authentification est efficace pour les réseaux de capteurs sans fil. Plusieurs protocoles ont été proposés dans ce domaine pour sécuriser les nœuds capteurs mais qui étaient mets en cause par leur faiblesse aux attaques déni de service, l'homme au milieu et de falsification ainsi que leur coût élevé dus au problème du logarithme discret des courbes elliptiques. Pour pallier à ces problèmes problèmes les auteurs ont proposé un protocole d'authentification convenable à une large

échelle d'application basé sur le cryptage biométrique et les fonctions de hachage applicable aux réseaux de capteurs sans fil.

L'avantage de ce protocole est que l'iris est utilisé pour générer la clé de l'utilisateur à chaque fois que ce dernier veut s'authentifier. Ce protocole résiste à plusieurs attaques (vole de capteur, déni de service, etc.), assure la sécurité des données par l'utilisation des fonctions de hachage et la réduction du temps de communication. L'espace mémoire utilisé dans ce protocole est élevé par rapport à la capacité des capteurs, ainsi que le coût de calcul des différentes fonctions est considéré élevé.

2.4.3 Protocole d'authentification biométrique sur internet

2.4.3.1 Password hardened fuzzy vault for fingerprint authentication system

Hammadi et Bey [3], ont proposé un système bio-cryptographique qui combine entre les transformées des empreintes digitales et l'utilisation de coffre-fort flou qui génère un mot de passe traduit par l'utilisateur. Le coffre-fort flou d'empreintes digitales est basé sur une nouvelle structure de paires minuties. C'est une méthode hybride conçue dans le cadre de sécurisation des données dans les communications à distances.

L'utilisation de la biométrie (empreinte digitale) dans les systèmes d'authentification offre plusieurs avantages (l'unicité, non-falsification, etc.) et avec la transformation appliquée et le code génère à partir de cette donnée, elle garantit la sécurité. L'utilisation du coffre-fort flou l'augmente aussi dans tous les cas existant (sauvegarde, envoi, vol). La transformée de la donnée biométrique en un code binaire réduit sa taille ce qui implique la réduction d'espace mémoire, le coût de communication est réduit car le protocole nécessite que deux échanges d'informations et la taille de ces derniers est réduite. L'inconvénient major de ce protocole est le temps de calcul nécessaire à la transformation de l'empreinte à chaque fois que l'utilisateur tente de s'authentifier et sa vulnérabilité à quelques attaques (usurpation d'identité).

2.4.3.2 Fingerprint Based Identity Authentication for Online Examination System

Liu et al. [41], ont décrit un protocole d'authentification d'identité basé sur l'empreinte digitale pour un système interrogatoire en ligne au lieu de l'authentification traditionnelle

basée sur le mot de passe. Dans ce protocole, les empreintes digitales et les services d'équilibrage de charge coopèrent avec le système interrogatoire en ligne pour compléter la phase d'authentification faite par l'algorithme d'appariement de minuties.

Ce protocole traite les candidats à distance et l'évaluation des réponses est automatique, il utilise une classification des empreintes stockée pour réduire la taille de l'espace de recherche des empreintes digitales dans la base. L'inconvénient du système interrogatoire en ligne est l'incapacité de surveillance de tous les candidats, sa faiblesse contre les attaques existant sur internet qui présente plusieurs menaces sur les données stockées. Les coûts de calcul et de communication de ce protocole sont élevés.

2.4.3.3 Fingerprint Based Multi-Server Authentication System

Bennet et Perumal [35], ont proposé un système d'authentification basé sur les empreintes digitales dans les multiserveurs. Cette solution est basée sur l'extraction des caractéristiques des doigts et un nouveau protocole cryptographique pour l'identification d'un utilisateur sur un réseau. La mise en œuvre de ce nouveau système utilise les courbes elliptiques pour la génération des clés.

Ce protocole est compagnie d'une petite application qui est facile à implémenter et peut être utilisé dans les applications web, parmi les avantages de cette solution, la réduction de coût de communication, celui de calcul et sa résistance contre l'attaque de dictionnaire. Avec l'utilisation des courbes elliptiques et les fonctions de hachages il garantit la sécurité des données, la réduction de l'espace mémoire utilisé, mais à cause de la simplicité et de la facilité de cette application elle risque d'être vulnérable à plusieurs attaques (déni de service, etc.).

2.4.3.4 FingerKey, un crypto système biométrique pour l'authentification

Viet et al. [57], ont développé un cryptosystème d'authentification biométrique à base d'empreinte digitale en s'inspirant de celui de Juels et Wattenberg [75] s'appuyant sur une caractérisation de l'empreinte par analyse de texture (la mise en valeur des crêtes et vallées de l'empreinte autour d'un point fixe appelé centre morphologique) et sur la notion de codes correcteurs et les fonctions de hachages.

Ce protocole n'utilise ni le stockage de la donnée biométrique brute ni la donnée de référence pour réduire l'espace mémoire utilisé et éviter le risque de vol des données

biométriques et les faux rejets liés à la variabilité de l'empreinte, il présente aussi un taux de FAR réduit. Il fait face à plusieurs attaques et son coût de communication est réduit car il utilise les fonctions de hachage. Le seul inconvénient de ce protocole est le grand délai de traitement de l'empreinte digitale, dû aux opérations d'extraction des vallées et des crêtes et la génération des FingerKey.

2.5 Comparaison des protocoles d'authentification étudiés

Nous présentons dans ce qui suit une comparaison entre les protocoles étudiés. Cette comparaison se base sur les critères définis auparavant, nous commençons par la comparaison de sécurité de ces protocoles, ensuite la comparaison de leur coût du système et enfin la comparaison de leur efficacité.

2.5.1 Comparaison de sécurité des protocoles d'authentification étudiés

Le tableau suivant donne un aperçu global sur les protocoles qui assure ou pas la sécurité de données et la fonctionnalité conviviale d'authentification mutuelle, ainsi que s'ils sont protégés contre les attaques les plus courantes (déni de service, force brute, etc.).

Nous pouvons juger que le protocole Veit et al. [57], est performant car il peut empêcher toutes les attaques citées et la sécurité de ces données est assurée sauf qu'il n'aborde pas le sujet d'authentification mutuelle. Alors que les deux protocoles Liu et al. [41], Bennet et Perumal [35], sont vulnérables à toutes les attaques et qu'ils n'assurent pas l'authentification mutuelle. Pour Liu et al. [41], il n'assure même pas la sécurité des données. Pour le reste des protocoles ça varie entre performant ou pas selon leur principe.

Protocoles / Critères	Analyse de sécurité							
	Etat de données	**Authentification mutuelle**	**Attaque physique**	**Attaque de déni de service**	**Attaque de rejoue**	**Attaque de Force brute**	**Attaque de l'homme au milieu**	**Attaque d'usurpation d'identité**
Kai et al. [37]	Sécurisé	NA	Non	NA	Oui	Oui	NA	NA
Yoon et Yoo [7]	Non Sécurisé	NA	Non	Non	NA	Oui	NA	Oui
Wang et Li. [48]	Sécurisé	√	Non	Oui	Oui	NA	Oui	Oui
Lin et al. [16]	Non Sécurisé	√	Oui	NA	Oui	NA	Oui	Oui
Khan et al. [20]	Sécurisé	√	Oui	Oui	Oui	NA	NA	Oui
Xin et al. [17]	Sécurisé	√	Oui	Oui	Oui	Oui	Oui	Oui
Yuan et al. [40]	Sécurisé	×	Oui	Non	Oui	NA	NA	Oui
Ohood et al. [19]	Sécurisé	√	Oui	NA	Oui	NA	NA	NA
Hammadi et Bey [3]	Sécurisé	NA	Non	NA	NA	NA	NA	Non
Liu et al. [41]	Non Sécurisé	×	Non	Non	Non	Non	Non	Non
Bennet et Perumal [35]	Sécurisé	×	Non	Non	Non	Non	Non	Non
Veit et al. [57]	Sécurisé	NA	Oui	Oui	Oui	Oui	Oui	Oui

√ : Assure, **×** : Non assure, **NA** : Non abordé, **Oui** : Empêche l'attaque, **Non** : Incapable d'empêche l'attaque.

TABLE 2.1 – Analyse de sécurité des protocoles d'authentification étudiés.

2.5.2 Comparaison de coût de système des protocoles d'authentification étudiés

◇ Le tableau 2.2 illustre une comparaison par rapport au coût de calcul, le coût de communication établie entre les différentes entités et l'espace mémoire requis dans chaque protocole.

▷ Nous avons calculé le coût de calcul à base de temps nécessaire pour chaque opération effectuée. Puisque nous ne pouvons pas avoir le temps en seconde, nous avons défini différents indices utilisés dans le calcul du coût de calcul pour chaque protocole dans la phase d'enregistrement et la phase d'authentification (nous avons négligé les opérations qui ne nécessitent pas un grand temps de calcul).

▷ Le coût de communication dépond de nombre de messages transportés sur le canal de transmission et de leurs tailles. Á partir des protocoles analysés on constate que la plupart des messages échangés sont des condensés (résultat du hachage).

▷ Le coût d'espace mémoire requis se calcule seulement lors de la phase d'enregistrement. Dans le tableau suivant nous calculons l'espace mémoire requis pour toutes les entités (utilisateur, serveur).

Les indices utilisés dans les calculs sont les suivant :

- T_H : temps nécessaire à l'exécution d'une fonction de hachage ;
- T_{XOR} : temps nécessaire à l'exécution d'une opération XOR ;
- T_{EC} : temps nécessaire à l'utilisation d'une courbe elliptique ;
- $T_{C/D}$: temps nécessaire à l'exécution d'une opération de chiffrement ou de déchiffrement ;
- T_{TE} : temps nécessaire à la transformation de la donnée biométrique ;
- T_G : temps nécessaire pour la génération d'une clé ;
- N : nombre entier, dépond de degré de polynôme P (P devisé en N parties) ;
- C_{ID} : la taille de l'identificateur ID_i est de 64 bits ;
- C_H : la taille des fonctions de hachage est de : 128 bits ;
- C_{ECC} : la taille des résultats d'application d'une EC est de 160 bits ;
- C_{ED} : la taille d'une empreinte transformée ou d'une empreinte brute ;
- $C_{C/D}$: la taille du résultat de l'opération de chiffrement ou déchiffrement ;

- E_{ID} : espace mémoire requis par l'ID d'un utilisateur ;
- E_{ED} : espace mémoire requis par l'empreinte brute ou par sa transformée ;
- E_H : espace mémoire requis par le résultat de l'opération de hachage ;
- $E_{C/D}$: espace mémoire requis par le résultat de chiffrement ou déchiffrement.

Protocoles \ Critères	Coût de système : Coût de calcul	Coût de système : Coût de communication	Coût de système : Coût d'espace mémoire
Kai et al. [37]	$T_{TE} + 4T_{ENK/DEK} + T_{EC}$	$C_1 + 2C_{Enc/Dec} + C_2 = 512$ bits.	$E_{ID} + sn*n = (76*n)$ bits.
Yoon et Yoo [7]	$8\ T_H + 9\ T_{XOR}$	$M + C_H = 321$bits.	$E_{ID} + pw + n + 2*E_{ED} = 344$ bits.
Wang et Li [48]	$6T_H + 13T_{XOR}$	$C_{ID} + 4C_H = 576$ bits	$2E_{ID}+6E_H+2E_{ED}= (896+2E_{ED})$ bits
Lin et al. [16]	$6T_H + 9T_{XOR} + 4T_{ENK/DEK}$	$2C_H + C_{Enc/Dec} = (384+C_{Enc/Dec})$ bits	$2E_{ID}+ 2E_H + E_{ED}= (384+ E_{ED})$ bits
Khan et al. [20]	$13T_H + 20T_{XOR}$	$7C_H= 896$ bits	$5^E_H= 640$ bits
Xin et al. [17]	$T_{TE}+2T_H + 2T_{ENK/DEK}$	$2C_{ID} + pw + C_{ED} + T + C_{Enc/Dec}= 393$ bits.	$E_{ID} + pw+ E_{ED}= 200$ bits.
Yuan et al. [40]	$8T_H + 3T_{XOR}$	$4C_H= 512$ bits	$E_{ID}+3C_H= 448$ bits
Ohood et al. [19]	$T_{TE}+ 8T_H + 3T_{XOR} + 3T_{ENC/DEC}$	$C_{ID}+ C_H + 2*T+ C_{Enc/Dec}= 322$ bits.	$2E_{ID}+ E_I+ Y= 384$ bits.
Hammadi et Bey [3]	$2T_{TE} + 2T_G$	$C_{ID} + C_{EC} + 256 = (320+C_{EC})$ bits	$E_{ID}+ E_{ED}+ 256= 2368$ bits
Liu et al. [41]	$2T_H + 2T_{TE}$	$C_{ID}+ C_{ED}+ req= 1216$ bits.	$E_{ID}+ E_{ED}= 192$ bits.
Bennet et Perumal [35]	$2T_H + 2T_{EC} + 2T_{ENC/DEC}$	$C_{ECC}+2C_{Enc/Dec} = 672$ bits	$2E_H+E_{ECC}+2E_{Enc/Dec} = 928$ bits
Veit et al. [57]	$NT_H + NT_{XOR} + 2T_{TE}$	$C_{ED}= 128$bits.	poly+ $E_{ED}= 1152$ bit.

TABLE 2.2 – Comparaison de coût de calcul, coût communication et espace mémoire requis des protocoles d'authentification étudiés.

2.5.3 Comparaison d'efficacité des protocoles d'authentification étudiés

◇ Le tableau 2.3 effectue une comparaison entre les protocoles d'authentifications étudiées selon les fausses acceptations et les faux rejets, ici nous ne pouvons pas avoir des résultats numériques, mais nous les avons estimés.

	Analyse de fiabilité		
Critères / **Protocoles**	**FFR**	**FAR**	**EER**
Kai et al. [37]	Élevé	Réduit	Élevé
Yoon et Yoo [7]	Réduit	Réduit	Réduit
Wang et Li [48]	NA	NA	NA
Lin et al. [16]	NA	NA	NA
Khan et al. [20]	NA	NA	NA
Xin et al. [17]	NA	NA	NA
Yuan et al. [40]	NA	NA	NA
Ohood et al. [19]	NA	NA	NA
Hammadi et Bey [3]	Élevé	Nul	Élevé
Liu et al. [41]	NA	NA	NA
Bennet et Perumal [35]	NA	NA	NA
Veit et al. [57]	Réduit	Nul	Réduit

TABLE 2.3 – Comparaison de FFR, FAR et EER des protocoles d'authentification étudiés.

2.6 Conclusion

Diverses approches ont été proposées pour l'authentification biométrique des utilisateurs dans les réseaux à faibles ressources. Dans ce présent chapitre, nous avons présenté quelques travaux que nous avons jugés intéressant pour prouver l'accroissement potentiel apporté par le type d'authentification à base d'empreinte digitale. Ensuite nous avons fait une comparaison entre ces divers protocoles en les projetant sur des critères de comparaison que nous avons choisis.

Dans le chapitre suivant, nous allons introduire une nouvelle technique d'authentification à base de l'empreinte digitale ne nécessitant pas de stockage des données biométriques. Notre construction a comme avantage de limiter le risque de vol des données biométriques et de ce fait, améliore la sécurité de l'authentification.

Chapitre 3

Protocole d'authentification à base d'empreinte digitale d'un patient pour le système de soins et de santé à domicile

3.1 Introduction

Nous avons montré à travers l'étude critique des protocoles d'authentification que l'utilisation de la biométrie permet d'augmenter la sécurité des réseaux à faibles ressources. Cependant ces protocoles présentent des risques en matière de respect des droits et des libertés fondamentales. Le fait de capturer et de conserver des données biométriques brutes peut constituer une invasion de la vie privée.

Dans ce chapitre, nous décrivons d'abord le fonctionnement de notre protocole d'authentification des patients, dotés d'un réseau de capteurs sans fil BANet (Body Area Network) connecté à un dispositif mobile, en explicitant son architecture et sa politique d'authentification. Nous consacrons par la suite le reste du chapitre à l'etude de sécurité de notre protocole contre les attaques les plus répétées dans le domaine de l'authentification à base de la biométrie.

3.2 Motivation

L'application des nœuds capteurs et des dispositifs mobiles (Smartphone, Personal digital Assistant PDA, Ordinatuer portable, etc.) dans différents domaines (environne-

mental, médical, etc.) devient de plus en plus large et quotidienne. Pour sécuriser cette application il est impératif de définir une politique d'authentification stricte.

Plusieurs protocoles d'authentification ont été proposés, mais en matière d'efficacité la majorité d'entre eux sont vulnérable aux différentes attaques telles que (attaque de déni de service, attaque de rejoue, attaque de force brute, attaque d'usurpation d'identité et l'attaque de l'homme au milieu) qui influencent la sécurité de données, ils souffrent aussi du coût de communication élevé force à la grande taille des données échangées entre les entités communiquantes, qui engendrent ainsi la lenteur des différents processus exécutés [37]. Leur coût de calcul aussi est considéré élevé le fait de répéter le traitement de la donnée biométrique et de sa vérification qui nécessite une longue durée de calcul. Même l'espace mémoire requis par ces données volumineuses présente un problème du stockage pour ces protocoles. Leur fiabilité est variable et dépend de leurs performances.

Pour remédier aux inconvénients cités auparavant une combinaison de l'approche biométrique avec les techniques de la cryptographie est indispensable. D'ailleurs la biométrie et la cryptographie sont devenues mutuellement complémentaires [37]. Il est raisonnable et faisable d'incorporer la biométrie dans l'infrastructure cryptographique des protocoles pour pouvoir établir un protocole bio-cryptographique efficace qui transforme la donnée biométrique en une donnée révocable sûre utilisée dans l'authentification des patients. Le protocole doit utiliser des téchniques cryptographiques pour minimiser le coût de calcul et celui de communication et garder la donnée biométrique en sécurité pour proteger la vie privée du patient qui est un critère très important dans le domaine de la biométrie. L'utilisation de cette donnée biométrique pour la génération des paires de clés enrichie la sécurité du processus d'authentification et d'autres service de sécurité comme la confidentialité grâce au chiffrement des données échangées entre le patient et le serveur de traitement, l'intégrité et la non-répudiation grâce à la signature numérique des données échangées par la clé privée du signataire.

3.3 Modèle du réseau

L'architecture du réseau dédiée au protocole d'authentification proposé est constituée de trois parties : la première partie se compose d'un patient doté d'un certain nombre de biocapteurs placés sur ou à proximité immédiate de son corps et un dispositif mobile, ils forment ensemble une architecture BANet. La deuxième partie est le canal de communication entre le patient et le serveur de traitement de l'hôpitale. La troisiéme partie est constituée d'un serveur de traitement d'informations relatives à l'état de santé des patients enregistrés, déployé à l'hôpital.

Dans notre protocole le serveur de traitement est supposé sécurisé physiquement sauf pour les personnes autorisées et son horloge est supposée synchroniser avec celle du dispositif mobile du patient. Nous supposons aussi que l'architecture BANet assure une communication secrète et légitime entre les biocapteurs et le dispositif mobile. L'architecture du réseau décrite ci-dessus est illustrée dans la figure 3.1 :

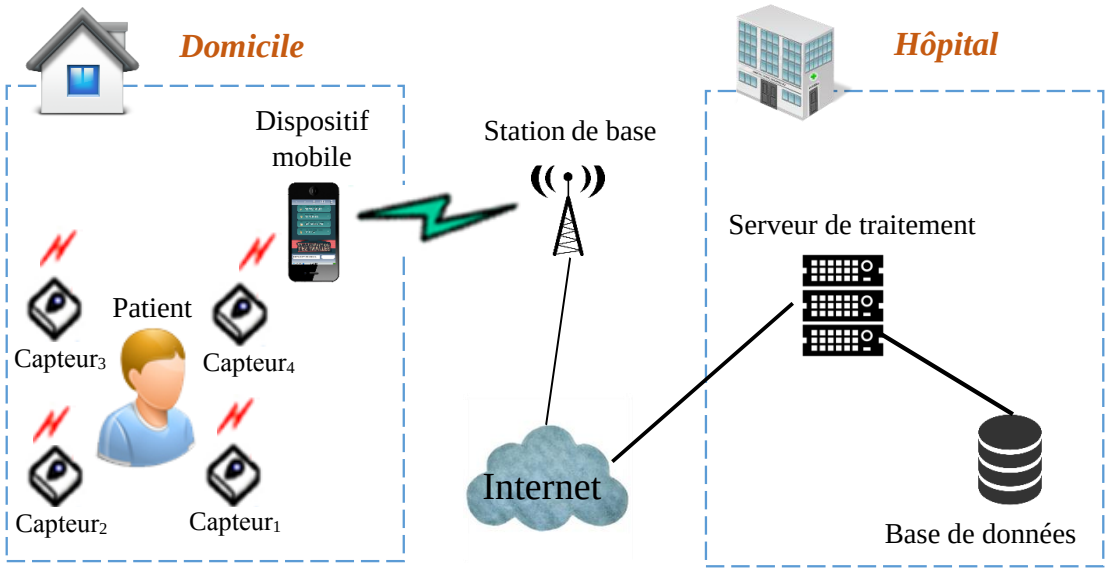

FIGURE 3.1 – Structure du système de soins et de santé à domicile de notre protocole.

Il y a trois parties impliquées dans notre protocole d'authentification, les acteurs participants dans ces parties sont décrits comme suit :

◇ **Bio-capteur :** (capteur biométrique) petit appareil, placé sur une zone du corps d'un patient afin de capter les variations morphologiques ou physiques jugées anormales et de les envoyer comme une alerte au dispositif mobile du patient [33][68] ;

◇ **Patient :** Agent humain doté d'un certain nombre de bio-capteurs placés sur ou à proximité immédiate de son corps et d'un dispositif mobile connecté à ces bio-capteurs [16] ;

◇ **Dispositif mobile :** Un appareil sans fil qui peut être un smartphone, un PDA ou un ordinateur portable, etc. Sensé à recevoir l'alerte de bio-capteurs et la transmettre au serveur de traitement [27] ;

◇ **Serveur de traitement :** Machine puissante en matière de calcul et de stockage placé à l'hopital, consiste à recevoir et à traiter la requête venant du dispositif mobile du patient et de répondre à cette requête [16].

Les méthodes d'authentification biométriques proposées avaient l'air efficace mais avec l'évolution des applications et de l'environnement de leur utilisation, plusieurs problèmes sont apparus comme par exemple le stockage et l'utilisation de la donnée biométrique brute qui augmente l'espace mémoire requis et les couts de communication et de calcul.

De ce fait, trouver un compromis entre les avantages de l'utilisation de la biométrie et les inconvénients engendrés par sa manipulation est la problématique à résoudre pour établir un protocole d'authentification efficace avec une donnée biométrique sécurisée.

3.4 Notre protocole

3.4.1 Aperçu sur la solution

Le protocole proposé est basé sur la combinaison de la cryptographie à courbes elliptiques et la biométrie (les empreintes digitales des patients). Il se dévise en deux phases à savoir : la phase d'initialisation (génération des paramètres de sécurité et l'enregistrement) et la phase d'authentification mutuelle (vérification et validation des identités du patient et du serveur). Une explication détaillée de ces deux phases ainsi qu'un tableau de notations utilisées dans notre protocole sont présentées dans ce qui suit :

Notation	Signification
F_p	Un corps finis
$E(F_p)$	Une courbe elliptique : « $y^2=x^3+ax+b$» définie sur F_p tel que $4a^3 = 27b^2 \neq 0$.
P	Point de base de la courbe elliptique $E\ (a, b)$.
ID_i	Identificateur unique d'un patient i.
N_i	Numéro de série de dispositif mobile du patient i.
B_i	Empreinte digitale d'un patient i.
(C_s, C'_s)	Clé (publique/privé) du serveur
(C_i, C'_i)	Clé (publique/privé) du patient i.
T_i / T'_i	Estampille de patient dans deux instants différents.
T_s / T'_s	Estampille de serveur dans deux instants différents.
ΔT	Intérvalle du temps valide.
M	Message d'alerte.
$H(.)$	Fonction de hachage à sens unique sécurisée.
$\|\|$	Opération de concaténation.
SM	Clé de session partagée entre le dispositif mobile et le serveur.
+	Opérateur de somme dans les courbes elliptiques.
×	Opérateur de multiplication dans les courbes elliptiques.

TABLE 3.1 – Notations utilisées dans le protocole proposé.

3.4.2 Phase d'initialisation

La phase d'initialisation se fait hors-ligne ce qui veut dire que l'enregistrement d'un patient se fait avec sa présence physique (le paient doit se rendre physiquement à l'hôpital où il fait ses visites médicales), cette phase se déroule en trois étapes :

◇ **Etape 1 :** le patient i présent imprime son empreinte digitale B_i (à l'aide d'un lecture capteur d'empreinte) et présente au serveur le numéro de série de son dispositif mobile N_i.

◇ **Etape 2 :** le serveur ayant la paire de clé (C_s : Publique, C'_s : Privée), génère un identifient unique ID_i pour le patient présent, hache l'empriente digitale B_i du patient i, tel que $B_i(S_i = H(B_i))$

Il choisit ensuite une courbe elliptique $E_p(a,b)$, son point de base P et il calcule la clé publique du patient comme suit :

$C_i = P \times C_i'$ tel que C_i' est la clé privée du patient calculé comme suit :

$$C_i' = H(ID_i \,||\, N_i \,||\, S_i).$$

Le seveur enregistre à la fin dans sa base de données les deux paramètres ID_i et C_i.

◇ **Etape 3 :** le patient enregistre sur son propre dispositif mobile la clé publique du serveur de l'hôpital C_s et son ID_i.

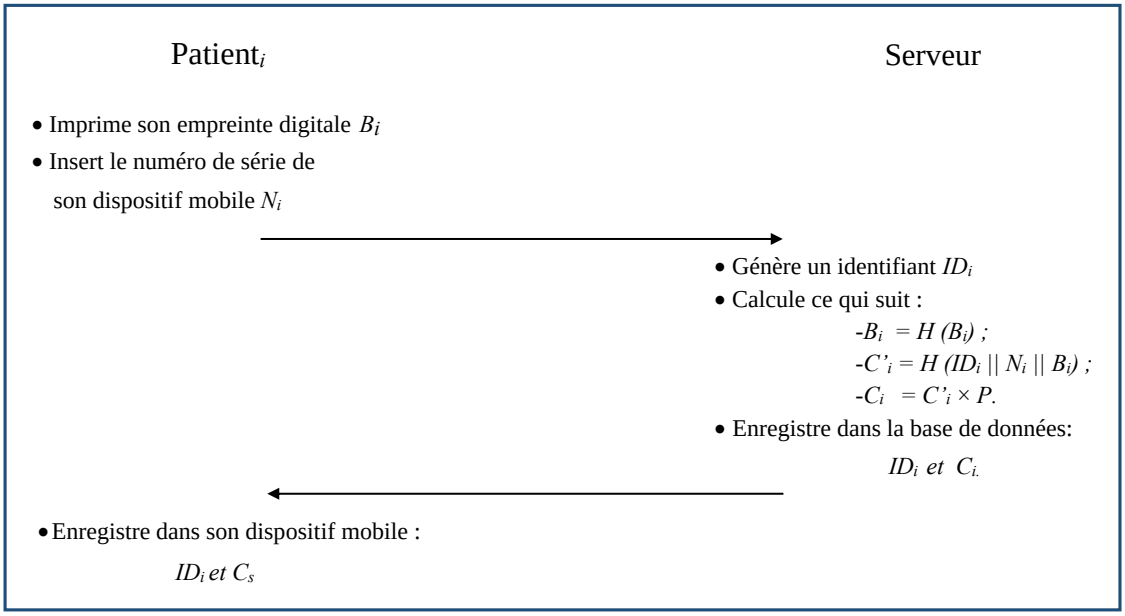

FIGURE 3.2 – Phase d'initialisation de protocole proposé.

3.4.3 Phase d'authentification

La phase d'authentification n'est entamée que si un bio-capteur détecte une situation anormale sur l'état de santé du patient [38]. Il déclenche une alerte M qui l'envoie au dispositif mobile du patient, suite à ce déclenchement d'alerte la phase d'authentification commence et elle se déroule en quatre étapes décrites comme suit :

◇ **Etape 1 :** le patient pose son doigt sur son dispositif mobile programmé à capturer l'empreinte digitale B_i' de ce doigt et lui appliquer une fonction de hachage $B_i' = H(B_i')$ Le dispositif mobile lance ainsi la fonction qui récupère son numéro de série N_i et

récupère aussi son $ID_i^{'}$ et l'estampille T_i, il calcule ainsi sa clé privée comme suite : $C_{i1}^{'} = [H(ID_i^{'}||N_i||B_i^{'})]$.

Il signe l'alerte M par la clé privée $C_i^{'}$, il forme le message req comme suit :

$Req = [ID_i^{'}, T_i, M, (M)_{C_i^{'}}]$

Il le chiffre avec les courbes elliptiques en utilisant sa clé privée $C_i^{'}$ et la clé publique du serveur C_s qui forme une nouvelle clé K_{is} (voir 1.3.2), et l'envoie via le réseau Internet au serveur de traitement de l'hôpital et il attend un délais qui dépond de type d'alerte, s'il ne reçoit aucun ACK il renvoi la même alerte.

◇ **Etape 2 :** à la réception de $(Req)_{C_s}$, le serveur déchiffre avec sa clé privée $C_s^{'}$ et la clé publique du patient C_i qui fomre la clé K_{si}, il récupère l'ensemble $\langle ID_i^{'}, T_i, M, (M)_{C_i^{'}} \rangle$, compare T_i reçu avec son estampille T_s actuelle comme suit : $T_s - T_i \leq \triangle T$, ou $\triangle T$ est l'intervale de temps valide pour un délais de transmission, si ce n'est pas vérifié, il rejeter la demande d'œverture de session (voir 3.5.2), sinon il effectue les opérations suivantes : Il vérifie la validation de l'identité du patient $ID_i^{'}$ et récupère de sa base de données la clé publique correspondante à cet identificateur $ID_i^{'}$ pour vérifier la signature de l'alerte $(M)_{C_i^{'}}$ et le comparer avec M, si $[(M)_{C_i^{'}})_{C_i}] = M$ alors le patient est authentifié et le serveur répond par un acquittement $ACK = [T_s^{'}, M, ((M)_{C_i^{'}})]_{K_{si}}$ chiffré avec la clé K_{si} des courbes elliptiques au dispositif mobile (voir 1.3.2), sinon il rejette la demande d'ouverture de session.

◇ **Etape 3 :** à la réception de l'ACK, le dispositif mobile déchiffre l'ensemble $[T_s^{'}, M, (M)_{C_s^{'}}]$ par la clé K_{is} (voir 1.3.2), compare $T_s^{'}$ reçu avec son estampille courant $T_i^{'}$: $T_i^{'} - T_s^{'} \leq \triangle T$, si ce n'est pas vérifié il rejeter la demande d'œverture de session, sinon il effectue les opérations suivantes : Il vérifie la validété de la signature numérique $\langle (M)_{C_s^{'}} \rangle$ avec la clé publique du serveur, compare le résultat avec M, si $M = [(M)_{C_s^{'}}]_{C_s}$ alors le serveur est authentifié, sinon le dispositif mobile rejette la demande d'ouverture de session.

◇ **Etape 4 :** après l'authentification mutuelle entre le dispositif mobile du patient et le serveur de traitement, ils génèrent la clé de session $SM = H(ID_i||T_s^{'}||M)$ pour protéger les futures communications. La Figure 3.3 illustre d'une manière globale les étapes de la phase d'authentification.

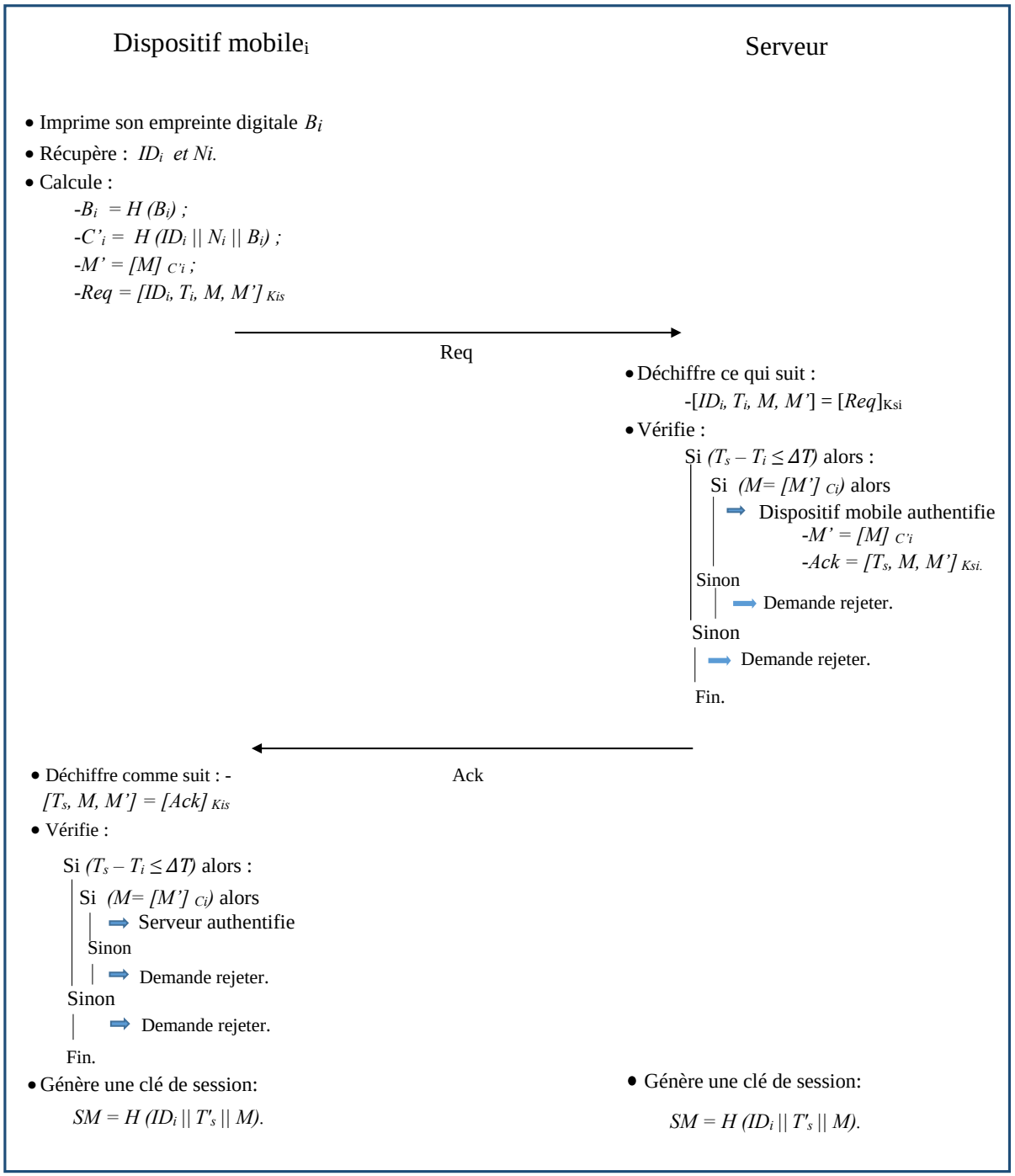

FIGURE 3.3 – Phase d'authentification de protocole proposé.

3.5 Analyse de sécurité de notre protocole

Dans cette section nous allons évaluer la sécurité de notre protocole face aux attaques existant dans la littérature.

3.5.1 Attaque d'usurpation d'identité

C'est où un adversaire vole ou trouve un dispositif mobile d'un patient légitime, il fait une copie des informations nécessaires à une authentification comme l'identificateur ensuite l'utiliser ultérieurement dans ses propres communications avec le serveur.

Dans notre protocole proposé, si un attaquant obtient l'ID_i du patient légitime et il le réutilise dans son propre message, le serveur détecte que la clé privée de l'attaquant ne correspond pas à la clé publique du patient ayant l'identifiant ID_i.

3.5.2 Attaque de rejoue

L'attaque de rejoue est une action offensive par laquelle un adversaire peut jouer le rôle d'un patient légitime en réutilisant une information obtenue à partir d'un processus précédent du protocole [13][27][34].

Dans notre protocole le message $\langle ID_i, T_i, M, [(M)_{C_i'}]_{K_{is}} \rangle$ envoyé au serveur est déchiffré par la clé privée du serveur et la clé publique du patient, donc le message ne peut être déchiffré que par le serveur lui-même. Si un adversaire veut rejouer un ancien message il ne peut modifier le paramètre de temps inclus dans ce message, ce qui fait le serveur détecte facilement qu'il s'agit d'une attaque car $T_s - T_i > \triangle T$.

3.5.3 Attaque d'interception

C'est une attaque ou un adversaire tente seulement d'écouter un message envoyé par un patient légitime vers le serveur de l'hôpital et d'essayer par la suite d'utiliser les informations récoltées par cette écoute [12].

l'information échangée entre le dispositif mobile et le serveur est signée ensuite chiffrée réspectivement par la clé secrète du patient ensuite par la clé publique du serveur. Donc même si l'intrus intercepte le message il est impossible d'obtenir l'information originale car elle est signée par une clé privée non enregistrée et chiffrée par deux clés qui ne sont connues que par leurs propriètaires.

3.5.4 Protection de la vie privée

Le domaine de la biométrie est très sensible puisqu'il touche à la vie privée des utilisateurs, donc le meilleur protocole utilisant la biométrie est celui qui assure que cette vie

privée est toujours protégée dans tous les cas de son utilisation [1][2][10][54].

Les données secrètes du patient, dans notre protocole, que ce soit son empreinte ou ses données médicales, sont sécurisées par sa clé privée $C_i^{'}$ qui ne peut être divulgué car elle n'est jamais enregistrée.

3.5.5 Attaque d'interruption

C'est une attaque ou un adversaire tente de ne pas laisser un message passer vers sa destination pour empêcher la réception d'une réponse où pour qu'il envoie lui-même une réponse (fabrication).

Notre protocole remédie à cette attaque par le processus suivant : après qu'un patient envoi son message au serveur, il attend qu'un délai de temps termine, s'il ne reçoit aucun acquittement du serveur il renvoie le message. Sinon il vérifie l'estampille T_s de l'acquittement reçu et la signature du serveur légitime .

3.5.6 Attaque physique

Elle survient lorsqu'un adversaire essaye toutes les attaques précitées et ne réussit pas à casser le protocole, il tente pour une dernière chance d'attaquer le patient physiquement et de lui voler son dispositif mobile pour obtenir les informations qui lui permettent de s'authentifier à sa place.

Le protocole proposé procède d'une façon que même si le dispositif mobile du patient est volé, rien n'est enregistré à part la clé publique du serveur et l'identifiant du patient qui ne suffit pas pour s'authentifier.

3.6 Conclusion

Dans ce chapitre, nous avons présenté en détail le principe de notre approche. En résumé, notre solution consiste à combiner la cryptographie à courbe elliptique avec la biométrie pour en sortir avec un système d'authentification encore plus résistant et fiable qui utilise l'empreinte digitale du patient non seulement pour s'authentifier mais aussi pour générer la paire de clés utiliser dans la signature et le chiffrement des données échangées lors de la communication entre le patient et le serveur de traitement de l'hôpitale.

Afin de valider notre proposition, nous implémentons dans le chapitre suivant une application client/serveur sous Java. Nous effectuons ensuite une analyse par des tests sur les performances de ce protocole pour estimer sa fiabilité sa rapidité et son efficacité.

Chapitre 4

Évaluation des performances

4.1 Introduction

L'évaluation de performances est un processus qui consiste à implémenter un modèle du système (réel) étudié, mener des expérimentations sur ce modèle, interpréter les observations fournies par le déroulement du modèle et formuler des décisions relatives au système [24].

Ce chapitre est consacré à l'évaluation des performances de notre protocole proposé. Il est divisé en trois parties, la première partie concerne l'implémentation et les outils de développement que nous avons choisis pour valider notre protocole. On s'intéresse dans la seconde partie, à l'évaluation du temps d'exécution de notre protocole. On le compare dans la dernière partie avec d'autres protocoles d'authentification existant dans la littérature.

4.2 Implémentation

Pour la validation de notre protocole proposé, nous avons implémenté un prototype sous java, les détails de l'implémentation sont les suivants :

4.2.1 Outils de développement

Pour pouvoir implémenter un prototype d'authentification utilisant l'empreinte digitale et la cryptographie à courbes elliptique (ECC), nous avons choisi d'utiliser " Java " qui est un langage de programmation moderne, développé par Sun Microsystems (aujourd'hui racheté par Oracle). Une des plus grandes forces de java est son excellente portabilité

c'est-à-dire son fonctionnement sur toutes les plateformes. Son utilisation nous a permis aussi de tirer profit de l'architecture de la cryptographie Java JCA (Java Cryptography architecture) qu'elle fournit. JCA est un Framework pour l'accès et le développement de fonctionnalités cryptographiques. Elle comprend des APIs qui permettent plusieurs implémentations interopérables d'algorithmes et d'autres services de sécurité implémentés dans des providers ajoutés dans la plateforme via une interface standard qui facilite aux applications d'utiliser ces services de sécurité sans connaître les détails de leurs implémentations (le provider utilisé dans notre prototype est celui de bouncycastle). Les APIs sont utilisés pour un grand nombre de services cryptographiques, comprenant :

- Algorithmes de hachage ;
- Algorithmes de signature numérique ;
- Chiffrement en mode bloc (block Cipher) ;
- Cryptographie à courbe elliptique (ECC) ;
- Générateurs de clés secrètes et de pair de clés ;
- Générateurs de nombres pseudo aléatoires (PRNG).

À cause des contrôles d'exportation imposés par le gouvernement U.S sur les logiciels de cryptographie, les APIs Java cryptographiques sont organisés dans deux packages différents :

- Le package java.security contient des classes non concernées par les contrôles d'exportation (comme digital signature et message digest) ;
- Le package javax.crypto contient des classes concernées par les contrôles d'exportation (comme KeyAgreement).

Le tableau 4.1 illustre les packages utilisés dans notre prototype et leur description :

Package	Description
java.securité.SecureRandom	Pour la génération des nombres aléatoires.
Java.security.MessageDegest	Pour la fonction de hachage.
org.bouncycastle.math.ec.*	Pour la génération de la courbe elliptique et ses paramètres de base.
java.math.BigInteger	Pour générer des nombre aléatoire très grand.
java.util.Calendar;	Pour l'obtention de l'estampille du système.
java.security.Signature	Pour la classe de signature numérique et sa vérification fournies par bouncycastle.
javax.crypto.Cipher;	Pour le chiffrement et le déchiffrement de bouncycastle.

TABLE 4.1 – Packages utilisées dans notre cryptosystème implémenté.

L'utilisation de ces packages nous a fourni des fonctionnalités cryptographiques de base sans se préoccuper de l'implémentation des algorithmes, ils permettent d'avoir un code java léger, claire et avec un minimum de nombre de lignes d'instructions.

4.3 Évaluation en temps d'exécution

Notre protocole s'exécute en deux phases, dans chaque phase un ensemble d'opérations est effectué. Dans la phase d'initialisation nous avons appliqué deux fois la fonction de hachage et une seule opération de multiplication d'ECC (Elliptic Curve Cryptography) pour générer la clé publique du patient. Dans la phase d'authentification nous avons signé, ensuite chiffré le message avec ECC.

Pour évaluer le temps d'exécution de notre protocole, nous avons varié la taille de la clé générée par les courbes elliptiques (en changeant le domaine des paramètres générés) et constater l'évolution de temps d'exécution de chaqu'une des opérations cryptographiques utilisées. Les résultats obtenus sont les suivants :

4.3.1 Temps de génération des clés

Le tableau 4.2, illustre l'évolution du temps nécessaire pour génèrer les paramètres de la courbe (la courbe, point de base, paire de clé, etc.) en foction de la taille de la clé à

générer.

La taille de la clé (Bites)	Temps de génération de paramètres (ms)
160	0.003
192	0.004
224	0.005
256	0.006
384	0.011
512	0.012

TABLE 4.2 – Temps de génération des paramètres en fonction de la taille des clés.

4.3.2 Temps de génération de la signature et sa vérification

Le tableau 4.3, illustre le temps nécessaire pour signer et vérifier la signature en variant la taille de la clé.

La taille de la clé (Bites)	Le temps nécessaire à une signature (ms)	Le temps nécessaire à la vérification (ms)
160	0.004	0.006
192	0.005	0.007
224	0.006	0.008
256	0.007	0.010
384	0.008	0.011
512	0.010	0.013

TABLE 4.3 – Temps de signature et de vérification.

4.3.3 Temps de chiffrement et de déchiffrement

Le tableau 4.4, illustre le temps nécessaire pour chiffrer et déchiffrer en fonction de la taille de la clé.

La taille de la clé (Bites)	Le temps nécessaire à un chiffrement (ms)	Le temps nécessaire à un déchiffrement (ms)
160	0.005	0.006
192	0.004	0.007
224	0.005	0.009
256	0.005	0.011
384	0.008	0.012
512	0.010	0.014

TABLE 4.4 – Temps de chiffrement et de déchiffrement.

4.3.4 Temps d'exécution total de protocole proposé

Le tableau 4.5, illustre le temps d'exécution total de notre protocole en augmentant à chaque fois la taille de la clé.

La taille de la clé (Bites)	Le temps total (ms)
160	0.045
192	0.050
224	0.061
256	0.072
384	0.089
512	0.106

TABLE 4.5 – Temps d'exécution total.

Nous constatons que le temps d'exécution de notre protocole, le temps nécessaire aux opérations de génération de clés, de signature numérique et sa vérification, de chiffrement et de déchiffrement augmentent à chaque fois qu'on augmente la taille de la clé, mais il reste minimal et très rapide, par exemple, le temps nécessaire à une génération des paramètres de la courbe est négligeable il atteint 0 .012 ms pour la plus grande clé (512

bites), pour notre protocole on les génère dans 0.04 ms avec une clé de 192 bites. Le temps nécessaire à la signature numérique augmente en fonction de la taille de la clé mais il est toujours inférieur à celui de la vérification de la signature. Même le temps d'opération de chiffrement (déchiffrement) augmente lentement en fonction de l'augmentation de la taille de la clé.

4.4 Comparaison

Dans le tableau 4.6, nous avons effectué une comparaison entre le temps d'exécution pratique de notre protocole et celui de Kai et al. [37], Ohood et al. [19] et Yoon et al. [36] pour des tailles de la clé différentes :

Taille de la clé / Protocole	128	192	224	256	384	512
Kai et al. [37]	0.73 ms	1.10 ms	1.29 ms	1.47 ms	2.21 ms	2.95 ms
Ohood et al. [19]	3.508 ms	5.262 ms	6.139 ms	7.016 ms	10.524 ms	14.03 ms
Yoon et al. [36]	23.634 ms	35.451 ms	41.58ms	47.268 ms	70.90 ms	94.536 ms
Notre protocole	0.045 ms	0.050 ms	0.061 ms	0.072 ms	0.089 ms	0.0106 ms

TABLE 4.6 – Comparaison temps d'exécution de notre protocole avec ceux d'autres protocoles.

Pour Kai et al. [37], il a calculé son temps d'exécution pour une clé de 256 bites qui est égale à 1.47 ms, Ohood et al. [19] a comparé entre son temps d'exécution et celui de Yoon et al. [36] pour une clé de 256 bites et il a trouvé que le sien est meilleur. Dans notre protocole on utilise une clé de taille 192 bites, le temps d'exécution de notre protocole est de 0.050 ms, c'est le meilleur par rapport aux autres surtout en le comparant avec Kai et al. [37], le protocole qu'on a jugé le plus performant parmi ceux que nous avons étudiés.

L'utilisation des courbes elliptiques avec l'empreinte digitale nous a permis de concevoir un protocole très performant en termes de l'overhead et de temps d'exécution en

réduisant la taille des clés ainsi la taille des données transmises.

4.5 Conclusion

Dans ce chapitre, nous avons évalué les performances de notre protocole en la comparant avec les protocoles d'authentification existantes .Nous avons varié la taille de la clé et constater l'évolution du temps d'exécution.

Les résultats obtenus montrent que notre protocole présente une haute performance en terme de temps d'exécution, il est très rapide et ne consomme pas d'espace mémoire et son Overhead est léger ce que lui permet d'être idéal pour les dispositifs mobile à faibles ressources.

Conclusion générale et perspectives

L'usage de la biométrie s'est vite étendue dans de nombreuses applications destinées à gérer l'accès à des ressources physiques (aéroports, laboratoire, etc.) et logiques (ordinateurs, comptes bancaires, etc.). La biométrie est un terme dont on entend de plus en plus parler dans la vie quotidienne. Cependant, elle n'est pas vraiment récente, son apparition remonte au 19ème siècle. Elle est définie comme l'art qui vise à identifier un individu d'une manière unique à partir de ses caractéristiques physiques, ou, un ensemble de technologies qui exploitent des caractéristiques biologiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et un geste de main pour différencier des personnes. Ses caractéristiques sont traitées par certains ordres de processus automatisés à l'aide de dispositifs comme des modules de balayage, des appareils-photo ou des capteurs d'empreintes digitales. Les caractéristiques de ces empreintes attirèrent l'attention de la communauté scientifique qui s'intéresse à l'utilisation de celles-ci pour l'identification des personnes.

Plusieurs systèmes d'authentification à base d'empreinte digitale ont été proposés, cependant la plupart souffrent de problèmes de stockage et d'utilisation des données biométriques. En effet, l'optimisation de l'utilisation de l'empreinte digitale dans un système d'authentification nécessite de déterminer les bonnes techniques pour la manipulation de ces empreintes.

Dans notre protocole, nous avons utilisé le concept de l'empreinte digitale pour authentifier les patients, utilisateurs de réseau corporel BANet (Body Area Network), sur leurs smartphones. Pour une bonne manipulation des données biométriques connues par leur taille considérable et dans le but de réduire l'espace mémoire quelles requises, de minimi-

ser le temps d'exécution du traitement et de réduire l'Overhead de communication, nous avons opté à utiliser les courbes elliptiques pour la génération de la paire de clés d'un patient à partir de son empreinte digitale et pour la signature, la vérification, le chiffrement et le déchiffrement des messages échangés entre le patient et le serveur de traitement.

Pour la validation de notre proposition nous avons implémenté un prototype sous Java. Les scénarios d'évaluation de performances et les résultats de comparaisons de notre protocole avec d'autres solutions ont montré que notre solution offre de meilleures performances en matière de : charge de communication qui est réduit grâce à l'utilisation de condensés de hachage dans les échanges et en termes aussi de temps d'exécution avec l'utilisation des courbes elliptiques.

En guise de perspectives, nous envisageons en premier lieu l'intégration de notre protocole sur des dispositifs mobiles réels. Une autre perspective que nous jugeons intéressante serait de résoudre le problème de " variabilité de l'empreinte digitale ". En effet, parfois l'acquisition de l'empreinte peut générer de fausses valeurs d'identification, due principalement à des facteurs extérieurs du système qui dépondent principalement de la manière avec laquelle les doigts sont posés ou de leur degré d'humidité. La génération d'une fausse donnée d'identification génère une fausse clé et ainsi un rejet d'authentification par le serveur de traitement malgré la légitimité éventuelle de l'utilisateur. Nous avons réfléchi à un début de solution qui peut résoudre cette problématique et qui nécessite d'être étudiée. Elle consiste à l'étude du degré de variabilité par un utilisateur et lier toute la plage de valeurs possibles à son empreinte digitale. Cette démarche peut résoudre le problème de faux rejets à condition que la plage de valeur ne chevauche pas avec une plage de variation d'un autre utilisateur.

Bibliographie

[1] R. Belguechi, T. Le-goff, E. Cherrier, C. Rosenberger Study of the robustness of a cancelable biometric system, Manuscrit auteur, publié dans une conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information, 2014.

[2] Aude Plateaux, Solutions opérationnelles d'une transaction électronique sécurisée et respectueuse de la vie privée, thèse pour l'obtention de grade doctorat de l'université de Caen Basse-Normandie. 2014.

[3] Farid Benhammadi, Kadda Beghdad Bey, Password hardened fuzzy vault for fingerprint authentication system, publié par Image and Vision Computing, 2014.

[4] Eun-Jun Yoon et Kee-Young Yoo, A Biometric-based Authenticated Key Agreement Scheme using ECC for Wireless Sensor Networks, article publié par Computer-Communication Networks, 2014.

[5] Muhammad Khurram Khan1 and Saru Kumari, An Improved User Authentication Protocol for Healthcare Services via Wireless Medical Sensor Networks, publié par Hindawi Publishing Corporation ; 2014.

[6] Yanbo Shou Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs, thése d'obtenir le grade de doctorat de l'Université de Franche-Comté 2014.

[7] Eun-Jun Yoon et Kee-Young Yoo, A New Fingerprint Biometric Remote User Authentication Scheme Using Chaotic Hash Function On Mobile Devices, article publie par Intelligent Automation and Soft Computing, 2013.

[8] Kamel Aloui, Caractérisation du cerveau humain : application à la biométrie, publié par archives-ouvertes, 2013.

[9] Samer Chantaf, Biometrie par signaux physiologiques, publié par archives-ouvertes, 2013.

[10] A. Plateaux and P. Lacharme and A. Jøsang and C. Rosenberger, Biométrie à usage unique pour la monétique, article publie par Laboratoire GREYC de Caen (France), 2013.

[11] Mahammedi Nadjiba, Mahdadi Houda, Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques Fp et F2n, Thèse d'obtention du grade de Master à l'université de Kadsi Merbah Ouargla, 2013.

[12] SK Hafizul Islam , G.P. Biswas, Design of improved password authentication and update scheme based on elliptic curve cryptography, publié par Mathematical and Computer Modelling, 2013.

[13] Samuel GRAU, Courbes Elliptiques, Implémentation de la Signature Electronique, Thèse d'obtention du grade de doctorat à l'Université de Rouen, 2013.

[14] Juan Gabriel Barros Gavilanes, Réseaux de capteurs pour applications de suivi médical, Thèse d'obtention du grade de doctorat à l'Université de Toulouse, 2013.

[15] Ahmed Zaid Aghiles, Segmentation d'image appliquée en biométrie : cas des images d'iris, Thèse d'obtention du grade de Magistère à l'Université de Mouloud Mammeri, Tizi Ouzou, 2013.

[16] Qiuyan lin, Woongryul leon, Changwhan Lee, Youngchul Choi, and Dongho Won ; Fingerprint-based user authentication scheme for home healthcare system, publié par IEEE, 2013.

[17] Xin Liu, Yongjun Shen, Shuxian Li and Fenglan Chen, A Fingerprint-based User Authentication Protocol with One-time Password for Wireless Sensor Networks, International Conference on Sensor Network Security Technology and Privacy Communication System, 2013.

[18] Ashok Kumar Das et Bezawada Bruhadeshwar, A Biometric-Based User Authentication Scheme for Heterogeneous Wireless Sensor Networks, International Conference on Advanced Information Networking and Applications Workshops, 2013.

[19] Ohood Althobaiti, Mznah Al-Rodhaan, and Abdullah Al-Dhelaan, An Efficient Biometric Authentication Protocol for Wireless Sensor Networks, publié par Hindawi Publishing Corporation, 2013.

[20] Muhammad Khurram Khan, Saru Kumari et Mridul K.Gupta, More efficient key-hash based fingerprint remote authentication scheme using mobile device, Springer-Verlag Wien, 2013.

[21] Demba SOW, Courbes elliptiques, Cryptographie à clés publiques et Protocoles d'échange de clés, Thèse d'obtention du grade de Doctorat, 2013.

[22] V. Gayoso Martnez et L. Hernandez Encinas, Implementing ECC with Java Standard Edition 7 International Journal of Computer Science and Artificial Intelligence, 2013.

[23] Thomas De Pujo et Alexy Roger, Panorama des algorithmes de cryptage de l'information, rapport du projet de veille technologique effectué au sein de l'Ecole Centrale de Nantes et traitant des algorithmes de chiffrement de l'information, 2013.

[24] Mohammedi Mohamed et Moulai Lila, Proposition d'une stratégie MIMO (2_2) coopérative pour les Réseaux de capteurs sans fil, mémoire de fin d'étude Master 2 en informatique, 2013.

[25] Labraoui Nabila,La sécurité dans les réseaux sans fil AD HOC, thèse pour l'obtention de grade doctorat de l'université de TLEMCEN, 2012.

[26] Lahoucine Ballihi, Biométrie faciale 3D par apprentissage des caractéristiques géométriques : Application à la reconnaissance des visages et à la classification du genre, thèse pour l'obtention de grade doctorat Université Lille, 2012.

[27] Eun-Jun Yoon, Sung-Bae Choi et Kee-Young Yoo ; A Secure And Efficiency Id-Based Authentication Key Agreement Scheme Based On Elliptic Curve Cryptosystem For Mobile Devices, publié par International Journal of Innovative Computing, Information and Control, 2012.

[28] Chen CL, Lee CC, Hsu CY ,Mobile device integration of a fingerprint biometric remote authentication scheme, 2012.

[29] Truong TT, Tran MT, Duong AD Robust mobile device integration of a fingerprint biometric remote authentication scheme, publié par Proceedings of 26th IEEE International Conference on Advanced Information Networking and Applications, pp 678-685, 2012.

[30] Berbar Nassima et Benkerrou Hayet, Protocole hiérarchique basé sur lévaluation de la redondance pour la garantie de la couverture dans les réseaux de capteurs sans fil,

mémoire de fin de cycle en vue dobtention du diplôme de master recherche à l'Université A/Mira de Béjaïa, 2013.

[31] M. Mohamad El Abed, Evaluation de systèmes biométriques, Thèse d'obtention du grade de doctorat, 2011.

[32] Akrouf Samir, Une Approche Multimodale pour l'Identification du Locuteur, thèse d'obtention du grade de doctorat, 2011.

[33] Youssouf Zatout, Conception et évaluation de performances d'un réseau de capteurs sans fil hétérogène pour une application domotique, Thèse d'obtention du grade de doctorat, 2011.

[34] Noureddine Chikouche, Foudil Cherif et Mohamed Benmohammed, Conception et Vérification d'un Protocole d'Authentification de Système Combiné RFID-Biométrique, 2011.

[35] D.Bennet et S.Arumugaperumal, Fingerprint Based Multi-Server Authentication System, publié par IEEE, 2011.

[36] E.-J.Yoon et K.-Y.Yoo, A new biometric-based user authentication scheme without using password for wireless sensor networks, publié par Proceedings of the 20th IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises, pp. 279-284, Paris, France, 2011.

[37] Kai Xi et Tohari Ahmad, Fengling Han and Jiankun Hu A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment, 2010.

[38] Samir Athmani, Protocole de sécurité Pour les Réseaux de capteurs Sans Fil, Thèse d'obtention du grade de Magistère à l'Université Hadj Lakhder Batna, 2010.

[39] Charles De Clercq, Aurélien Greuet, Cryptographie symétrique, courbes elliptiques et échanges de clés sécurises, 2010.

[40] Yuan Jianjun, Jiang Changjun, Jiang Zuowen, A Biometric-Based User Authentication for Wireless Sensor Networks, Wuhan University et Springer-Verlag Berlin Heidelberg, 2010.

[41] Liu Wei, Zhou Cong, Ye Zhiwei, Fingerprint Based Identity Authentication for Online Examination System, publié par Second International Workshop on Education Technology and Computer Science, 2010.

[42] Aqeel Khalique, Kuldip Singh et Sandeep Sood, Implementation of Elliptic Curve Digital Signature Algorithm, department d'Electronics et Computer Engineering, Indian Institute of Technology Roorkee Roorkee India, 2010.

[43] x.y Liu, TL. Huang, X. Wang, X.l Tang, A User Authentication Scheme Based On Dynamic Password for Wireless Sensor Networks, publié par IEEE Intelligent Computing and Integrated Systems (ICISS), International Conference, 2010.

[44] Géraldine Vache Marconato, Évaluation quantitative de la sécurité informatique : approche par les vulnérabilités, thèse pour l'obtention de grade de doctorat de l'université de Toulouse, 2009.

[45] J. Bhatnagar et A.Kumar, On estimating performance indices for biometric identification, publié par Pattern Recognition, Vol.42, pp.1803-1815, 2009.

[46] Bruno Winckler, Les courbes elliptiques, théorème de Mordell-Weil, mémoire de fin d'étude de magistère, 2009.

[47] Lorène Allano, La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles, Thèse d'otention de grade de doctorat de l'Institut National des Telecommunications, 2009.

[48] DE-Song Wang, Jian-Ping Li, A New Fingerprint-Based Remote User Authentication Scheme Using Mobile Devices, publié par IEEE, 2009.

[49] Guy Gogniat, Cryptographie matérielle, publié dans le séminaire de Laboratoire Lab-STICC CNRS, UMR 3192 Université de Bretagne Sud-UEB, 2009.

[50] Préposé fédéral à la protection des données et à la transparence PFPDT, Guide relatif aux systèmes de reconnaissance biométrique, 2009.

[51] Anthony Larcher, Modèles acoustiques à structure temporelle renforcée pour la vérification du locuteur embarquée, thèse en vue de l'obtention de grade du doctorat de l'université d'Avignon et des Pays de Vaucluse, 2009.

[52] ISO/IEC FCD 19792. Information technology - security techniques - security evaluation of biometrics, 2008.

[53] Souhila guerdi ababase, Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D, thèse en vue de l'obtention du doctorat l'université D'Evry Val D'Essonne, 2008.

[54] Julien Bringer, Bruno Kindar, Malika Izabachène, David Pointcheval, Qiang Tang, Sebastien Zimmerji, Gèrard Cohen et Gilles Zèmor, C2 (Codage, Cryptographie) et Biométrie, Conférence de la Journées Codage et Cryptographie à Carcans, 2008.

[55] M. K. Khan, Z. Jiashu, and X. M. Wang ; Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices ; 2008.

[56] TH. Lee, Simple Dynamic User Authentication Protocols for Wireless Sensor Networks, The 2nd International Conference on Sensor Technologies and Application (SEN-SORCOMM'08), IEEE Computer Society, 2008.

[57] V. Viet Triem Tong, H. Sibert, J. Lecoeur et M. Girault, FingerKey, un cryptosystème biométrique pour l'authentification, Conférence sur la Sécurité et Architectures Réseaux, 2007.

[58] Stéphane Ballet et Alexis Bonecaze, Courbes Elliptiques Application à la Cryptographie, Cours de Cryptographie Avancée, Ecole Polytech de Marseille ; 2007.

[59] Yoon E.J., and Yoo K.Y., A secure chaotic hash-based biometric remote user authentication scheme using mobile devices, APWeb/WAIM, Huang Shan, pp. 612-623, 2007.

[60] H.R. Tseng, R.H. Jan, W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks, publié par IEEE Global Communications Conference (GLOBECOM'07), 2007.

[61] ISO/IEC 19795-1, Information technology - biometric performance testing and reporting - part 1 Principles and framework, 2006.

[62] Hägler Michael, Courbes elliptiques et cryptographie, cours de magistère sur les courbes elliptiques. 2006.

[63] Pascal Joyeux, La biométrie Ses différentes techniques, thèse de préparation au probatoire d'ingénieur CNAM aux Conservatoire National des Arts et Métiers ajouté Centre de Lyon-Rhône-Alpes, 2006.

[64] Rima Belguechi, Contribution A La Reconnaissance D'Empreintes Digitales Par Une Approuche Hybride, Mémoire de fin d'étude présenté pour l'obtention du diplôme de Magistère à l'Institut National de formation en Informatique, 2006.

[65] K.H.M. Wong, Y Zheng, IN. Cao, S.w. Wang, A Dynamic User Authentication Scheme for Wireless Sensor Networks, publié par IEEE International Conference on

Sensor Networks, Ubiquitous, and Trust worthy Computing (SUTC'06), IEEE Computer Society, 2006.

[66] Scott Vanstone, Deployments of Elliptic Curve Cryptography, cours de magistère à l'université de Waterloo, 2005.

[67] Z. Benenson, N. Gedicke, and O. Raivio, Realizing robust user authentication in sensor networks, publié par Real-WorldWireless Sensor Networks (REALWSN), vol. 14, 2005.

[68] Lyes Khelladi et Nadjib Badache, Les réseaux de capteurs : état de l'art, Rapport de recherche de Laboratoire des Logiciels de Base, CERIST, 2004.

[69] Kristin Lauter, The Advantages of Elliptic Curve Cryptography for Wireless Security, article publié par IEEE Wireless Communications.2004.

[70] Watro R, Kong D, Cuti S, et al. TinyPK : Securing sensor networks with public key technology[C]//ACM Workshop Security of Ad Hoc Sensor Networks, publié par Washington D C : ACM Press, 2004.

[71] Florent Perronnin et Jean-Luc Dugelay, Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo, 2002.

[72] Don Johnson, Alfred Menezes et Scott Vanstone, The elliptic curve digital signature algorithm (ecdsa), publié par International Journal of Information Security, 1(1) :36-63, 2001.

[73] P.Philips, A.Matrin, C.Wilson et M.Przyboky. An Introduction to Evaluating Biometric Systems, publié par Computer, Vol 33 No 2 pp56-63, 2000.

[74] Ari Juels and Martin Wattenberg, A fuzzy commitment scheme, In CCS '99 : Proceedings of the 6th ACM conference on Computer and communications security, pages 28-36, New York, NY, USA, 1999.

[75] René Schoolf, Elliptic curves over finite fields and the computation of square root, publié par Mathematics of Computation, Vol.44, N°382, 1985.

Annexe

Génération de l'identifiat

```
public String uniqueid () {
             String ch="" ;
             ch =  id().toString();
            for (int i = 0; i <ch.length(); i++) {
                  if (ch.charAt(i)=='a') {
                        ch=ch.replace('a', '1');
                  }  if (ch.charAt(i)=='b') {
                        ch=ch.replace('b', '2');
                  }if (ch.charAt(i)=='c') {
                        ch=ch.replace('c', '3');
                  }if (ch.charAt(i)=='d') {
                        ch=ch.replace('d', '4');
                  }if (ch.charAt(i)=='e') {
                        ch=ch.replace('e', '5');
                  }if (ch.charAt(i)=='f') {
                        ch=ch.replace('f', '6');
                  }else {
                        ch=ch.replace('-', '7');
                  } {
                  }
            }
      return ch;
                  }
      public UUID id() {
            UUID uniqueKey = UUID.randomUUID();
                  return uniqueKey;
      }
```

Récupération et hachage de l'empriente digitale

```
      File fnew=new File("012_5_1.jpg");
      String emp="";
public String hacheimage() throws IOException, NoSuchAlgorithmException {

           BufferedImage originalImage=ImageIO.read (fnew);
           ByteArrayOutputStream baos=new ByteArrayOutputStream ();
           ImageIO.write (originalImage, "jpg", baos);
           byte[] imageInByte=baos.toByteArray();

           MessageDigest md = MessageDigest.getInstance("MD5");
           md.update((byte) imageInByte.length);

           byte[] byteData = md.digest();

           StringBuffer hexString = new StringBuffer();
           for (int i=0;i<byteData.length;i++) {
                 String hex=Integer.toHexString(0xff & byteData[i]);
                 if(hex.length()==1) hexString.append('0');
                 hexString.append(hex);
           }

      emp=hexString.toString();
           return emp;

     }
```

Génération de la clé privée

```
          static String Ns = "357318069660970";

       public String concaténation(String id, String ns, String e) {

                 return id+ns+e;

            }
            String s="";
      public  String hacheclé() throws NoSuchAlgorithmException, IOException {
                       principale pr=new principale();
                       s=pr.uniqueid()+Ns+pr.hacheimage();
                MessageDigest m = MessageDigest.getInstance("MD5");
                 m.update(s.getBytes(),0,s.length());
                 String res=new BigInteger(1,m.digest()).toString(16);

                 return res;

            }
```

Génération des paramètres de la courbe elliptique et la clé publique

```
public static String toHex(byte[] data) {
                StringBuilder sb = new StringBuilder();
                for (byte b: data) {
                  sb.append(String.format("%02x", b&0xff));
                }
                return sb.toString();
              }
       String ec="";
public String  EC(String privatekey) throws NoSuchAlgorithmException,
IOException {

      X9ECParameters ecp = SECNamedCurves.getByName("secp192r1");
      ECDomainParameters domainParams = new
      ECDomainParameters(ecp.getCurve(),
                         ecp.getG(), ecp.getN(), ecp.getH(),
                         ecp.getSeed());

      ECKeyGenerationParameters keyGenParams = new
                                       ECKeyGenerationParameters
                                      (domainParams, new SecureRandom());

      ECKeyPairGenerator generator = new ECKeyPairGenerator();
                                     generator.init(keyGenParams);

      byte[] b =hacheclé().getBytes();

      ECPoint Q = domainParams.getG().multiply(new BigInteger(b));

      System.out.println( toHex(Q.getEncoded(true)));

      return ec;
                        }
```

Signature et vérification de la signature du méssage

```
public static byte[] signPlainText(String plainText, PrivateKey privateKey)
                     throws SignatureException, InvalidKeyException,
                     NoSuchAlgorithmException, NoSuchProviderException
      {

            return signPlainBytes(plainText.getBytes(), privateKey);
      }

public static byte[] signPlainBytes(byte[] plainBytes, PrivateKey privateKey)
                     throws SignatureException, NoSuchAlgorithmException,
                     NoSuchProviderException, InvalidKeyException
     {
            Signature signature = Signature.getInstance("ECDSA", "BC");
            signature.initSign(privateKey, new SecureRandom());
            signature.update(plainBytes);
            byte[] signBytes = signature.sign();

        return signBytes;
      }

public static boolean verifySignature(String plainText, byte[] signBytes,
                     PublicKey publicKey) throws InvalidKeyException,
                     SignatureException, NoSuchAlgorithmException,
                     NoSuchProviderException
     {
      return verifySignature(plainText.getBytes(), signBytes, publicKey);
      }

public static boolean verifySignature(byte[] plainBytes, byte[] signBytes,
                    PublicKey publicKey) throws InvalidKeyException,
                    SignatureException, NoSuchAlgorithmException,
                    NoSuchProviderException
      {
            Signature signature = Signature.getInstance("ECDSA", "BC");
            signature.initVerify(publicKey);
            signature.update(plainBytes);

            return signature.verify(signBytes);
      }
}
```

Chiffrment et déchiffrement du méssage

```
public final class ECEncryptor {

  public boolean encryptEC192(ECPublicKey pubKey, byte[] input, byte[] output)
                              throws InvalidCipherTextException
      {

            bc.init(true, publicParam);

      System.out.println("InputBS: " + bc.getInputBlockSize() + " OutputBS: "+
                          bc.getOutputBlockSize() + "\n");
                          bc.processBytes(input, 0, input.length);

      output = bc.doFinal();

            return true;
      }

  public boolean decryptEC192(ECPrivateKey privKey, byte[] input, byte[]
                              output) throws InvalidCipherTextException
      {
            bc.init( false, privParam);
      System.out.println("InputBS: " + bc.getInputBlockSize() + " OutputBS: "
                         + bc.getOutputBlockSize() + "\n");
                          bc.processBytes(input, 0, input.length);

      output = bc.doFinal();

          return true;
      }
}
```

Le programme principale

```
public static void main(String[] args) throws IOException,
                                        GeneralSecurityException {


principale pr=new principale();

System.out.println("le temps est :" +  pr.temp ()+ " S");
System.out.println("L'unique identifiant:");
System.out.println(pr.uniqueid());
System.out.println("L'image hachée:");
System.out.println(pr.hacheimage());
System.out.println("La concaténation est:");
System.out.println(pr.uniqueid()+Ns+pr.hacheimage());
System.out.println("la clé privée est:");
System.out.println(pr.hacheclé());
System.out.println("la clé publique a partir de la clé privée: ");
System.out.println(pr.EC(pr.hacheclé()));

String plainText = "University of A.Mira - Bejaia";

byte[] signBytes = principale.signPlainText(plainText,
                   principale.GenerateKeys().getPrivate());

System.out.println ("Le message signé est : ");
System.out.println(toHex(signBytes));
System.out.println("le paquet à envoyer est: ");
System.out.println(pr.uniqueid()+ pr.temp()+plainText+pr.toHex(signBytes));
System.out.println("le message chiffré est :");
System.out.println(toHex(signBytes));
System.out.println("le déchiffrement du message est fait !");
System.out.println("la vérification du temps est faite");
System.out.println("l'identificateur reçu est identique avec celui du
patient !");


boolean verification = principale.verifySignature(plainText, signBytes,
                            principale.GenerateKeys().getPublic());

System.out.println("La vérification de la signature : "+verification);
System.out.println("le temps est :" +  pr.temp ()+ " S");

      }

      }
```

Résumé

Bien que la problématique d'authentification dans les réseaux à faibles ressources soit largement abordée, les exigences des applications en matière de fiabilité, sûreté et de rapidité laissent cette problématique toujours à la recherche d'une résolution optimale. Notre contribution combine l'usage de la biométrie et de la cryptographie. Elle hérite à la fois de la biométrie l'unicité et la fiabilité en matière d'authentification et de la cryptographie la fiabilité en termes de performances en temps d'exécution, communication et stockage. Nous avons développé un prototype de notre protocole sous Java. Une évaluation de performances est menée avec comparaison à des travaux de la littérature et dans laquelle notre protocole présente de meilleurs résultats.

Mots clés : Biométrie, cryptographie à courbes élliptiques, authentification, réseaux à faibles ressources.

Abstract

Although the authentication issue on resource-limited networks is widely addressed, the application requirements for reliability, safety and speed leave this problematic still in research activity. Our contribution combines the use of the biometry and cryptography mechanisms. It inherits from the biometry the uniqueness and the reliability in terms of authentication and from the cryptography the reliability in terms of execution time, communication and storage. We have developed a prototype of our protocol in Java. A performance evaluation is conducted with comparison to some protocols, where our protocol shows the best results.

Key words : Biometry, elliptic curve cryptography, authentication, resource-limited networks.