الجمهـوريـــة الجزائـــريـــة الديمقـــراطيـــة الشـعبيـــة
République Algérienne Démocratique et Populaire
وزارة التـــعلـــيـــم العـــالـــي والبـحـــث العـلمـــي
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

جامعة وهران 2 محمد بن أ حمد
Universitéd'Oran 2 Mohamed Ben Ahmed

معهد الصيانة و الأمن الصناعي
Institut de Maintenance et de Sécurité Industrielle

Département De Maintenance en Electromécanique

MÉMOIRE

Pour l'obtention du diplôme de Master

Filière : Electromécanique
Spécialité : Electromécanique Industrielle

Thème

Simulation D'un Système RFID Pour Authentification Par Badges Electroniques

Présenté et soutenu publiquement par :

Cherifi Oualid et Loumir Oussama

Devant le jury composé de :

Nom et Prénom	Grade	Etablissement	Qualité
CHENNOUFI Mohamed	MCB	Université d'Oran 2	**Président**
ROUAN-SERIK Mehdi	MCB	Université d'Oran 2	**Encadreur**
ADJELOUA Abd el aziz	MAA	Université d'Oran 2	**Examinateur**

Année 2019/2020

Dédicaces

Je dédie ce modeste travail

A

Mon très cher père et ma très chère mère pour leur soutien, leurs sacrifices et les efforts qu'ils ont déployés pour mon éducation ainsi que ma formation.

A

Mes chers frères pour leur affection, compréhension et patience.

A

Tous mes amis d'enfance et du long parcours scolaire et universitaire.

CHERIFI OAULID

Je dédie ce modeste travail et ma profonde gratitude

A

Mes chers parents, pour tous les sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études.

A

Mes chers frères pour leurs appuis et leur encouragement tout au long de mon parcours universitaire.

A

Mes chers amis pour leur soutien permanent.

LOUMIR OUSSAMA

Remerciements

Nous remercions tout d'abord Dieu le tout puissant qui nous a accordé la volonté et le courage pour l'accomplissement de ce travail. Al Hamdoulillah, qui nous a offert la force de réaliser beaucoup de choses au-delà de nos capacités normales.

Nous exprimons nos remerciements avec un grand plaisir et un grand respect à notre encadreur Monsieur Mehdi Rouan-Serik qui nous a proposé le sujet de ce mémoire, pour sa patience, sa disponibilité tout au long de la réalisation de ce travail et surtout ses judicieux conseils, nous ne le remercions jamais assez, grâce à lui nous avons pu réaliser ce travail.

Nous remercions également tous nos professeurs pendant notre cursus universitaire au sein de l'institut de maintenance et de sécurité industrielle pour leur soutien et leur accueil chaleureux et sympathique.

Nous tenons à remercier également les membres du jury pour avoir accepté d'examiner ce travail.

Enfin, nous adressons nos plus sincères remerciements à nos parents, nos proches et nos amis pour leur contribution et leur soutien.

Merci à vous tous

Résumé

Ce mémoire présente une étude sur la technologie d'identification par radiofréquence (RFID) qui a apporté des solutions efficaces dans différents domaines, elle permet de tracer les produits et les animaux, d'identifier des personnes, de sécuriser des lieux, etc. La RFID est une méthode permettant de mémoriser et récupérer des données à distance. Le système est activé par un transfert d'énergie électromagnétique entre un tag et un lecteur RFID. Cette technologie est reconnue par son aptitude de la lecture des données sans contact et même sans ligne de vue directe, la rapidité et l'unicité des ID des tags. L'étude décrit la technologie actuelle, y compris les gammes de fréquences utilisées, les normes et les protocoles de communication.L'objectif de cette étude est de pouvoir simuler et concevoir un système de contrôle d'accès par badges RFID.

Mots-clés : Radio Fréquence, RFID, authentification, identification, lecteur, tags.

Abstract

This thesis presents a study on radio frequency identification (RFID) technology that has brought effective solutions in various fields, it allows to trace products and animals, identify people, secure places, etc. RFID is a method for storing and retrieving data remotely. The system is activated by a transfer of electromagnetic energy between a tag and an RFID reader. This technology is recognized by its ability to read data without contact and even without a direct line of sight, the speed and uniqueness of the tag IDs. The study describes the current technology, including the frequency ranges used, standards and communication protocols. The objective of this study is to be able to simulate and design an access control system using RFID badges.

Keywords: Radio Frequency, RFID, authentication, identification, reader, tags.

Table des matières

Chapitre 1 : Généralites Sur RFID

Table des matières

Chapitre 2 : Methodologie D'extraction De L'information Du Capteur

Table des matières

Chapitre 3 : Authentification Par RFID

Table des matières

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des figures

Liste des tableaux

Chapitre 1

Chapitre 2

Introduction générale

La technologie d'identification par radiofréquence le plus souvent désignée par le sigle RFID (Radio Frequency IDentification) est actuellement l'une des technologies d'identification automatique les plus prometteuses dont l'utilisation se répand rapidement. Comme son nom l'indique, le but de la RFID est de permettre l'identification d'objets ou d'individus par des machines. Un système RFID se compose de lecteurs RFID dotés d'antennes, d'ordinateurs hôtes et de tags qui sont reconnus par les lecteurs. Un tag RFID est identifié d'une manière unique par un numéro d'identification stocké dans sa mémoire. Ces identifiants sont spécifiés par des normes internationales.

La technologie RFID a la spécificité de fonctionner à distance (sans contact), selon le principe suivant : un lecteur diffuse un signal radio et reçoit en retour les réponses des tags qui se trouvent dans son champ d'action. Il existe une grande variété de systèmes RFID classés selon différents types de mémoire, différentes fréquences, différentes portées et différents types d'alimentation. Le domaine applicatif de la technologie RFID est tellement vaste que toutes les applications ne peuvent être citées. Nous citons à titre non restrictif, l'authentification, les systèmes de paiement, les systèmes antivols et le suivi de la localisation.

Ce mémoire décrit l'ensemble de nos travaux. Il est constitué de la présente introduction, de quatre chapitres et d'une conclusion. Dans le premier chapitre, nous réalisons une présentation générale de la technologie RFID et ses différents domaines d'application. Nous ferons un descriptif des composants du système RFID, son mode de fonctionnement et les gammes de fréquence utilisées en mettant l'accent sur les défis de la RFID.

Le second chapitre concerne la méthodologie d'extraction de l'information du capteur, description des principes physiques des systèmes RFID, le codage des données et la modulation des signaux. Nous détaillions aussi les mécanismes de couplages et les problèmes techniques dans la RFID.

Le troisième chapitre est consacré à l'authentification par RFID, nous représentons les types d'attaques de base, la méthode de vérification du tag et du lecteur en identifiant les protocoles d'authentification RFID.

Le quatrième chapitre est dédié à la simulation et la conception d'un système de contrôle d'accès à base RFID. Finalement, la conclusion résumera l'ensemble des travaux de cette thèse et présentera les perspectives envisagées.

Chapitre 1

Généralités Sur RFID

Chapitre 1 : Généralités sur RFID

Présentation de chapitre

Le développement rapide et le déploiement des systèmes d'identification par radiofréquence (RFID) pourraient avoir des répercussions sur nombreuses industries et applications différentes. Nous présentons dans ce chapitre une introduction sur la radio-identification, un bref historique de la technologie RFID et les systèmes d'identification automatique aussi les applications répertoriées jusqu'à présent. Nous résumons les caractéristiques principales de cette technologie en décrivant le principe de fonctionnement de la RFID et le rôle de chaque composant et ses normes. Enfin, nous abordons plusieurs défis et obstacles à l'adoption de la RFID, ainsi que les technologies émergentes pertinentes à la RFID.

Sommaire

1.1 Introduction

La radio-identification généralement désignée par l'acronyme RFID (en anglais Radio Frequency Identification), c'est une technologie en plein essor qui a le potentiel pour avoir un impact économique important sur de nombreuses industries. Bien que la RFID soit une technologie relativement ancienne, les progrès les plus récents dans la technologie de fabrication des puces rendent la RFID pratique pour les nouvelles applications et les nouveaux paramètres, en particulier l'identification automatique à distance sans contact ni vision des biens ou des individus en utilisant les ondes radiofréquences.

Les systèmes RFID sont constitués de petits transpondeurs ou tags, fixés sur des supports physiques qui ont la capacité de mémoriser et récupérer automatiquement les données. Les tags RFID pourraient bientôt devenir la micro puce la plus répandue de l'histoire. Il existe de nombreux types de systèmes RFID utilisés dans des applications et des contextes différents. Les systèmes ont des sources d'énergie, des fréquences de fonctionnement et des fonctionnalités différentes. Certaines des applications RFID les plus familières sont l'étiquetage des produits avec des codes électroniques, des cartes de proximité pour le contrôle d'accès physique et les systèmes de paiement sans contact.

Bien que l'adoption de RFID présente de nombreux avantages sur le plan de l'efficacité, elle se heurte encore à plusieurs obstacles. Outre les défis typiques de la mise en œuvre de tout système de technologie de l'information et les obstacles économiques, la sécurité et la protection des renseignements personnels dans les systèmes RFID suscitent de grandes préoccupations, sans une protection adéquate les systèmes RFID pourraient créer de nouvelles menaces pour la sécurité des données.

1.2 Historique

Les origines de la technologie RFID remontent au 19^{e} siècle, lorsque les chercheurs de cette époque ont fait des grands progrès scientifiques dans l'électromagnétisme d'une pertinence particulière pour la RFID. La découverte de l'inductance électronique par Faraday, la formulation des équations décrivant l'électromagnétisme par James Clerk Maxwell, et les expériences de Heinrich Rudolf Hertz validant les prédictions de Faraday et Maxwell ont mis les bases de la radio-identification.

L'un des premiers brevets pour un système d'identification automatique par radiofréquence était un émetteur radio pour la détection des objets conçus par John Logie Baird en 1926 [1] et aussi le brevet de Watson-Watt en 1935 pour un système de "détection et télémétrie radio". La technologie de communication passive utilisée dans la RFID a été présentée pour la première fois dans l'article de Henry Stockman fondateur de "Communication by Means of Reflected Power" en 1948 [1].

L'une des premières applications d'un système d'identification par radiofréquence a été dans les systèmes "Identify Friend or Foe" (IFF) déployés par les forces aériennes de l'armée britannique pendant la seconde guerre mondiale. L'IFF a permis aux opérateurs radar et aux pilotes d'identifier les cibles amies, via des signaux radio-fréquence, donc prévenir les incidents de "tir ami" et intercepter les avions ennemis.

Les activités commerciales de la technologie RFID ont commencé dans les années 1960 grâce aux travaux de Harrington sur la théorie électromagnétique de R.F, dont "Fields Measurements Using Active Scatterers" et "Theory of Loaded Scatterers" [2] publiés en 1963 et 1964 respectivement. Au cours de cette décennie, des équipements électroniques de surveillance des articles (EAS) pour les applications antivols et de sécurité ont été mis au point. Ces systèmes étaient des systèmes 1-bit qui permettaient uniquement de détecter la présence d'objets, plutôt que les identifier.

Dans les années 1960, le laboratoire national de Los Alamos a effectué des travaux plus étroitement liés à la RFID moderne pour explorer le contrôle d'accès. Il a incorporé des tags RFID dans les badges des employés pour identifier automatiquement les personnes, limiter l'accès aux zones sécurisées et rendre plus difficile la falsification des badges. Dans les années 1980, des tags passifs (tags RFID ou transpondeurs) sont apparus, ce qui a permis d'élargir le domaine d'applications de la RFID.

Les années 1990 ont également été importantes pour la RFID, puisqu'elle a commencé à entrer dans le courant dominant des affaires et de la technologie. La RFID a commencé à être utilisée dans les systèmes de péage pour les véhicules, le contrôle d'accès et d'autres applications dans le commerce.

En 2003, la création du standard EPC (Electronic ProductCode) par les associations EAN (Efficient Article Numbering Association), Auto-ID Center, UCC (Uniform Code Council) intégrant les technologies RFID et l'internet pour mettre en place le réseau de traçabilité des objets [3].

En 2010-2013, il a été prévu dans le projet de loi américain sur la santé, création d'un registre national d'identification, pour un meilleur suivi des patients en ayant toutes les informations relatives à leur santé.

1.3 Applications de la RFID

Avant de passer à une discussion plus détaillée sur les diverses technologies et principes de la RFID, nous résumerons les applications actuelles et futures de la RFID :

1.3.1 Authentification

À des fins d'authentification, la RFID est utilisée pour fournir des mécanismes d'identification sécurisés pour les personnes et les objets. Les exemples importants d'authentification personnelle sont les badges de contrôle d'accès, les cartes de système de transport, les passeports électroniques et les cartes d'identité. Les domaines actuels d'application de l'authentification des objets comprennent le marquage des médicaments dans le secteur pharmaceutique et des produits de grande valeur dans le secteur du luxe pour prévenir la contrefaçon.

1.3.2 Les systèmes de paiement

La technologie RFID est utilisée dans les systèmes de paiement pour sécuriser les transactions, les exigences de sécurité pour les tags sont très élevées. Les systèmes sont également caractérisés par une portée de lecture très faible pour éviter l'interférence des cartes de paiement, la RFID est utilisé aussi dans les systèmes de péage électronique.

1.3.3 Affichage automatique des informations

Dans le domaine émergent de l'affichage automatique de l'information, les éléments sontétiquetés pour fournir des informations supplémentaires sur les produits et services lorsqu'ils sont lus, les premières applications peuvent être trouvées au point de vente ou dans le secteur public, par exemple, dans les musées.

1.3.4 Systèmes antivols

Les tags RFID au niveau des produits sont utilisés pour prévenir le vol tout au long de la chaîne d'approvisionnement ou sur le point de vente, dans ce cas, on utilise des systèmes RFID bas de gamme (par exemple des tags à 1 bit). Les applications de lutte contre le vol dans la vente par correspondance des produits de grande valeur comme les téléphones portables utilisent des tags plus sophistiqués.

1.3.5 Suivi de la localisation

La technologie RFID est incluse dans le contrôle de la circulation et la gestion du stationnement et aussi dans la surveillance et suivi de la faune et du bétail.

1.3.6 Santé

L'étiquetage RFID est utilisé pour la transfusion et l'analyse du sang, un tag RFID peut être fixé sur un bracelet qui contient des informations sur un patient spécifique, un lecteur sans fil communique avec le tag et les informations qu'il contient apparaissent sur l'écran de l'appareil mobile du consultant.

1.4 Les composants du système RFID

Les discussions sur la technologie RFID ont tendance à se concentrer uniquement sur les dispositifs d'étiquetage, il est plus précis de voir la RFID comme un système complet qui comprend non seulement des tags, mais aussi d'autres composants.

Les systèmes RFID sont composés d'au moins de trois éléments principaux :

- Les tags RFID contiennent des données permettant d'identifier les objets.
- Les lecteurs RFID, ou émetteurs-récepteurs, lisent et écrivent les données des tags.
- Les bases de données pour l'enregistrement des données d'identification des tags.

1.4.1 Le tag (étiquette)

Les tags ou transpondeurs sont attachés à tous les objets à identifier dans un système RFID. Un tag est généralement composé d'une antenne ou d'un élément de couplage pour transmettre et recevoir des signaux et d'un circuit intégré pour stocker et traiter les informations. L'assemblage est emballé pour être plus résistif aux conditions dans lesquelles il fonctionnera. La distinction qui sera discutée plus tard est la source d'alimentation d'un tag. Souvent, les tags n'ont pas de source d'alimentation et doit recueillir passivement toute l'énergie d'un signal radio-fréquence. Les tags RFID sont également dotés d'une mémoire non volatile, qui comprend une logique programmable ou fixe pour les données du capteur et leur transmission.

Les informations contenues dans un tag RFID sont considérées comme un identificateur unique (UII, Unique Item Identifier ou code EPC, Electronic Product Code, etc.). Une fois que cet identifiant a été écrit dans le circuit électronique, il ne peut plus être modifié, seulement lu. (Ce principe est appelé WORM Write Once Read Multiple), certaines puces électroniques ont une autre mémoire dans laquelle les utilisateurs peuvent écrire, modifier et effacer leurs propres données, la taille de ces mémoires varie de quelques bits à des dizaines de kilobits [4]. Les tags peuvent être de différents types comme le montre la figure 1.

Figure 1-1 : Différents types de tags RFID

1.4.2 Le lecteur

Le deuxième élément de base d'un système RFID est l'interrogateur ou le lecteur, le terme "lecteur" techniquement est impropre, les unités de lecture sont des émetteurs-récepteurs (c'est-à-dire un émetteur et un récepteur combinés). Mais, comme leur rôle habituel est d'interroger un tag et d'en recevoir des données par un canal radio-fréquence, ils sont considérés comme "lecteur du tag ». Le lecteur peut avoir une antenne intégrée, comme il peut être séparé.

L'objectif principal d'un lecteur RFID est de transmettre et recevoir des signaux, en transformant les ondes radio provenant des tags en un format que les ordinateurs peuvent lire. Les lecteurs viennent sous de nombreuses formes comme le montre la figure 2 et opèrent sur de nombreuses fréquences différentes et offrent une large gamme de fonctionnalités. Ils peuvent avoir leur propre puissance de traitement et de stockage interne et également être intégrés à des appareils mobiles portatifs.

Figure 1-2 : Différents types des lecteurs RFID

1.4.3 Antenne

Un élément qui est souvent intégré dans le tag et le lecteur RFID, l'antenne permet la réception des données et la transmission des informations.

1.4.4 Logiciel RFID

Un middleware RFID gère les lecteurs et les données brutes provenant des tags, et les transmet au un système de base principal des données. Il facilite la communication entre les lecteurs RFID et le système de base, il permet également de collecter, filtrer, agréger et appliquer des règles sur les données reçues des lecteurs. Logiciel RFID est également chargé de fournir la gestion et le contrôle des fonctionnalités, en veillant à ce que les lecteurs soient connectés, fonctionnent correctement et soient configurés correctement. Les logiciels peuvent être mis en œuvre sur un ordinateur hôte, un serveur centralisé ou sur des lecteurs intelligents.

1.5 Bref descriptif du mode de fonctionnement

À un niveau simple, la technologie RFID est basée sur l'émission de champ électromagnétique par le lecteur RFID qui provoque l'activation des tags situés dans le champ de lecture, les tags RFID contiennent un circuit intégré et une antenne, qui sont utilisés pour transmettre des données au lecteur, ce dernier convertit ensuite les ondes radio reçues en une forme de données plus utilisable.

Les informations recueillies à partir des tags sont ensuite transférées par une interface de communication à un système informatique hôte, où les informations peuvent être stockées dans la base de données et analysées ultérieurement. La lecture des tags par la technologie RFID est à distance même sans ligne de vue directe et peut traverser de fines couches de matériaux.

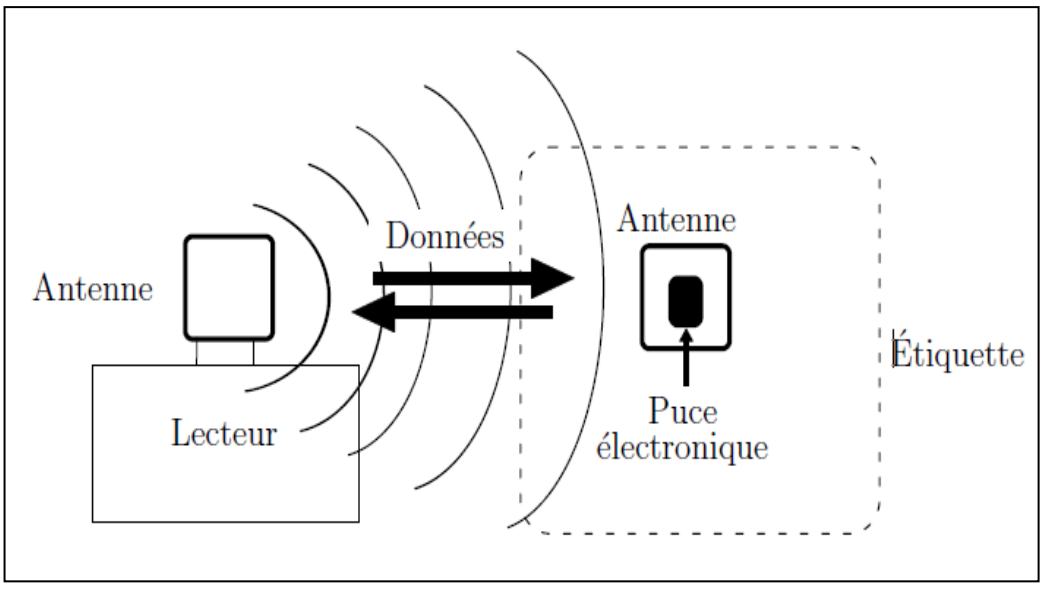


Figure 1-3 : Principe de fonctionnement RFID

1.6 Classification des tags RFID

Les différences fondamentales entre les types de tags sont la présence d'une source d'alimentation, la capacité du stockage, le taux de transfert, la portée, la taille et le prix.

1.6.1 Les tags actifs

Ce sont des tags ayant un émetteur et leur propre source d'énergie, qui est généralement sous la forme d'une pile ou d'une batterie interne. La source d'énergie est utilisée pour déclencher les circuits de micro-puce et l'envoi du signal au lecteur pour capturer les signaux transmis à partir des tags. Les tags actifs parce qu'ils n'ont pas besoin d'être alimentés par le lecteur, ils ne sont pas limités à fonctionner dans un champ proche. Ils peuvent être interrogés et répondre à des longues distances, ils sont donc en particulier pour le suivi des biens de grande valeur, qui doivent être surveillés sur des longues distances.

- **Les avantages**

  - Une distance de portée et de communication élevée.
  - Grande capacité de stockage.
  - Nombreuses fonctions supplémentaires.
  - La rapidité de transmission des données.

- **Les inconvénients**

  - Le coût des tags actifs est très élevé.
  - Une durée de vie limitée.
  - Les tags actifs sont énormes et lourds.

1.6.2 Les tags passifs

Les tags RFID passifs ne contiennent ni batterie ni d'autre source d'alimentation, par conséquent, ils doivent attendre un signal d'un lecteur. Le tag passif contient un circuit de résonance capable d'absorber l'énergie de l'antenne du lecteur qui émet des ondes électromagnétiques pour induire le courant dans l'antenne du tag et donc il sera capable de communiquer avec le lecteur. Les tags passifs sont utilisés pour des opérations de routine moins coûteuses.

- **Les avantages**
  - Un coût faible.
  - Une durée de vie importante.
  - Une petite taille.
- **Les inconvénients**
  - Impossibilité de lecture plusieurs tags passifs simultanément.
  - Courte portée qui dépend de champ proche.
  - Moins fiables que les tags actifs et plus fragiles.

1.6.3 Les tags semi-passifs

Les tags semi-passifs sont équipés d'une source d'énergie, souvent une batterie interne qui est utilisée pour faire fonctionner le circuit de la micro-puce mais pas pour diffuser un signal au lecteur. Au niveau de la communication, ces tags agissent comme les tags passifs, ils utilisent l'énergie tirée des ondes électromagnétiques émises par le lecteur pour générer une réponse. Ces tags sont généralement utilisés dans le suivi des produits. Le tableau 1 illustre les principales différences entre les tags actifs, passifs et semi-passifs.

Propriétés	Tag actif	Tag passif	Tag semi-passif
Source d'énergie	Batterie intégré	Aucune batterie (induction électromagnétique)	Batterie intégré
Capacité de stockage	Extensible et variante	512 octets jusqu'à 4 ko	Extensible et variante
Taux de transfert	128 ko/s	1 ko/s	16 ko/s
Distance de lecture	Grande (plus de 100 m)	Petite (de quelques cm à 3m)	Moyenne (plus de 30m)
Le coût	Elevé (15 à 70 €)	Faible (0,15 à 5 €)	Moyen (5 à 15 €)
La taille	Grande	Petite	Grande
Durée de vie	Limitée (3à 8 ans)	Longue (jusqu'à 20 ans)	Limitée (3à 8 ans)

Tableau 1-1 : Comparaison entre les différents types de tags [5]

1.7 Standardisation de la technologie RFID

Le nombre considérable d'applications dans lesquelles la RFID est utilisée et la nécessité d'une interopérabilité entre les différents systèmes exigent une normalisation de la technologie RFID.

L'objectif des normes RFID est de créer une uniformité dans le secteur de la RFID et par conséquent d'améliorer l'efficacité de cette technologie et élargir ses domaines d'application, parmi les nombreux organismes de normalisation existant dans le monde, il convient de mentionner les suivants car elles ont influencé l'industrie de la RFID [2] :

- Organisations internationale de normalisation (ISO).
- Electronic Product Code Global (EPC Global).

1.7.1 International Organizations for Standardization (ISO)

Responsable de générer des standards applicables dans le monde entier, parmi les normes ISO les plus pertinentes, nous pouvons trouver les deux normes pour les systèmes de suivi des animaux qui utilisent une basse fréquence, connu sous les noms ISO 11784 et ISO 11785, des normes pour les cartes d'identité RFID, travaillant à haute fréquence tels que ISO 10536, ISO 14443 et ISO 15693, et enfin les normes pour les technologies RFID AIDC(Automatic identification and data capture) et de gestion des articles, dont certaines ont été publiées récemment en 2004 qui ont devenu très important pour la promotion de la technologie RFID.

Les normes pour RFID AIDC comprennent ISO 15961, ISO 15962, ISO 15963, ISO 18001 pour la gestion des articles RFID et ISO 18000 pour fournir des protocoles de communication communs pour l'utilisation internationale de la RFID. [6]

1.7.2 Electronic Product Code Global (EPC Global)

David Brock, chercheur principal à l'institut du Massachusetts de technologie (MIT) a suggéré l'utilisation d'un numéro unique pour identifier un objet et l'utilisation du réseau pour télécharger les informations de l'objet, à partir de cette idée, le code EPC est devenu un schéma d'identification permettant d'identifier universellement les objets physiques par RFID. Le code EPC possède quatre attributs clés qui permettent une identification unique de chaque objet : l'en-tête, le numéro du gestionnaire EPC, la classe d'objet et le numéro de série de l'objet. Comme le montre la figure 4, ce tag est d'une longueur de 96 bits.

Ce type du tag (avec 28 bits pour le numéro du gestionnaire, 24 bits pour la classe d'objet et 36 bits pour le numéro de série), est capable d'identifier de manière unique 268 millions d'entreprises, dont chacune pourrait ont jusqu'à 16 millions de produits différents et 68 milliards de numéros de série uniques pour chaque produit. Cela est plus que suffisant pour identifier tous les produits manufacturés du monde pour de nombreuses années [7].

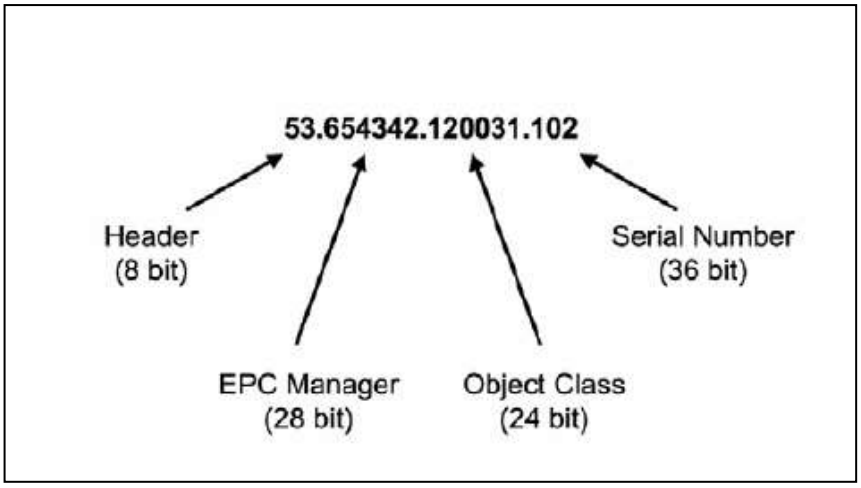


Figure 1-4 : Un exemple de système de numérotation EPC [2]

1.8 Les gammes de fréquences en RFID

Différents systèmes RFID fonctionnent à des fréquences radio variées, chaque fréquence offre sa propre gamme de fonctionnement, ses propres besoins en énergie et ses propres performances. Les différentes gammes peuvent être soumises à des réglementations ou des restrictions différentes qui limitent les applications pour lesquelles elles peuvent être utilisées.

La fréquence de fonctionnement détermine la manière dont les composants RFID interagissent entre eux. D'autre part la bande de fréquence est importante pour déterminer les dimensions physiques d'un tag RFID. Des antennes de tailles et de formes différentes fonctionneront à des fréquences différentes. Le tableau 2 affiche les gammes de fréquences utilisées en RFID.

Gamme de fréquence	Fréquences	Type du tag	Distance
Basse fréquence (LF)	120-140 KHz	Passif	10-20 cm
Haute fréquence (HF)	13.56 MHz	Passif et semi-passif	10-150 cm
Ultra-haute fréquence (UHF)	433 MHz	Actif	3 -10 m
	868-928 MHz	Actif et passif	3-15 m
Micro-ondes	2.45 - 5.8 GHz	Actif , passif et semi-passif	3 -30 m

Tableau 1-2 : Fréquences d'exploitation de la RFID [1]

1.8.1 Basse fréquence (LF)

Les tags RFID à basse fréquence (LF) fonctionnent généralement dans la gamme 120-140 kilohertz. Le plus souvent, les tags LF sont passivement alimentés par l'induction, en conséquence, ils ont généralement une portée de lecture très courte de 10-20 centimètres. Les tags LF sont particulièrement appropriés à des applications requérant une très grande sécurité, ils sont généralement utilisés dans de contrôle d'accès et les systèmes d'immobilisation des voitures, une voiture ne démarre que si un tag LF attaché à la clé de contact est à proximité de l'allumage, ceci profite de la courte portée de lecture de LF et l'utilise comme une fonction de sécurité. L'inconvénient des tags de basse fréquence est qu'ils ont un taux de lecture de données très faible par rapport à d'autres fréquences d'exploitation. Les tags RFID LF sont spécifiés par la norme ISO 18000-2 [7].

1.8.2 Haute fréquence (HF)

Les tags RFID à haute fréquence (HF) fonctionnent à la fréquence de 13,56 mégahertz, elles sont généralement très minces, cela les rend utiles pour le contrôle d'accès aux immeubles, les cartes de crédit sans contact et les badges d'identification, la portée de lecture relativement courte de la HF est un avantage dans ces cas-là. Les tags HF sont également utilisés dans de nombreuses applications de suivi des objets aussi dans le traitement des bagages à aéroports. Les tags HF offrent un taux de lecture des données plus élevé que les tags LF, mais ne sont pas aussi performants dans la proximité de métaux ou de liquides.

La gamme de fréquences HF se situe sur une partie fortement réglementée du spectre radioélectrique et les signaux diffusés par les lecteurs doivent fonctionner dans une bande de fréquences étroite, cela pose un problème pour les environnements comportant des appareils électroniques sensibles, comme les équipements médicaux, qui fonctionnent sur des fréquences proches.

Les spécifications de l'organisation internationale de normalisation (ISO) pour les tags RFID HF sont données par la norme ISO 18000-3, les spécifications connexes pour les cartes à puce sans contact HF et les cartes de proximité figurent dans les normes ISO 14443 et 15693 [8].

1.8.3 Ultra-haute fréquence (UHF)

Les tags RFID à ultra-haute fréquence (UHF) fonctionnent dans la gamme de 868 à 928 mégahertz. Les tags européens fonctionnent généralement dans la gamme 868-870 MHz, tandis que les États-Unis et le Canada fonctionnent dans la gamme 902-928 MHz. Les tags UHF sont le plus souvent utilisés pour le suivi des articles et les applications de gestion de la chaîne d'approvisionnement. Cela s'explique en grande partie par le fait qu'ils offrent une plus grande portée de lecture [1].

L'un des principaux inconvénients des tags UHF est qu'ils subissent des interférences à proximité des liquides ou des métaux, de nombreuses applications comme le suivi des animaux, le suivi des conteneurs métalliques, ou même de nombreux systèmes de contrôle d'accès sont infaisables avec les tags UHF, certains matériels ont la capacité de protéger les tags UHF contre les distorsions liées au métal, mais ces tags peuvent être d'un coût prohibitif à utiliser dans la pratique. Les tags UHF présentent une technologie relativement plus récente que les tags LF ou HF, et les coûts des lecteurs sont généralement plus élevés. Les spécifications des tags RFID fonctionnant aux fréquences UHF sont définies par la norme ISO 18000-6 [9].

1.8.4 Micro-onde

Les systèmes fonctionnant autour des fréquences centrales de 2,45 Ghz et 5,8 Ghz dans les bandes industrielles, scientifiques et médicales (ISM) entrent dans cette catégorie. Les tags passifs, semi-passifs et actifs sont disponibles dans cette gamme de fréquence.

Les systèmes à micro-ondes offrent des taux de lecture plus élevés que les systèmes UHF et des portées de lecture passive équivalentes.

Les inconvénients des tags à micro-ondes sont la grande consommation d'énergie comparativement à leurs homologues à basse fréquence et la dégradation des performances au voisinage de l'eau ou des métaux, tout comme les tags UHF.

1.9 Les défis de la mise en œuvre de la RFID

1.9.1 Techniques

Les systèmes RFID se heurtent encore à de nombreux défis techniques et obstacles à leur adoption pratique. L'un des principaux obstacles consiste simplement à faire fonctionner les systèmes RFID dans des environnements réels, les lecteurs et les tags ont souvent subi des interférences causées par d'autres systèmes sans fil, ou sources inconnues. Aussi la RFID ne fonctionne pas bien avec les métaux et les liquides, car il est difficile d'obtenir une lecture correcte des biens, dans le cas des métaux, les ondes radio rebondissent partout. De même, le liquide peut absorber les signaux des tags RFID.

1.9.2 Économiques

Un obstacle majeur qui subsiste encore dans les systèmes RFID est tout simplement le coût, notamment le cas de l'étiquetage EPC. Un deuxième problème de coût concerne en particulier les lecteurs UHF, qui se vendent à un prix bien élevé. La RFID nécessite des équipements coûteux, qu'il s'agisse de logiciels ou de matériel pour cela de nombreuses entreprises hésitent encore à les adopter en raison de leur prix élevé.

1.9.3 Sécuritaires

De nombreuses préoccupations ont été exprimées au sujet de la sécurité et de la confidentialité des systèmes RFID, la sécurité et en particulier la protection de la vie privée deviendra des questions importantes car les données et les informations ne sont pas à l'abri de l'espionnage, des personnes extérieures pourraient accéder clandestinement aux données stockées par un système RFID surtout si sa configuration est basée sur un protocole très répandu, aussi les données échangées durant une communication légitime entre un tag et un lecteur peuvent être dérobées par un récepteur spécial pour intercepter une conversation non protégée, de puissants signaux électromagnétiques pourraient endommager physiquement ou détruire les systèmes RF lors d'une attaque destructive.

1.10 Conclusion

La RFID est une technologie émergente qui fait partie intégrante de notre vie quotidienne, elle commence à se généraliser sur des axes d'applications très variés : authentification, les systèmes de payement, le suivi de localisation, etc. Malgré les avantages apportés par les RFID, cette technologie n'est pas encore suffisante pour être efficace et performante dans certains domaines car elle peut encore comporter des lacunes technologiques.

Dans ce chapitre, nous avons essayé de fournir des réponses à la plupart des questions clés concernant la technologie RFID, nous avons en premier lieu présenté cette technologie, son historique, ses domaines d'applications et son principe de fonctionnement. Nous avons abordé la constitution des systèmes RFID, les normes et les fréquences allouées. Enfin nous avons cité les défis de la mise en œuvre de la RFID.

Chapitre 2

Méthodologie d'extraction de l'information du capteur

Chapitre 2 : Méthodologie d'extraction de l'information du capteur

Présentation du chapitre

La nouvelle technologie RFID a une plus grande flexibilité, ce qui rend l'échange des informations plus rapide et plus efficace. Ce deuxième chapitre s'occupe uniquement de l'organisation de la communication entre lecteur et tag (s) et la façon dont les données sont échangées. Nous présentons dans ce chapitre les principes physiques des systèmes RFID ainsi le codage et la modulation des données, nous parlerons aussi des mécanismes du couplage et les normes de la communication entre le lecteur et le tag. Enfin nous abordons les différents types d'interférences dans les systèmes RFID.

Sommaire

2.1 Introduction

La radio-identification est un système d'identification automatique et de saisie des données qui utilise les ondes radio pour transférer les informations entre un lecteur et un objet étiqueté dans le but de l'identifier, le catégoriser ou le suivre. Il ne nécessite pas de ligne de vue ou du contact. La communication se produit lorsqu'un objet étiqueté entre dans l'environnement de lecture de l'interrogateur, de telle sorte que le lecteur initialise la communication en envoyant un signal et que le tag absorbe ces signaux et les utilise comme sa propre énergie pour renvoyer les données stockées. Les tags peuvent contenir différents types des données sur l'objet marqué, ces données peuvent inclure le numéro de série, l'heure, les configurations, etc.

Les performances d'un système RFID sont concrétisées dans la fiabilité et l'efficacité du traitement des données échangées entre le lecteur et le tag, un enregistrement plus rapide et des taux d'interrogation plus élevés. Cela nécessite donc un système puissant capable de gérer des informations provenant de diverses sources, de stocker les données et de les transmettre d'une manière fiable et continue pendant de longues périodes. La transmission des données durant la communication est une partie extrêmement importante de la RFID donc comprendre la façon dont un système RFID communique et la façon dont les données sont échangées au moins à un niveau de base est une nécessité.

2.2 Les principes physiques de systèmes RFID

Le transfert des données dans la RFID se fait principalement par des principes physiques pour aider à la compréhension de ces systèmes, nous étudierons la propagation des ondes dans le champ lointain et les principes de la technologie radar.

2.2.1 Force du champ magnétique

Lorsque le courant traverse un circuit, un champ magnétique est créé. L'ampleur du champ magnétique créé est connue sous le nom de la force du champ magnétique. Il est désigné par H [10]. Mathématiquement, il est écrit comme:

$$\sum I = \oint H \,.\, \delta S \tag{2-1}$$

H représente l'intensité du champ magnétique (ampère/mètre) et I représente le courant dans le circuit (ampère).

L'équation (2-1) peut être utilisée pour dériver l'intensité du champ magnétique le long d'un conducteur droit. La figure 1 permet de calculer l'expression de l'intensité du champ magnétique le long d'un conducteur rectiligne.

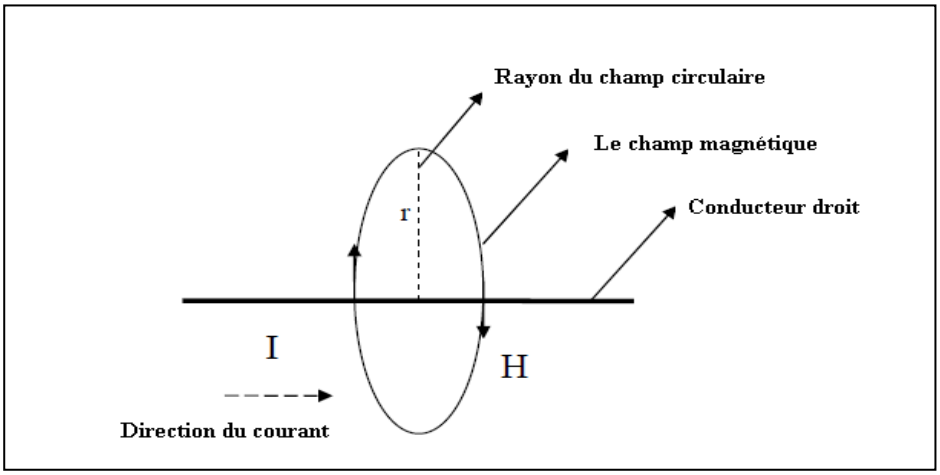


Figure 2-1: Courant circulant à travers un conducteur droit créant un champ magnétique

r désigne le rayon du champ magnétique, H est la force du champ magnétique donné par l'équation suivante [10]:

$$H = \frac{I}{2\pi r} \tag{2-2}$$

2.2.2 Flux magnétique (Φ)

Le flux magnétique est désigné par Φ. Il s'agit du nombre total des lignes du champ magnétique passant par une bobine conductrice du courant. On peut l'écrire mathématiquement comme:

$$\Phi = B.A \tag{2-3}$$

B désigne la densité du flux magnétique, qui est le flux magnétique par unité zone de la section perpendiculaire à la direction du flux. La densité du flux magnétique peut s'exprimer en termes de la force du champ magnétique comme suit:

$$B = \mu_0.\mu_r.H = \mu.H \tag{2-4}$$

μ_0 représente la perméabilité de l'espace libre et μ_r représente la perméabilité du milieu. Dans l'équation (2-4), μ_0 est la constante du champ magnétique dont la valeur $4\pi.10^{-7}$ $H.m^{-1}$ décrit la perméabilité du vide. μ_r est également la perméabilité relative et explique la perméabilité du matériau si elle est supérieure ou inférieure à μ_0. [10]

2.2.3 Inductance

Le champ magnétique est tout le temps généré lorsque le courant s'écoule dans un conducteur et si le conducteur est sous la forme d'une bobine, le champ magnétique sera plus fort. Si le conducteur du courant comporte N enroulements, un flux magnétique sera généré dans chaque boucle. Par conséquent, le flux total peut être exprimé mathématiquement comme suit [10] :

$$\psi = \sum \Phi N = N.\Phi = N.\mu.H.A \tag{2-5}$$

N représente le nombre des spires de la bobine, Φ représente le flux magnétique et H est la force du champ magnétique. L'inductance est maintenant définie comme le flux total qui se produit dans une zone "A" entourée par le courant "I". Il peut être mathématiquement défini comme suit [10] :

$$L = \frac{\Psi}{I} = \frac{N.\Phi}{I} = \frac{N.\mu.H.A}{I} \tag{2-6}$$

L représente l'inductance, ψ représente le flux total dans l'espace.

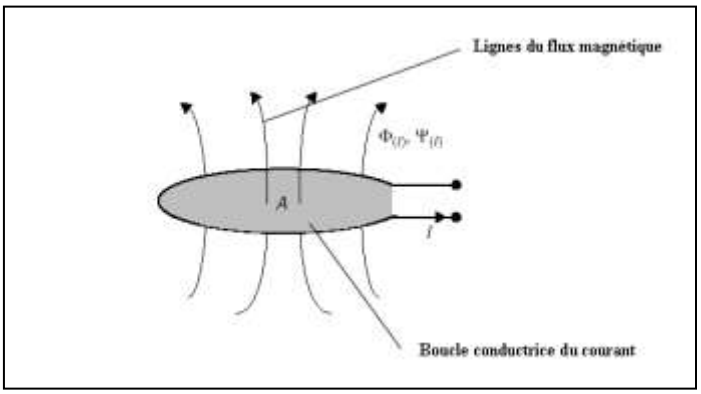


Figure 2-2 : Phénomène d'induction électromagnétique

2.2.4 Inductance mutuelle

L'inductance mutuelle est le principe physique selon lequel un système RFID fonctionne. L'inductance mutuelle explique le couplage de deux circuits avec un champ magnétique, dans lequel l'unité et ses dimensions sont les mêmes que l'inductance expliquée dans la partie précédente. Elle fonctionne de telle manière que si les bobines du deuxième conducteur bouclent avec la zone A2 située à proximité du premier conducteur, la zone A1 dans laquelle le courant circule sera affectée par le flux magnétique généré par A1, une partie du flux passera ainsi à travers la deuxième bobine où ce flux est appelé flux du couplage qui relie les deux bobines par induction. L'idée d'inductance mutuelle est représentée dans la figure 3.

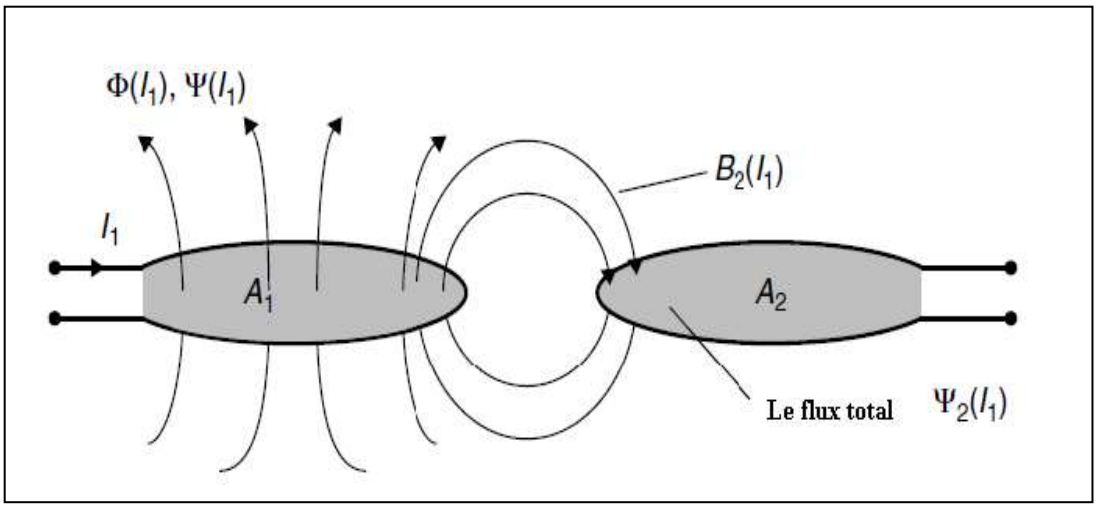


Figure 2-3 : Inductance mutuelle M_{21} par couplage de deux bobines à travers un flux partiel

Dans l'inductance mutuelle, la qualité du couplage inductif dépend de la géométrie des deux bobines, de leur position l'une par rapport à l'autre et de la perméabilité du milieu entre elles. Le flux mutuel qui traverse les deux bobines est appelé flux du couplage et indiqué par ψ_{21}, l'inductance mutuelle est indiquée par M_{21} et celle-ci est définie comme le rapport entre ψ_{21} qui traverse la deuxième bobine et le courant L_1 dans la première bobine est représenté par l'équation (2-7).

$$M_{21} = \frac{\psi_{21}(I_1)}{I1} = \oint_{A_2}^{\infty} \frac{B_2(I_1)}{I1} . d_{A_2} \tag{2-7}$$

On suppose que la même relation fonctionne dans l'autre sens, c'est-à-dire qu'un courant L_2 dans la deuxième bobine génère un champ magnétique qui induit un courant dans la première bobine à travers le flux du couplage. La relation entre l'inductance mutuelle peut être illustrée par l'équation suivante :

$$M = M_{21} = M_{12} \tag{2-8}$$

En outre, le champ magnétique d'inductance mutuelle M_{12} entre deux bobines est donné par :

$$M_{12} = \frac{B_2(I_1).N_2.A_2}{I_1} = \frac{\mu_0.H(I_1).N_2.A_2}{I_1} \tag{2-9}$$

H (I1) est l'intensité du champ magnétique H due au courant I1 (c'est la même chose que H).

2.2.5 La loi de Faraday

Cette loi impose qu'une modification du flux magnétique Φ entraîne la création d'un champ électrique E. Le champ électrique généré dépend des propriétés magnétiques du milieu pour un conducteur avec N enroulements, la loi de Faraday peut être écrite comme suit [11] :

$$E_i = N.\delta\varphi/\delta t \tag{2-10}$$

Où :

E_i : Champ électrique induit par la modification du flux.

$\delta\varphi/\delta t$: Le changement du flux par rapport au temps.

La loi de Faraday est importante dans l'étude de la RFID, car l'application de cette loi à une surface métallique entraîne la création d'une force contre-électromotrice appelée courant de Foucault. Les courants de Foucault augmentent avec l'augmentation du flux alternatif. Par conséquent, dans la conception des systèmes RFID (tags ou lecteurs), il est essentiel d'éviter la construction ou l'installation sur ou à proximité des surfaces métalliques. C'est ce que montre la figure 4.

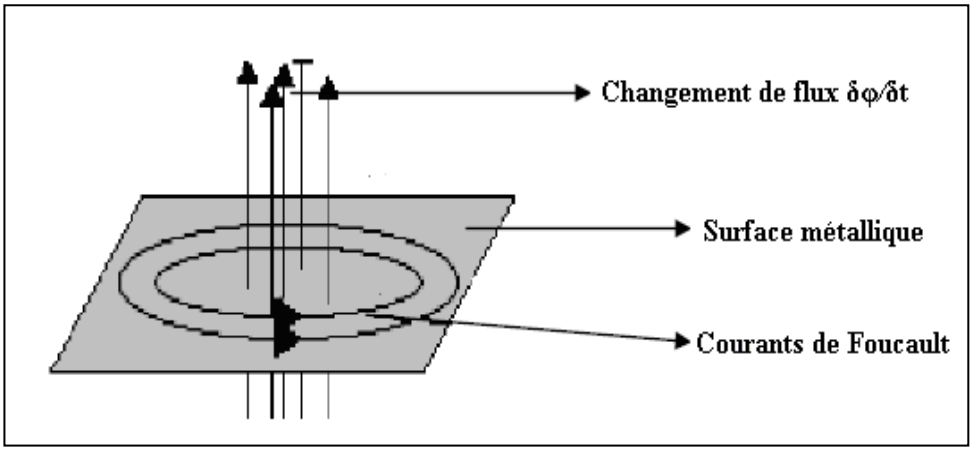


Figure 2-4 : La loi de Faraday appliquée à un conducteur métallique

Toute modification du flux magnétique Φ génère un champ électrique dont la caractéristique est décrite par la loi de Faraday. L'effet du champ électrique généré de cette manière dépend des propriétés matérielles de la zone environnante. L'induction d'un champ électrique dans le vide fait que l'intensité du champ E donne naissance à un champ électrique de la rotation. Une boucle conductrice ouverte provoque l'accumulation d'une tension ouverte aux extrémités d'une boucle conductrice presque fermée, ce qui est normalement appelé tension induite. La surface métallique fait également circuler des charges libres dans la direction de l'intensité du champ électrique. La loi de Faraday dans sa forme générale est donnée par l'équation suivante :

$$U_i = \oint E_i \,.\, d_s = -\frac{d\psi_{(t)}}{d_t} \qquad (2\text{-}11)$$

En outre, pour une bobine à N enroulements, cette équation peut être représentée comme

$$U_i = N.\frac{d_\psi}{d_t} \qquad (2\text{-}12)$$

2.3 Codage des données dans la RFID

Le codage des signaux est la première étape dans la préparation à la communication en RFID, il est effectué principalement pour des raisons de sécurité. Le lecteur RFID et le tag doivent convenir d'une technique du codage similaire afin que les données transmises ne soient décodées que par un lecteur spécifique qui connaît la technique du codage utilisée par le tag. Certaines des différentes techniques du codage utilisées dans la RFID sont examinées dans cette section, suivies d'une représentation graphique de chaque code par rapport à un signal des données et à une horloge.

2.3.1 Codage non-retour à zéro (NRZ)

Dans cette méthode, un 1 binaire est représenté comme une condition significative (niveau logique haut) et un 0 binaire est représenté par un niveau logique bas [17]. Pour une série des bits identiques, le signal reste sans transition. Comme il est montré dans la figure 5, lorsque des 1 logiques sont transmis le signal est à niveau haut et dans l'autre niveau lorsque des 0 logiques sont transmis.

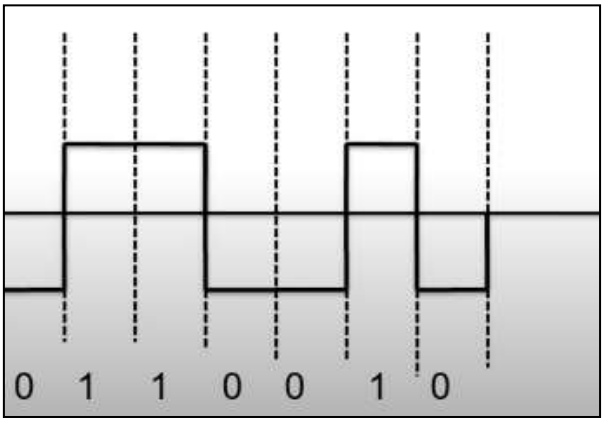


Figure 2-5 : Codage NRZ

2.3.2 Codage Manchester

Le codage Manchester est un codage synchrone, c'est-à-dire en plus des données à transmettre, les signaux transmis intègrent également l'horloge de la synchronisation nécessaire à leur décodage. Les changements du niveau se produisent toujours au milieu d'un cycle d'horloge. Un 0 binaire est traduit en une transition de bas en haut (0 à 1) et un 1 binaire est traduit en une transition de haut en bas (1 à 0). Ce type du codage est également appelé codage à phase divisée [17].

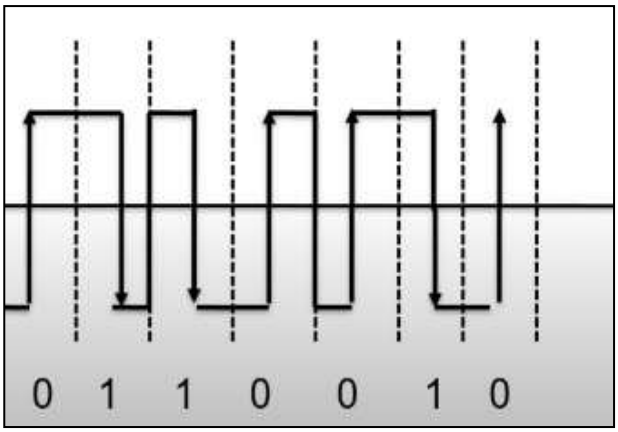


Figure 2-6 : Codage Manchester

2.3.3 Codage de Miller

Dans cette méthode, un 1 binaire est représenté par une transition. La transition peut être soit de bas en haut, soit de haut en bas et se produit au milieu d'un cycle d'horloge [17]. Un 0 binaire est représenté par une continuation du 1 sur le cycle d'horloge suivant. Ce type du codage est également connu sous le nom du codage de la sous-porteuse de Miller.

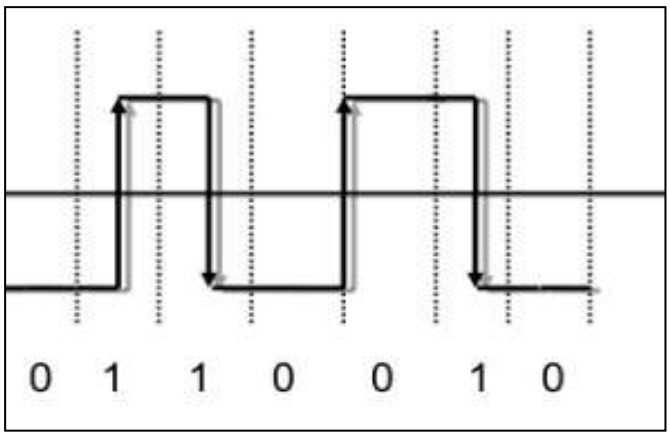


Figure 2-7 : Codage Miller

2.3.4 Codage FM0

Dans ce codage, une transition se produit au début de chaque cycle d'horloge. Un code binaire 1 est représenté par l'absence de transition au milieu du cycle d'horloge. Un 0 binaire est représenté par une transition supplémentaire au milieu du cycle d'horloge [17]. Le codage FM0 est également appelé codage spatial biphasé.

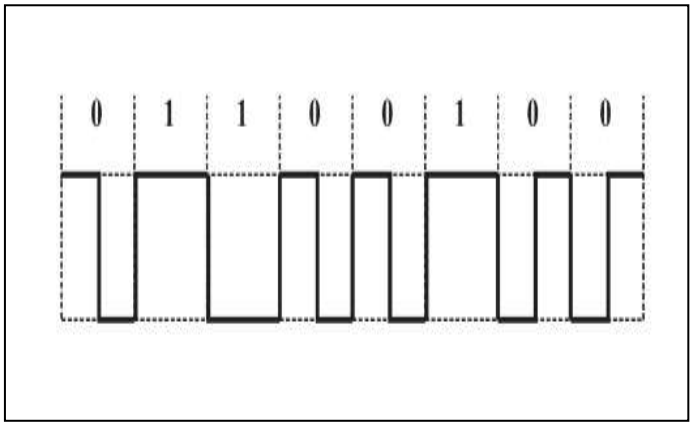


Figure 2-8 : Codage FM0

Comme il est montré dans la figure 8 la logique 0 représente la transition au centre du bit et la logique 1 représente qu'il n'y a pas de transition à partir du centre du bit.

2.3.5 Codage unipolaire RZ

Dans ce codage un 1 binaire est représenté par un niveau logique haut pendant la première moitié du cycle d'horloge alors qu'un 0 binaire est représenté par une absence d'impulsion pendant l'intervalle du temps alloué à un bit [17]. Le signal retourne à la valeur zéro après chaque pulse, même s'il y a une succession de deux zéros ou de uns binaires.

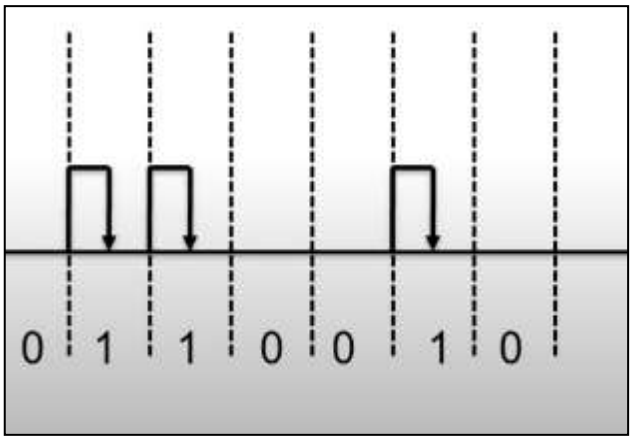


Figure 2-9 : Codage unipolaire RZ

2.3.6 Codage différentiel

Dans ce codage si le bit à coder est un 0, la transition est de sens inverse que la précédente au début de l'intervalle. Dans le cas où le bit à coder est 1, la transition est aussi dans le sens inverse de la précédente mais au milieu de l'intervalle [17].

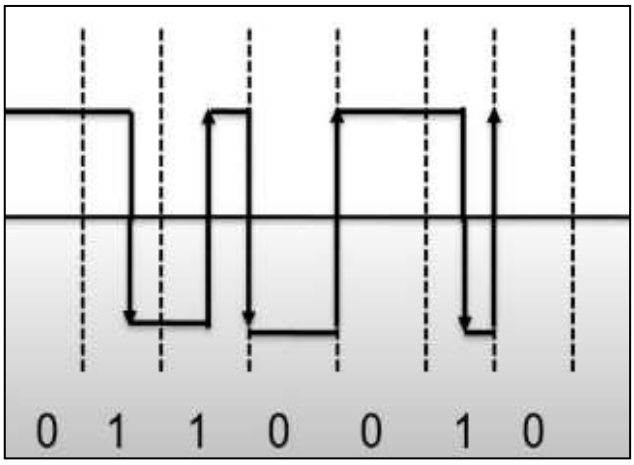


Figure 2-10 : Codage différentiel

Les techniques du codage des données expliquées dans cette section sont présentées sous forme du diagramme dans la figure 11.

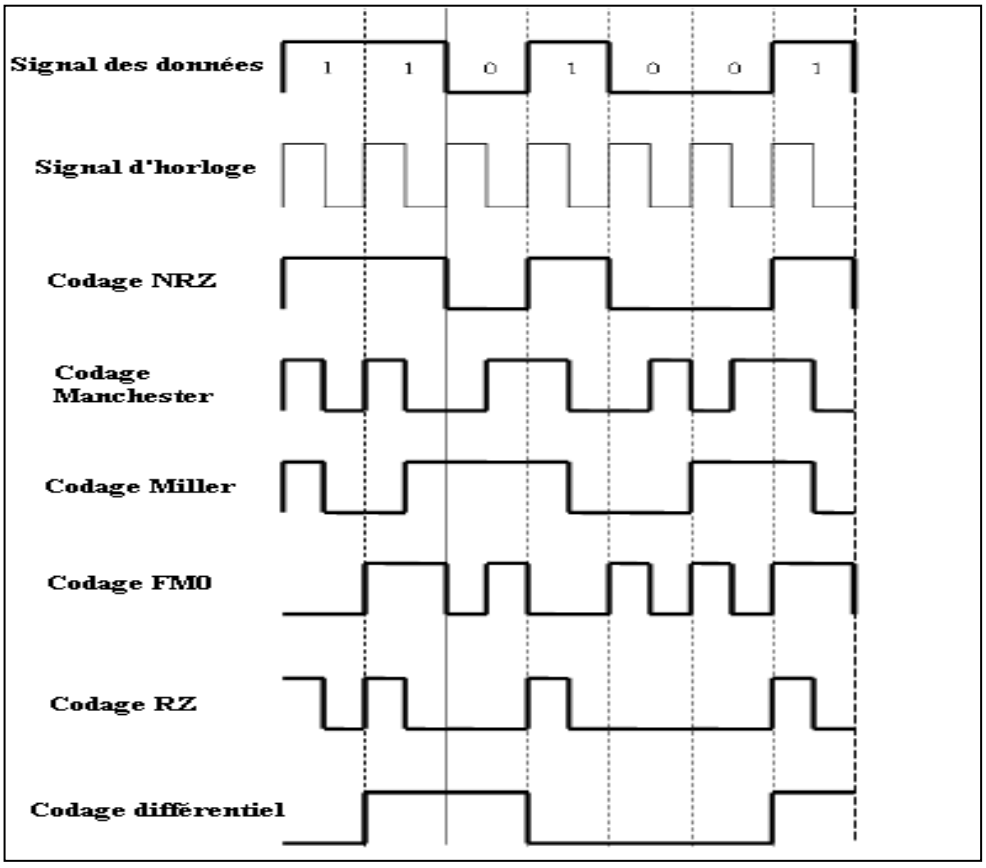


Figure 2-11 : Les techniques du codage numérique

2.4 Modulation

L'antenne d'un système RFID rayonne de l'énergie dans la zone environnante sous forme d'ondes radio. Un signal de données peut être modulé en influençant l'amplitude, la fréquence ou la phase du signal de données, ce processus est appelé modulation. L'avantage de la modulation est de pouvoir transmettre le signal fréquentiel des données. Les modulations les plus couramment utilisées sont :

2.4.1 ASK (Amplitude Shift Keying)

Modulation d'amplitude, il s'agit d'un type du codage dans lequel l'amplitude du signal des données est modifiée (en maintenant la fréquence et la phase constantes) pour produire un signal modulé. Un signal ASK est généré en multipliant le signal des données par un signal porteur à l'aide d'un mélangeur [13]. La figure 12 montre exactement comment cela est fait.

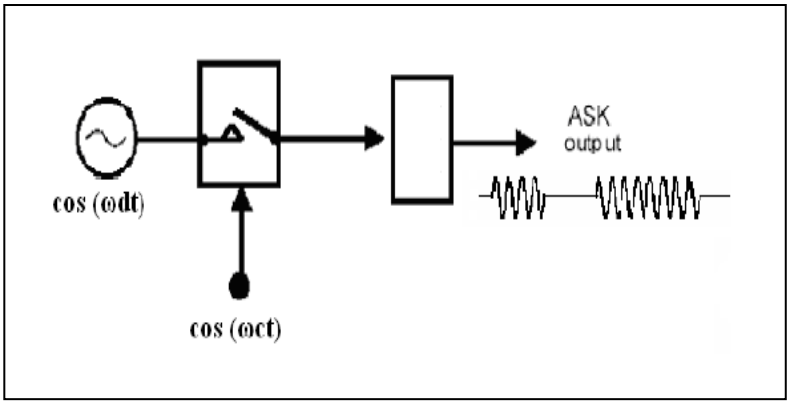


Figure 2-12 : Mélangeur ASK

2.4.2 FSK (Fréquence Shift Keying)

Cette forme de modulation modifie les paramètres de fréquence (en maintenant les tensions et la phase constantes) du signal des données en les multipliant par une onde porteuse de fréquence différente. Il existe deux méthodes pour générer des signaux FSK. La première méthode évidente consiste à commuter entre deux sources de fréquence différentes à l'aide d'un mélangeur. L'inconvénient de cette méthode est qu'elle entraîne une discontinuité de phase. La deuxième méthode permet de surmonter l'inconvénient de la première. Un oscillateur commandé en tension (VCO) est utilisé, le VCO donne une variation de fréquence linéairement proportionnelle au voltage appliqué. Par conséquent, lorsqu'un signal des données est multiplié par une sortie d'un VCO, la sortie sera sous forme d'onde continue.

2.4.3 PSK (Phase Shift Keying)

Une sortie PSK est générée en faisant varier la phase du signal des données. La technique PSK la plus simple est appelée modulation par déplacement de phase binaire (BPSK). Elle utilise deux phases du signal opposées (0 et 180 degrés), le signal numérique est décomposé dans le temps en bits individuels (chiffres binaires), l'état du chaque bit est déterminé en fonction de l'état du bit précédent. Si la phase de l'onde ne change pas, alors l'état du signal reste le même (0 ou 1), si la phase de l'onde change de 180 degrés - c'est-à-dire si la phase s'inverse alors l'état du signal change (de 0 à 1, ou de 1 à 0). Comme il existe deux phases d'onde possibles, cette modulation est parfois appelée modulation biphasée [13].

2.5 Mécanismes du couplage RFID

Le mécanisme du couplage est le moyen de communication entre le tag RFID et le lecteur il détermine la façon dont un circuit sur le tag et le lecteur RFID s'influencent mutuellement pour envoyer et recevoir des informations. Les deux principales méthodes du couplage sont :

- Couplage de la rétrodiffusion RFID
- Couplage inductif RFID

2.5.1 Couplage de la rétrodiffusion RFID

Le couplage de la rétrodiffusion RFID fonctionne en dehors du champ proche de telle manière qu'avec cette méthode du couplage, le lecteur diffuse des signaux radio, le tag reçoit le signal et l'applique en utilisant une partie du signal reçu comme sa propre source d'énergie et en réfléchissant une partie de l'énergie comme réponse du tag vers le lecteur sous forme des "données". La figure 13 illustre ce concept.

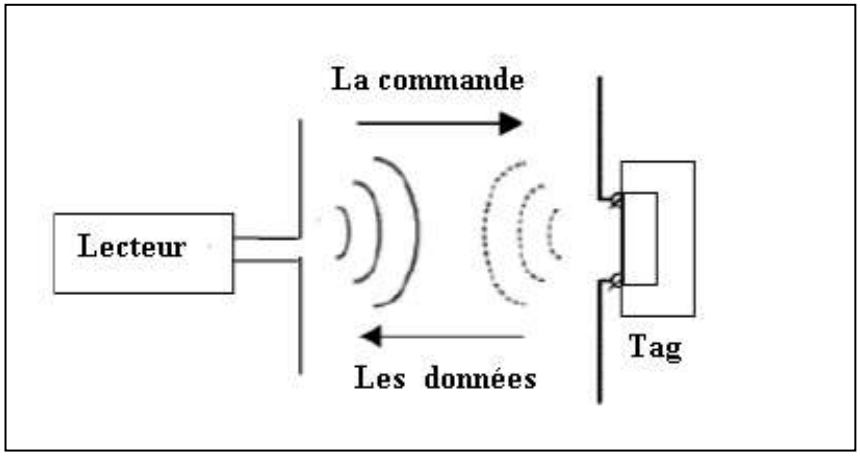


Figure 2-13: Idée de couplage de la rétrodiffusion

Le comportement du tag lors de la réponse au signal du lecteur semble être intéressant. La façon dont le tag répond au signal du lecteur dépend des propriétés du tag et de certains facteurs essentiels tels que les propriétés de l'antenne qui joue un rôle très important dans la réception et le rayonnement du signal. Afin de permettre la transmission et la réception d'un signal en même temps, un coupleur directionnel est souvent utilisé pour permettre au signal reçu d'être séparé de celui transmis. De plus, le lecteur doit être capable de détecter la modulation en présence d'une multitude d'autres réflexions. La conception du circuit électronique du transpondeur joue le rôle principal dans tout système de communication, c'est pourquoi nous donnons ici un aperçu de sa conception électronique. La figure 14 montre l'idée globale d'un circuit électronique du transpondeur et de la transmission de puissance entre les dispositifs de communication [12].

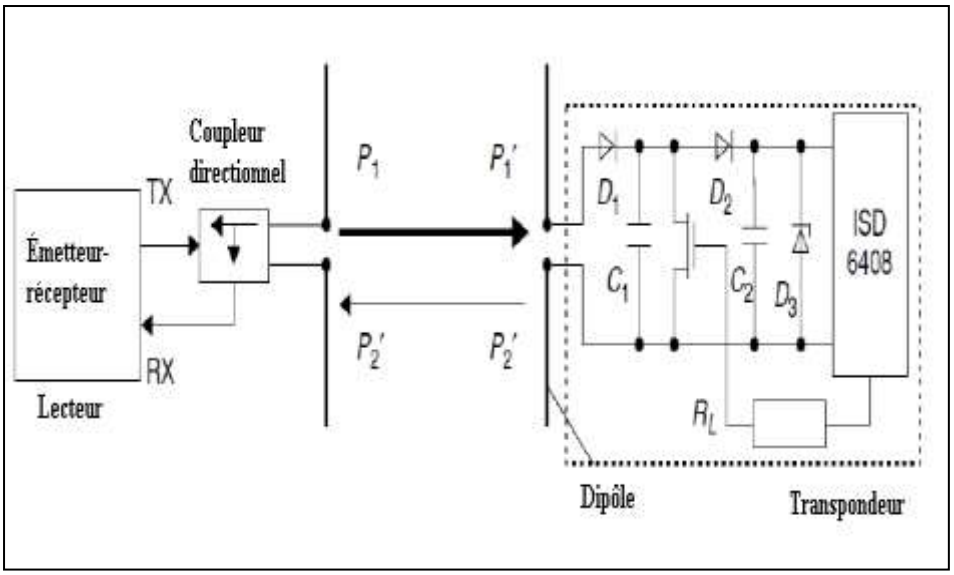


Figure 2-14: Principes du fonctionnement d'un transpondeur de rétrodiffusion

Comme le montre clairement la figure 14, la puissance P1 est émise par les signaux de l'antenne du lecteur et seule une petite partie de cette énergie atteint l'antenne du transpondeur. Ensuite, cette puissance sous forme de tension haute fréquence est fournie à la connexion de l'antenne et après le redressement par les diodes (D1 et D2), cette puissance peut être utilisée comme tension de mise en marche pour la désactivation et l'activation de l'économie d'énergie, ce qui est appelé mode de mise hors tension. Il est évident que pour cette faible énergie fournie au circuit, les diodes doivent être des diodes Schottky, où ce type des diodes a une énergie plus faible et une tension du seuil basse. La tension obtenue peut

également être suffisante pour servir d'alimentation pour des courtes distances. Une partie de la puissance entrante P1 est réfléchie par l'antenne et renvoyée sous forme de puissance P2.
Les caractéristiques de réflexion de l'antenne peuvent être influencées en modifiant la charge connectée à l'antenne. Afin de transmettre les données du transpondeur (Tag) au lecteur, une résistance de charge RL connectée en parallèle avec l'antenne est activée et désactivée en fonction du flux des données à transmettre. La puissance réfléchie P2 du tag rayonne dans l'espace libre et seule une petite partie de cette énergie est reçue par l'antenne du lecteur. Cette énergie se présente sous la forme d'un signal "Données" qui est captée par l'antenne du lecteur où il peut être découplé à l'aide d'un coupleur directionnel à l'entrée du récepteur du lecteur [12].

2.5.2 Couplage inductif de la RFID

Le mécanisme du couplage inductif de la RFID, défini par la norme ISO 15693, est une technique du couplage qui transmet l'énergie d'un circuit à un autre par inductance mutuelle entre les deux circuits. L'idée de l'inductivité est illustrée à la figure 15 le transpondeur et le lecteur appliquent tous deux la fonction d'inductivité pour la communication et la transmission des données.

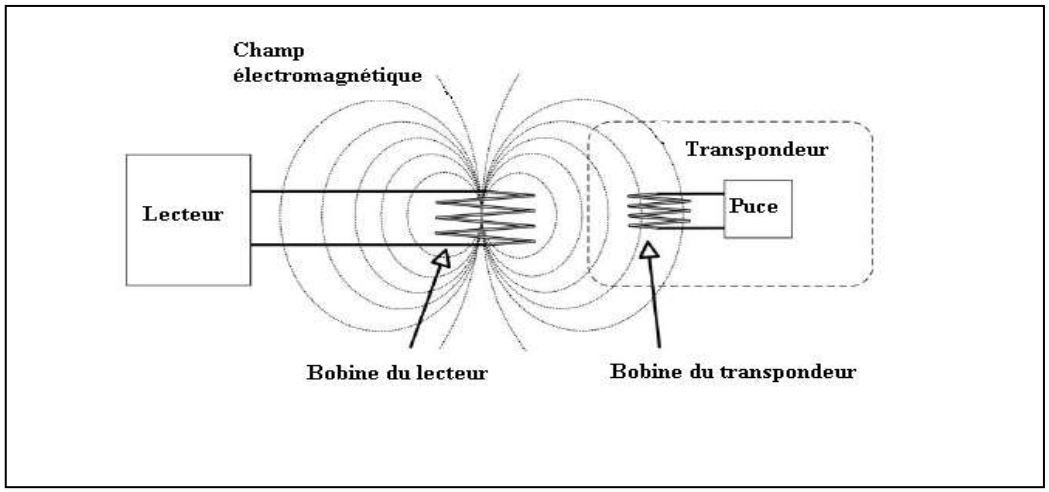


Figure 2-15 : La communication inductive entre le lecteur et un tag à l'aide de bobines

En termes du fonctionnement, le couplage inductif est le transfert d'énergie d'un circuit à l'autre par l'inductance mutuelle entre les deux circuits. Pour que le couplage inductif RFID puisse être utilisé, le tag et le lecteur seront tous les deux dotés des bobines d'induction ou "d'antenne".

Lorsque le tag est placé suffisamment près du lecteur, le champ de la bobine du lecteur se couple à la bobine du tag, une tension sera induite dans le tag qui sera redressée et utilisée pour alimenter le circuit du tag. Pour permettre aux données d'être transmises du tag au lecteur, le circuit du tag modifie la charge de sa bobine, ce qui peut être détecté par le lecteur grâce au couplage mutuel.

Le transfert des données est effectué en utilisant la modulation de charge mais avec quelques différences. Le couplage inductif utilise trois méthodes principales pour transférer les données du tag au lecteur. La première de ces méthodes est appelée la méthode sous-porteuse [10]. Dans cette méthode, le tag active et désactive rapidement sa résistance de charge. Cela permet de générer deux fréquences qui sont différentes de la fréquence du fonctionnement du lecteur. Ces deux fréquences générées par le lecteur sont appelées fréquences de sous-porteurs. Les données sont transférées par modulation avec l'une des fréquences des sous-porteurs.

La deuxième méthode du transfert des données s'appelle la méthode sub-harmonique [10]. Le tag divise la fréquence d'exploitation du lecteur par une valeur intégrale et transmet des données au lecteur à cette fréquence.

La troisième méthode du transfert des données dans un système inductif est appelée transfert séquentiel des données [10]. Ici, l'alimentation du lecteur vers le tag n'est pas continue, de sorte que le tag contient un circuit du condensateur qui stocke l'alimentation du lecteur lorsqu'elle entre dans le champ magnétique généré par le lecteur. Le tag contient également un circuit oscillateur pour créer son propre champ magnétique. Comme le lecteur est mis hors tension à ce stade, il est capable de détecter le champ généré par le tag et de transférer des données.

2.6 La portée des systèmes du couplage

Chacune de ces méthodes a sa propre caractéristique et diffère des autres. Le type de méthode du couplage affecte différents aspects du système RFID tels que la distance de communication, la gamme des fréquences et d'autres éléments du matériel RFID. En fonction de la portée de lecture créée entre le lecteur et un tag, il existe trois types du couplage : couplage rapprochée, couplage distant et couplage à longue portée.

2.6.1 Systèmes à couplage rapproché

La distance de lecture entre le tag et le lecteur est de 10 mm maximum, cela signifie que le tag doit être pressé contre le dispositif de lecture, cette courte distance présente certains avantages en cas d'absorption d'énergie par le tag car celle-ci peut tirer une grande quantité d'énergie du champ magnétique. Un autre avantage de ce couplage est qu'il offre une grande sécurité aux systèmes qui en ont besoin.

2.6.2 Systèmes à couplage distant

La plage de lecture se situe entre 10 mm et 1000 mm. Cette portée est généralement appliquée avec des tags passifs. Ces systèmes représentent plus de 90% des systèmes RFID vendus actuellement. Ce type du couplage est également appelé couplage à distance, le couplage inductif est un exemple du couplage distant.

2.6.3 Systèmes longue portée

La communication RFID à longue portée est utilisée pour des distances plus longues que les autres couplages. Normalement, la distance est comprise entre 1 m et 10 mètres, cette portée utilise la fréquence la plus élevée qui est spécifiée pour la RFID. Contrairement aux portées précédentes, ce couplage applique également la méthode de communication par rétrodiffusion. Cette distance plus élevée spécifie donc le type des tags et les modes de communication.

Dans ce cas, le système contient généralement des tags qui agissent à longue distance avec une très faible puissance ou des tags actifs qui contiennent une source d'énergie telle qu'une batterie. En plus de toutes les portées mentionnées ci-dessus, il existe des systèmes avec des distances supérieures à 10 mètres.

2.7 Normes de communication

Dans la technologie RFID, on distingue deux types de protocoles de communication :

- RTF (Reader-Talks-First)
- TTF (Tag-Talks-First)

2.7.1 RTF (Reader-Talks-First)

Nommé aussi ITF (Interrogator-Talks-First). Le lecteur envoie un signal d'alimentation, mais les tags du son champ restent inactives jusqu'à ce que le lecteur leur envoie une demande d'identification. Si le tag correspondant est à la portée du lecteur, il répondra. Le lecteur peut trouver les tags avec des identifiants particuliers en interrogeant tous les tags dont les identifiants commencent par 0 ou par 1. Si plusieurs tags réagissent, il exige à ceux dont l'identifiant débute par 01 de répondre et ainsi de suite. Cette famille du protocole est connue sous le nom d'algorithme de singularisation (anticollision) [14].

2.7.2 TTF (Tag-Talks-First)

Un tag RFID lorsqu'il est à la portée du lecteur, immédiatement il lui indique sa présence et reflète le signal reçu en lui envoyant son identifiant. Cette technique est très utile pour connaître tous les tags passant près du lecteur, en particulier les objets transportés par des tapis roulants dans les entrepôts ou les aéroports.

2.8 Les problèmes techniques

La technologie RFID, si elle a un petit côté « magique », elle restera imparfaite, voici quelques problèmes strictement limités au domaine technique :

2.8.1 L'orientation des antennes

Les tags RFID ne requièrent pas de connexion optique pour fonctionner, mais les lecteurs affrontent des difficultés et n'ont pas la capacité de communiquer normalement avec un tag dont l'antenne est orientée perpendiculairement à l'antenne du lecteur. Par exemple : si plusieurs produits sont disposés au hasard dans un chariot à commissions, certains seront orientés de telle sorte qu'ils seront invisibles par le lecteur. Si les produits marqués ne peuvent pas être réorientés, il faut alors modifier l'orientation du lecteur ou construire des antennes moins sensibles à l'orientation. [15]

2.8.2 Les interférences dans un système RFID

Les performances d'un système RFID peuvent être affectées par différents types d'interférences:

- **Interférence lecteur / tag**

Cela se produit lorsque plusieurs lecteurs tentent de lire (et donc alimenter) le même tag, ce qui engendre un blocage de lecture du tag. Lorsque deux lecteurs ou plus enverront une commande à un tag, et si la différence entre l'intensité de leurs signaux dépasse le seuil toléré par le tag, la lecture du ce dernier sera impossible. Une différence d'intensité de 6 à 15 dB (marge de tolérance) est nécessaire pour qu'un tag fasse la distinction entre deux signaux entrant en collision et réagisse à un seul lecteur [16].

- **Interférence lecteur/lecteur**

Ce type d'interférence se produit lorsque le lecteur A est en communication avec un tag et reçoit en même temps le signal d'un autre lecteur B à une fréquence très proche, si le signal de B est plus fort que celui du tag, le lecteur A ne peut pas décoder le signal provenant du tag. Ce problème est aggravé par le fait que la puissance du signal d'un tag passif vers un lecteur diminue plus rapidement (en fonction de la distance) que celle d'un lecteur vers un lecteur, c'est-à-dire que la puissance du signal pendant la communication tag/ lecteur diminue en fonction de la distance d par "$1 / d^4$" contre "$1 / d^2$" pour la force du signal du lecteur / lecteur [16].

- **Interférence tag / tag**

Cela se produit lorsque plusieurs tags répondent à un signal du lecteur en même temps, où les tags envoient simultanément des signaux à un seul lecteur, empêchant ce dernier de reconnaître correctement un tag particulier ce qui provoque l'échec de la transmission des données. Pour résoudre ces problèmes et permettre la communication dans un environnement à tags multiples, les lecteurs utilisent des méthodes ou algorithmes anti-collision (également appelés algorithmes de singularisation pour isoler les tags individuellement. [16]

2.9 Conclusion

Avec le développement massif des produits RFID, il est important de bien concevoir comment la technologie fonctionne et comment elle peut être utilisée. Le système RFID est activé par un transfert d'énergie électromagnétique entre un tag et un émetteur. Le tag est composé d'une puce électronique et d'une antenne, reçoit le signal radio envoyé par le lecteur, dont le rôle fondamental est d'extraire les données du tag une fois le couplage est assuré.

Dans ce chapitre nous avons détaillé la façon de récupération des données en représentant au premier lieu les principes physiques dans la RFID pour comprendre les mécanismes du couplage entre lecteur et tag, puis nous avons présenté les techniques du codage des donnés et les modulations utilisées ainsi que les normes de communication. Enfin nous avons montré les problèmes techniques durant la transmission des données.

Chapitre 3

Authentification par RFID

Chapitre 3 : Authentification par RFID

Présentation du chapitre

L'objectif de ce chapitre est de présenter les systèmes actuels de protection de la vie privée et de sécurité et d'étudier certains des protocoles d'authentification RFID proposés. D'abord nous commençons par une brève introduction sur la sécurité des systèmes RFID, puis nous présentons les attaques de base liées au déploiement potentiel de cette technologie et les précautions de sécurité à suivre. Nous analysons ensuite certains des principaux protocoles d'authentification et leurs procédures. Enfin nous abordons la classification basée sur les ressources des protocoles d'authentification RFID et sur des approches cryptographiques.

Sommaire

3.1 Introduction

Jour après jour, l'importance des systèmes d'identification par radiofréquence (RFID) augmente en raison de leurs puissantes capacités d'identification automatique, de localisation et de contrôle d'accès des personnes et des objets. Le canal de communication sans fil entre lecteur et tag met cette technologie vulnérable à de multiples attaques et à de nouvelles menaces. Ceci soulève deux problèmes principaux, l'un lié à la sécurité des données transmises et l'autre lié à la violation de la vie privée du possesseur du tag. Par conséquent, cette technologie requiert l'utilisation des mécanismes de sécurité pour contrer tout type d'attaques et de menaces, ce qui peut être réalisé par le service authentification. Ces menaces potentielles ont donné lieu à un domaine de recherche actif qui porte principalement sur la formalisation des modèles de sécurité et de protection de la vie privée et de la conception des protocoles d'authentification RFID sécurisés. Les principaux défis dans ce domaine sont la définition des modèles formels qui saisissent de manière exhaustive les capacités d'un attaquant du monde réel, et la conception des protocoles d'authentification qui sont manifestement sécurisés et qui préservent la vie privée en ce qui concerne les modèles formels qui correspondent aux ressources informatiques rigoureuses des tags RFID.

3.2 Types d'attaques de base

L'objectif des systèmes RFID est de parvenir à une meilleure congruence entre le monde virtuel des données et le monde réel [18]. Il est donc crucial pour l'intégrité des systèmes RFID que trois relations soient assurées :

- La relation entre les données stockées sur tag (transpondeur) et le tag lui-même. Cette relation doit être unique, car le tag est identifié uniquement par les données. La partie la plus importante des données est un numéro d'identification unique (numéro de série). L'identité peut être sécurisée par le stockage des clés ou d'autres informations de sécurité sur le tag. Il est impératif d'empêcher l'existence de deux tags portant la même identité.
- La relation entre le tag et l'article étiqueté qui est censé être identifié. Cette relation doit également être unique dans le sens qu'un tag ne doit jamais être attribué à des articles différents pendant son utilisation.
- La relation entre le tag et le lecteur (interface radio). Cette relation doit être établie de manière à ce que les lecteurs autorisés puissent détecter la présence du tag et accéder correctement aux données, tout en empêchant l'accès de lecteurs non autorisés.

Voici quelques types d'attaques sur les RFID :

3.2.1 Falsification du contenu

Les données peuvent être falsifiées par un accès en écriture non autorisé au tag. Au moment de l'attaque, l'ID (numéro de série) et toute autre information de sécurité qui pourrait exister (par exemple les clés) restent inchangées [18]. De cette façon, le lecteur continue à reconnaître correctement l'identité des tags. Ce type d'attaque n'est possible que dans le cas des systèmes RFID qui outre les informations d'identification et de sécurité, stockent d'autres informations sur le tag.

3.2.2 Falsification d'identité (tag)

L'attaquant obtient l'identifiant et toute information de sécurité d'un tag et les utilise pour tromper un lecteur et lui faire accepter l'identité de ce tag particulier. Cette méthode d'attaque peut être réalisée à l'aide d'un dispositif capable d'émuler n'importe quel type de tag ou en produisant un nouveau tag en tant que copie de l'ancienne (clonage)[18]. Ce type d'attaque a pour conséquence la mise en circulation de plusieurs tags ayant la même identité.

3.2.3 Désactivation

Ce type d'attaque rend le tag inutilisable par l'application non autorisée de commandes d'effacement ou de mise à mort, ou par la destruction physique. Selon le type de désactivation, le lecteur ne peut plus détecter l'identité du tag, ou il ne peut même pas détecter la présence du tag dans la zone de lecture.

3.2.4 Écoute clandestine

La communication entre le lecteur et le tag via l'interface radio est surveillée par l'interception et le décodage des signaux radio. C'est l'une des menaces les plus spécifiques qui pèsent sur les systèmes RFID.

3.2.5 Brouillage

L'échange de données via l'interface radio peut être perturbé par des moyens passifs tels que le blindage ou par des moyens actifs (émetteurs de brouillage). Comme l'interface radio n'est pas très robuste, même de simples mesures passives peuvent être très efficaces.

3.2.6 Blocage

Les tags dits "bloquants" simulent pour le lecteur la présence d'un nombre quelconque de tags, bloquant ainsi le lecteur. Un tag bloquant doit être configuré pour le protocole anti-collision utilisé.

3.2.7 Falsification d'identité (lecteur)

Dans un système RFID sécurisé, le lecteur doit prouver son autorisation au tag. Si un attaquant veut lire les données avec son propre lecteur, il doit falsifier l'identité d'un lecteur autorisé. Selon les mesures de sécurité en place, une telle attaque peut être possible à réaliser. Le lecteur peut avoir besoin d'accéder le back-end pour, par exemple, récupérer les clés qui y sont stockées.

3.2.8 Attaque par rejeu

C’est une forme d'attaque de réseau dans laquelle l'attaquant enregistre les informations transmises par canal radio entre le tag et le lecteur et les utilise plus tard pour s'authentifier dans un sens ou dans l'autre. Il s'agit d'un type d'usurpation d'identité.

3.3 Authentification RFID

L'authentification est un processus de vérification de l'identité d'une entité (personne ou ordinateur) par un système informatique pour autoriser ou pas à l'entité d'accéder à des ressources spécifiques. Lors de l'authentification, l'identité d'une personne ou d'un programme est vérifiée. Ensuite, sur cette base, il y aura une autorisation, c'est-à-dire que des droits, comme le droit d'accès aux données sont accordés. Dans le cas des systèmes RFID, il est particulièrement important que les tags soient authentifiés par le lecteur et vice versa. En outre, les lecteurs doivent également s'authentifier auprès du serveur principal, mais dans ce cas, il n'y a pas de problèmes de sécurité spécifiques aux RFID.

3.3.1 Vérification de l'identité du tag

Lorsque le système RFID détecte un tag, il doit vérifier son identité afin de déterminer si le tag a le droit de faire partie du système. Une réglementation mondiale et sans ambiguïté pour l'émission de numéros d'identification, sous la forme du code produit électronique (EPC) offre une certaine protection contre les tags falsifiés. Tout au moins, l'apparition des numéros qui n'ont jamais été émis ou de doublons (clonage) peut être reconnue dans certaines applications. En outre, l'authentification peut se faire par le biais du système du défi-réponse, dans lequel le lecteur envoie un nombre aléatoire ou un horodatage au tag (défi) que le tag renvoie sous forme cryptée au lecteur (réponse). La clé utilisée dans ce cas est un secret commun connu, au moyen duquel le tag prouve son identité. L'élément décisif de cette procédure est le fait que la clé elle-même n'est jamais transmise et qu'un nombre aléatoire différent est utilisé pour chaque défi. Par conséquent, le lecteur ne peut pas être trompé par l'enregistrement et la relecture de la communication (attaque par rejeu). Cette procédure d'authentification unilatérale est définie comme un "protocole d'authentification unilatérale à deux passages à clé symétrique" dans la norme ISO 9798 [18].

Un attaquant devrait s'emparer de la clé qui est stockée à la fois sur le tag et dans l'arrière-plan du système RFID. Pour ce faire, il serait nécessaire de décoder les données de réponse qui ont été transmises sous forme cryptée, ce qui est une tâche très complexe, voire presque impossible, selon la longueur de la clé. Une méthode de défi-réponse peut également être utilisée pour l'authentification mutuelle du lecteur et du tag. Dans ce cas, le tag doit également être capable de générer des nombres aléatoires.

3.3.2 Vérification de l'identité du lecteur

La méthode la plus simple pour authentifier le lecteur par rapport au tag est d'utiliser une protection par mot de passe, c'est-à-dire que le lecteur s'identifie au tag en transmettant le mot de passe. Le tag compare ce mot de passe avec le mot de passe stocké en mémoire. Si les deux sont identiques, le tag donne un accès complet aux données stockées. Certains produits offrent une protection par mot de passe pour certaines zones de la mémoire. Dans les systèmes de lecture seule les plus sophistiqués, le fabricant attribue à chaque tag un mot de passe individuel, qui est ensuite stocké dans sa mémoire.

Les mots de passe variables sont capables d'assurer une meilleure protection, mais ils ne fonctionnent qu'avec des tags en lecture-écriture. La longueur d'un mot de passe typique serait de 8, 24 ou 32 bits [18].Les systèmes de mots de passe sans cryptage sont considérés comme une méthode d'identification faible, car ils permettent d'espionner la transmission de mot de passe via l'interface radio non sécurisée. En outre, les mots de passe courts peuvent être craqués par simple essai systématique. Les systèmes de mots de passe sans cryptage peuvent être adéquats dans les cas où le tag n'est adressé qu'une seule fois ou lorsque le danger de découverte d'un mot de passe par espionnage est déjà faible. Si l'accès est limité, une liste de mots de passe uniques stockés dans le tag et dans le back-end peut également être utilisée au lieu d'un mot de passe unique. Contrairement aux procédures cryptographiques, ces systèmes de mots de passe n'exigent que peu d'informations et peuvent être mis en œuvre avec des tags simples en lecture seule.

La procédure de hachage (hash-lock) permet d'améliorer la sécurité contre les lectures non autorisées. Dans ce cas, avant qu'un tag ne soit écrit pour la première fois, un "meta-ID" est généré à partir d'une clé comme pseudonyme du tag. Cela se fait à l'aide d'une fonction de hachage, dont le calcul est pratiquement irréversible, et le méta-ID est stocké dans le tag. À partir de ce moment, le tag est verrouillé, c'est-à-dire qu'il réagit aux signaux d'un lecteur uniquement en transmettant le méta-ID. Pour déverrouiller le tag, le lecteur doit récupérer de la base de données la clé qui appartient au méta-ID et la transmettre au tag. Le tag applique la fonction de hachage à la clé qu'il a reçue et vérifie si le résultat est identique à son méta-ID. Si c'est le cas, le lecteur est authentifié et le tag permet d'accéder à ses données. [19]

Il serait presque impossible pour un attaquant de revenir à la clé d'origine. Par conséquent, dans de nombreuses zones de déploiement pratiques, une méta-ID constitue une protection suffisante contre la lecture non autorisée. Cependant, lors de la transmission par l'interface radio, la clé secrète appartenant à un méta-ID peut être espionnée par un attaquant qui peut ensuite tromper le tag pour qu'il reconnaisse le lecteur comme étant autorisé (attaque par rejeu). La procédure de hachage peut être mise en œuvre pour les tags même sans utiliser de crypto-processeurs sophistiqués [19], de sorte que cette procédure peut être utilisée même pour des tags peu coûteux.

Une protection maximale contre l'accès non autorisé aux tags est assurée par des procédures d'authentification avec cryptage selon le principe de défi-réponse (procédures cryptographiques fortes). Toutefois, ces procédures présupposent que le tag peut non seulement exécuter des algorithmes cryptographiques mais aussi générer des nombres aléatoires. Dans le cas des tags qui répondent à ces exigences et peuvent donc vérifier l'autorisation du lecteur à un niveau de sécurité élevé, il n'est pas utile de faire des compromis lorsque le problème inverse se pose (authentification du tag auprès du lecteur), car la capacité de traitement du lecteur ou du back-end ne constitue pas un obstacle. Par conséquent, dans le cas de tags à haute performance, des procédures d'authentification mutuelle forte sont appropriées.

3.3.3 Authentification mutuelle forte

La norme ISO 9798 définit diverses procédures de défi-réponse pour l'authentification forte dans le cas des cartes à puce à contact et des systèmes RFID, y compris l'authentification mutuelle [18]. Lorsqu'un tag reçoit une commande "get challenge" de la part d'un lecteur, elle génère un nombre aléatoire A et l'envoie au lecteur. Le lecteur génère à son tour un nombre aléatoire B et avec celui-ci et le nombre aléatoire A, il génère un bloc de données crypté (jeton T) sur la base d'un algorithme de cryptage et d'une clé secrète K. Le bloc des données est ensuite renvoyé au tag. Comme les deux parties utilisent le même algorithme de cryptage et que la clé K est stockée sur le tag, celui-ci est capable de décrypter le jeton T. Si le nombre aléatoire original A et le nombre aléatoire A', qui a maintenant été décrypté, sont identiques, cela prouve l'authenticité du lecteur. La procédure est alors répétée afin d'authentifier le tag auprès du lecteur. Dans ce cas, un deuxième jeton S est généré dans le tag et est transmis au lecteur. Si les nombres aléatoires décryptés B et B' sont identiques, alors l'authenticité du tag vis-à-vis du lecteur a également été prouvée.

Dans cette procédure, aucune clé secrète n'est jamais transmise via l'interface radio non sécurisée. Au lieu de cela, seuls des nombres aléatoires cryptés sont utilisés, ce qui donne un haut degré de protection contre les accès non autorisés. L'enregistrement et la lecture ultérieure de la séquence d'initialisation (attaque par rejeu) ne permettent pas non plus d'accéder au tag ou au lecteur.

3.4 Protocole d'authentification RFID

Un protocole d'authentification RFID permet une authentification mutuelle entre le lecteur et le tag, et devrait résister aux menaces et attaques potentielles en matière de sécurité, comme l'attaque par rejeu, etc. En plus de l'authentification mutuelle, l'anonymat et la transmission secrète sont également des propriétés souhaitables dans RFID. L'intérêt de garantir l'anonymat du système vise à protéger la confidentialité de l'identité des tags de telle sorte que les lecteurs non autorisés ne peuvent pas identifier ou suivre un tag spécifique. D'autre part la propriété du secret de transmission vise à protéger les communications passées lorsqu'un tag est impliqué, même si nous supposons qu'un attaquant peut avoir le pouvoir de compromettre le tag quelque temps plus tard.

Tout comme les tags de différents types actuellement disponibles sur le marché, les protocoles d'authentification RFID peuvent être très différents les uns des autres et les différences peuvent provenir des ressources distinctes requises ou des mécanismes variés adoptés. En conséquence, nous pouvons classer ces protocoles et spécifier les fonctionnalités de chaque type. Une classification, proposée est basée sur les ressources exigées par les protocoles [21]. Cette classification est très pratique, car comme nous l'avons dit plus tôt, il existe sur le marché des variétés de tags dont la plupart sont limités en termes des ressources et les ressources requises par ces protocoles peuvent être très différentes. Une deuxième classification est basée sur le type d'approche cryptographique adoptée, car c'est l'approche qui décide l'efficacité du protocole.

3.5 La classification basée sur les ressources des protocoles d'authentification RFID

Il existe plusieurs tags RFID sur le marché et les capacités de ces tags sont très variables, certaines peuvent soutenir des calculs à la clé publique et certains ne peuvent prendre en charge que des opérations simples au niveau des bits. En fonction de la capacité requise sur les tags, nous classons approximativement les protocoles d'authentification RFID en quatre classes :

- **Classe à part entière** : Fait référence aux protocoles qui exigent la prise en charge des fonctions cryptographiques classiques comme le cryptage symétrique, la fonction cryptographique à sens unique. L'une des principales applications de ces protocoles à part entière est le passeport électronique et la carte de crédit [24].
- **Classe simple** : Concerne les protocoles qui devraient prendre en charge un générateur de nombres aléatoires et la fonction de hachage unidirectionnel sur les tags.
- **Classe des protocoles légers :** Fait référence aux protocoles qui nécessitent un générateur des nombres aléatoires et des fonctions simples telles que la somme du contrôle du code de redondance cyclique (CRC) mais pas de fonction de hachage.
- C**lasse ultra-légère** : Fait référence aux protocoles qui n'impliquent que des opérations simples au niveau du bit (comme XOR, AND, OR, etc.) sur les tags. Peris- Lopez et al. ont proposé une série de protocoles d'authentification ultra-légers qui sont très efficaces

3.6 La classification basée sur des approches cryptographiques

Contrairement aux authentifications dans les applications classiques où l'anonymat et la non-traçabilité ne sont généralement pas des propriétés nécessaires, l'anonymat et la non-traçabilité sont propriétés souhaitables dans de nombreuses applications RFID. Selon la technique utilisée par le protocole d'authentification RFID pour identifier un tag tout en protégeant l'anonymat, nous pouvons classer les protocoles RFID anonymes dans les différentes approches suivantes. En décrivant ces approches, nous nous concentrons sur les techniques permettant d'identifier les tags tout en préservant l'anonymat, sans couvrir les détails des protocoles.

3.6.1 Approche du défi-réponse simple

Dans cette approche, chaque tag T_i partage une clé distincte K_i avec le serveur S/ le lecteur R. Lorsque le lecteur R sonde tag T_i en envoyant une valeur aléatoire N_R comme défi, T_i répond par h (K_i,N_R) où h() désigne un sens unique sécurisé ou une fonction qui peut produire un engagement sur ses apports tout en protégeant l'entrée non divulguée K_i.A la réception de la réponse h (K_i, N_R), le serveur calcule h (K_j, N_R) pour chaque tag potentiel T_j dans sa base des données afin de voir s'il existe un tag correspondant. Cette approche permet au serveur d'identifier un tag sans révéler l'identité aux écoutes clandestines. Chaque tag ne conserve qu'une seule clé secrète, mais le serveur doit effectuer le calcul pour chaque tag potentiel pour l'identification. Ainsi, l'espace de stockage du tag est O (1) mais le calcul pour l'identification d'un tag est O(n), où n est le nombre des tags possibles. [24]

3.6.2 Approche du pseudonyme variable (VP)

Dans cette approche, chaque tag synchronise son identifiant variable et son état interne avec le serveur. Même si certains protocoles basés sur le défi-réponse synchronisent également l'état entre les tags et le serveur, ces protocoles n'envoient pas un pseudonyme variable pour faciliter l'identification rapide du serveur, donc nous ne les comptons pas dans cette approche VP. L'identifiant variable est appelé pseudonyme. A la réception d'une demande de défi, le tag répond avec le pseudonyme actuel et l'engagement sur le défi et l'état interne secret. Sur la base de l'engagement, le serveur peut vérifier le tag.

Lors de l'authentification, le tag et le serveur mettent respectivement à jour leurs pseudonymes et leur état interne. Dans cette approche, le pseudonyme protège non seulement l'anonymat du tag mais permet également au serveur d'identifier le tag dans sa base des données avec une complexité de calcul O (1), car le serveur peut utiliser directement le pseudonyme pour localiser l'entrée correspondante dans sa base des données et effectuer les calculs nécessaires pour cette entrée correspondante uniquement. De plus, chaque tag ne nécessite qu'une quantité constante des valeurs internes O (1) du stockage de clé [24]. Ce sont ces excellentes caractéristiques qui le rendent assez attrayant que l'autre approche. Cependant, en raison de l'exigence de synchronisation, les systèmes basés sur VP sont enclins aux attaques de désynchronisation. La figure 1 illustre les principales idées de ces approches.

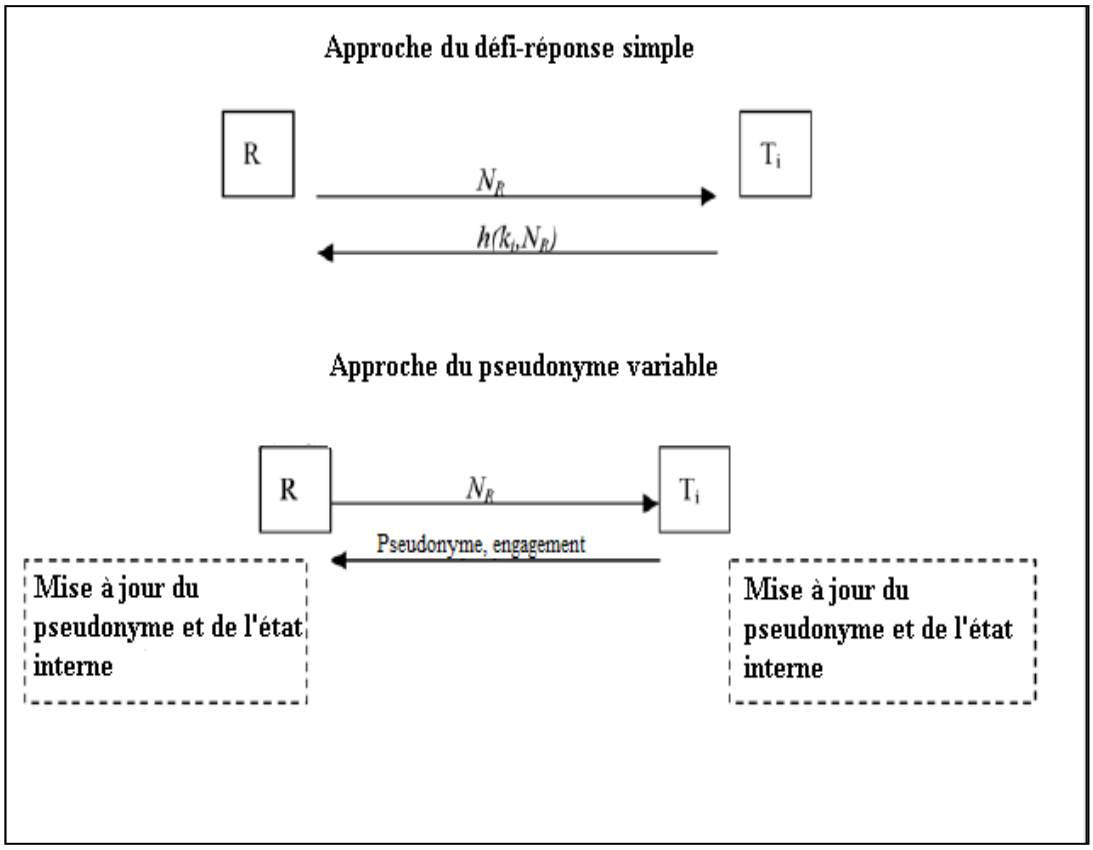


Figure 3-1 : Approches pour protéger l'identité des tags RFID [24]

3.7 Protocoles d'authentification exemplaires

Dans cette partie nous classifions des protocoles comme étant soit des méthodes à un seul tour ou à plusieurs tours, les notations utilisées sont introduites comme suit : r , r_T , r_R sont des nombres aléatoires à 1 bit. ID_T et ID_R représentent l'identité du tag T et l'identité du lecteur R respectivement. K_i est la clé secrète partagée entre le tag T_i et le lecteur R, h () et g() représentent des fonctions de hachage unidirectionnel sécurisées; h(), g():$\{0,1\}^* \rightarrow \{0,1\}^l$. f () est un générateur de nombres pseudo-aléatoires (fonction PRNG).

3.7.1 Protocole de Weis et al.

Weis et al. ont proposé une série de protocoles d'authentification RFID, leur protocole de contrôle d'accès est basé sur le hachage et le contrôle d'accès aléatoire [18].

- **Contrôle d'accès basé sur le hachage:** Chaque tag T_i compatible avec le hachage dans cette conception aura une portion de mémoire réservée à un méta-ID_i temporaire et fonctionnera dans un état verrouillé ou un état déverrouillé. Initialement, un propriétaire du tag stocke le hachage d'une clé aléatoire, méta-$ID_i \leftarrow h(k_i)$, dans le tag par le canal radio fréquence ou un contact physique pour verrouiller le tag. Le propriétaire stocke également la clé et le méta-ID_i dans un serveur principal. Dès la réception de la valeur méta-ID_i, le tag active son état verrouillé, et répond à toutes les requêtes avec seulement son méta-ID_i et n'offre aucune autre fonctionnalité. Pour déverrouiller le tag, le propriétaire se renseigne sur le tag et recherche la clé appropriée dans la base de données du back-end et transmet finalement la clé au tag. Le tag hache la clé reçue et la compare au méta-ID_i stocké. Si les valeurs correspondent, le tag se déverrouille et offre toutes ses fonctionnalités aux lecteurs à proximité [24]. Le protocole est illustré dans la figure 2.

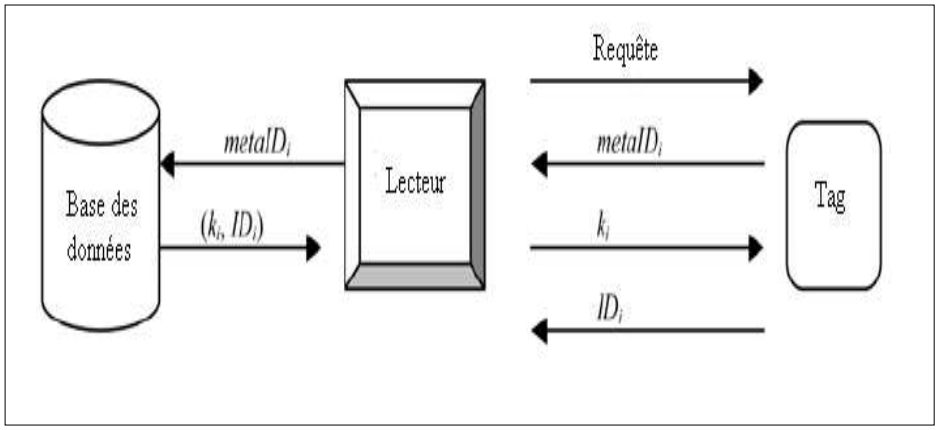


Figure 3-2 : Protocole du Weis et al. basé sur le hachage [24]

- **Contrôle d'accès aléatoire :** Dans le schéma précédent, le tag répond toujours avec son méta-ID_i aux requêtes, ce qui permet à toute partie de suivre un individu. Ainsi, Weis et al. ont proposé leurs systèmes de contrôle d'accès aléatoire où un tag ne répondra pas de façon prévisible aux requêtes par des utilisateurs non autorisés, mais doit encore être identifiable par les lecteurs légitimes. Les systèmes de contrôle d'accès aléatoire nécessitent des tags équipés d'un générateur de nombres aléatoires, en plus de la fonction du hachage unidirectionnelle. Lors de la réception d'une requête du lecteur, le tag répond avec les valeurs $(r, h(ID_i||r))$, où r est un nombre choisi aléatoire.

Un lecteur légitime identifie un de ses tags en effectuant une recherche par force brute de ses identifiants connus, hachant chacun d'eux concaténé avec r jusqu'à ce qu'il trouve une correspondance. Ce mode n'est possible que pour les propriétaires d'un nombre relativement faible de tags [24]. Le protocole est illustré à la figure 3.

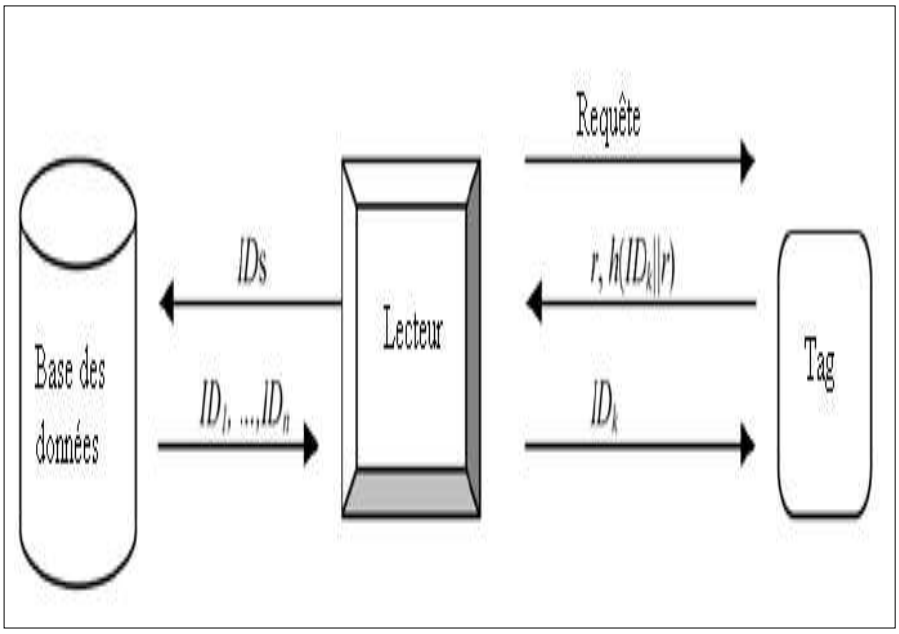


Figure 3-3 : Le contrôle d'accès aléatoire de Weis et al.

Les inconvénients

Le système d'accès aléatoire a été conçu pour protéger le méta-ID dans le système basé sur le hachage afin d'éviter le suivi individuel. Cependant, il est peu évolutif, il ne peut pas prendre en charge un grand nombre des tags car il doit effectuer une recherche par force brute pour trouver une identification correspondante. Il donne également à l'attaquant une très forte probabilité de trouver le tag correspondant, puisqu'il ne consulte qu'une petite base des données d'identifications possibles. Pire encore, le lecteur légal diffusera l'identifiant correspondant dans le canal direct de transmission. Ainsi, un attaquant pourrait enregistrer les données écoutées (r,h(ID_k||r))et facilement usurper les tags par la suite[24].

3.7.2 Protocole de Karthikeyan-Nesterenko

Karthikeyan et Nesterenko, basé sur une simple opération XOR⊕,et une opération matricielle, ont conçu un système efficace d'identification des tags et d'authentification des lecteurs. Initialement, deux matricesM_1 etM_2^{-1}sont stockées sur chaque tag, et deux matricesM_2 et M_1^{-1}sont stockées sur le lecteur, où toutes les matrices sont de taille p× p, etM_1^{-1}et M_2^{-1}sont les inverses de M_1 et M_2respectivement. Le tag et le lecteur stockent également une clé K qui est un vecteur de taille qoù q = r.p. Autrement dit, K peut être représenté par K = [K1, K2,…, Kr], oùK_i i= 1, 2 ..., r sont des vecteurs de taille p.Avec X = KM, où K est un vecteur de taille q et M est une matrice p× p,etXdésigne une multiplication par composants de K et M. Autrement dit, X = [X_1,…, X_r] = [K_1M,…, K_rM].

Lorsque le lecteur demande un tag, le tag calcule X = KM_1 et renvoie X au lecteur. Le lecteur transmet ensuite le message au serveur principal, où le serveur va rechercher dans sa base des données pour trouver une correspondance. S'il peut trouver une correspondance, le tag est identifié et le serveur effectue les opérations suivantes pour s'authentifier auprès du tag et renouveler la clé. Le serveur calcule d'abord Y = (K_1⊕ K_2 ⊕... ⊕K_r) M_2, sélectionne aléatoirement un nouveau vecteur X_{nv} de taille q, calculeK_{nv} = X_{nv} M_1^{-1}et Z = K_{nv} M_2, et envoie finalement (Y, Z) au lecteur, qui transmet (Y, Z) au tag. Lors de la réception de la réponse du lecteur, le tag vérifie si l'équation :Y M_2^{-1}=(K_1⊕ K_2 ⊕... ⊕K_r)est vraie, si c'est le cas le tag met à jour la clé en K_{nv}= ZM_2^{-1}le protocole est illustré dans la figure 4.[23]

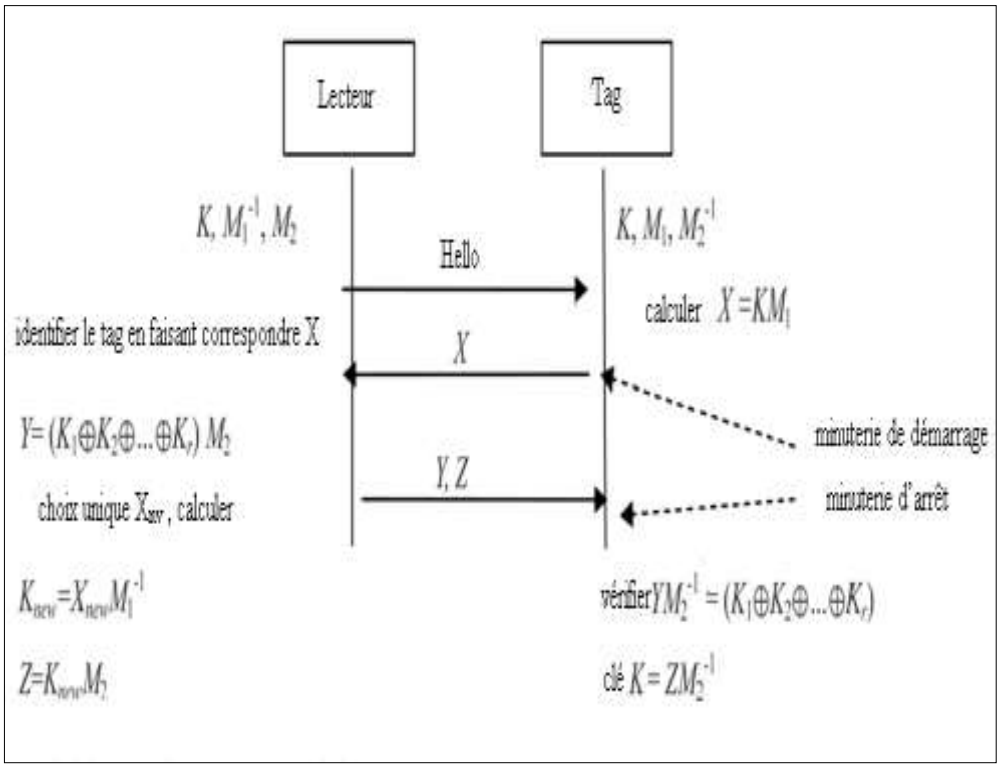


Figure 3-4 : Protocole du Karthikeyan-Nesterenko [24]

Les Inconvénients

Le système ne peut pas résister aux attaques et menaces suivantes attaque par déni de services (DOS), attaque par rejeu et traçage individuel. Dans le protocole de Karthikeyan-Nesterenko, le tag n'authentifie pas la valeur reçue Z lors de la mise à jour de la clé. Par conséquent, un attaquant peut remplacer le Z transmis par un ancien $\overline{Z}$ ou une valeur aléatoire Z* sans être remarqué, après avoir reçu un Y valide et le faux Z*le tag authentifiera le Y avec succès, puis mettra à jour la clé comme $K^{*}=M_2^{-1} \cdot Z^{*}$. Ainsi, le lecteur légitime et le tag ne peuvent plus s'authentifier puisque la clé n'est pas mise à jour correctement. Si l'attaquant remplace le Z par un ancien $\overline{Z}$ (en supposant que $\overline{Y}$ et $\overline{Z}$sont déjà envoyés dans la $i^{ème}$ session légale) dans l'attaque mentionnée ci-dessus, alors l'attaquant peut rejouer le $\overline{Y}$ dans la prochaine session pour tricher le tag en acceptant à tort la demande et accéder au tag en conséquence. Il peut même enregistrer les données transmises de plusieurs sessions, puis lance l'attaque ci-dessus plusieurs fois. Cela permettra à l'attaquant de tracer le tag. Par conséquent, la propriété de l'anonymat est violée.

3.7.3 Protocoles de Peris-Lopez et al.

Peris-Lopez et al. ont proposé une série de protocoles d'authentification RFID ultra-légers qui ont été conçus pour des tags à très faible coût. Leurs protocoles étaient très efficaces et n'impliquent que de simples opérations sur les bits. Nous passons en revue le protocole d'authentification mutuelle léger LMAP, qui est l'un des protocoles de Peris-Lopez et al.

LMAP n'implique que des opérations simples au niveau du bit: XOR ($\oplus$), AND ($\wedge$), OR ($\vee$),Le générateur des nombres aléatoires n'est requis que sur le lecteur. Pour protéger l'anonymat des tags, ils adoptent la technique des pseudonymes (IDS), d'une longueur de 96 bits, qui est mis à jour à chaque authentification réussie. Chaque tag partage un IDS et quatre clés (appelées K1, K2, K3 et K4, chacune de 96 bits) avec les lecteurs, et ils mettent à jour l'IDS et les clés après une authentification réussie. Il a besoin de 480 bits de mémoire en lecture/écriture et de 96 bits pour le numéro d'identification statique (ID). Le protocole se compose de trois étapes: phase d'identification des tags, phase d'authentification mutuelle et mise à jour des pseudonymes et phase de mise à jour des clés. Dans ce qui suit, ID_i désigne l'identification statique de tag_i, IDS^n_i désigne le pseudonyme du Tag_i à la $n^{ème}$ exécution, et $K1_i^n$/ $K\ 2_i^n$/ $K\ 3_i^n$/ $K\ 4_i^n$désignent les quatre clés de Tag_ià la $n^{ème}$ exécution. LMAP est représenté sur la figure 5. [25]

- **Identification du tag**: Initialement, le lecteur envoie « Hello » au tag_i, qui répond avec son IDS^n_iactuel.
- **Phase d'authentification mutuelle**: Le lecteur utilise IDS^n_i pour trouver les quatre clés correspondantes dans sa base de données, via l'aide du serveur back-end. Il sélectionne ensuite aléatoirement deux entiers n1 et n2, et calcule les valeurs A, B et C (les équations de calcul sont spécifiées sur la figure 5. De A || B || C, tag_i extrait d'abord n1 de A, puis vérifie la valeur de B. Si la vérification réussit, il extrait n2 de C et calcule la valeur de réponse D. À la réception de D, le lecteur vérifie les données D pour authentifier le tag.
- **Mise à jour du pseudonyme et de la clé**: Une fois le lecteur et le tag se sont authentifiés, ils mettent à jour leur pseudonyme et leurs clés locaux comme il est indiqué sur la figure 5.

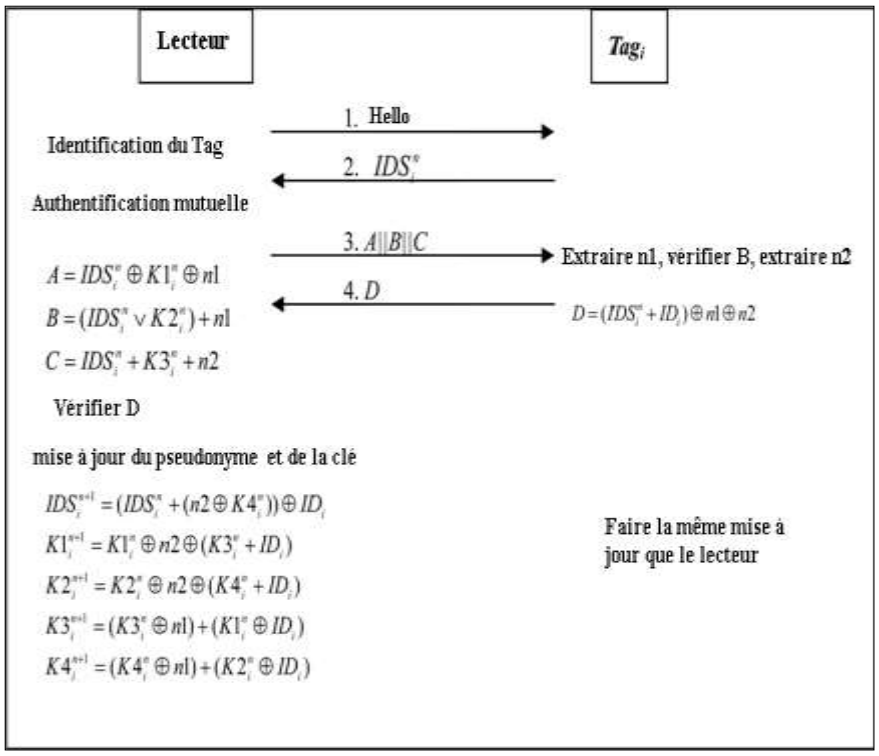


Figure 3-5 : Protocole d'authentification mutuelle légère LMAP

L'authentification du lecteur et du tag dans LMAP dépend de la synchronisation du pseudonyme et des clés. Cependant, il est très facile de désynchroniser ces valeurs en intercepter les données à l'étape 4 indiqué dans la figure 5 par l'attaque par déni de service (DOS).

3.8 Conclusion

La sécurité et le respect de la vie privée dans les systèmes RFID sont un aspect important qui nécessite une attention particulière car sans contrôle d'accès, n'importe qui peut lire les informations stockées sur les tags RFID. Par conséquent, les recherches actuelles en matière de technologie RFID ne se concentrent pas uniquement sur le système d'identification. Des mécanismes d'authentification et de contrôle d'accès sûrs et efficaces ont reçu beaucoup d'attention dans les recherches proposées. Ce chapitre examine les principales préoccupations en matière de protection de la vie privée, fuite d'informations d'un tag, traçabilité de la personne et usurpation d'identité du tag. Le problème de l'usurpation d'identité est toujours le premier à être analysé et résolu dans chaque cas, sinon l'attaquant peut collecter les informations envoyées par le tag et tenter une attaque d'usurpation ou attaque par rejeu pour usurper l'identité d'un tag cible. Ainsi la divulgation des informations lors d'une transmission de données peut révéler diverses informations personnelles à l'insu du possesseur du tag. Toutefois, la plupart des protocoles proposés ne peuvent pas vraiment éviter le problème de la traçabilité. Pour cela Nous pensons que malgré les efforts en termes de protocoles et les ressources nécessaires pour faire des calculs et des hachages, il est préférable d'avantager pour la sécurité des RFID, des solutions d'authentification physique.

Chapitre 4

Simulation et conception

Chapitre 4 : Simulation et conception

Présentation du chapitre

L'objectif de ce chapitre est de simuler et concevoir un système de contrôle d'accès basé sur RFID. D'abord nous commençons par la description du projet à simuler et les logiciels utilisés, puis nous présentons les composants du système et ses caractéristiques. Ensuite nous abordons la programmation par arduino IDE, ses fonctions et le code pour que notre système soit réalisable. Enfin nous présentons la méthode de compilation et de téléchargement du programme sur une carte arduino.

Sommaire

4.1 Introduction

La RFID (Radio Frequency Identification) est utilisée pour l'échange d'informations sans fil grâce à l'utilisation de champs électromagnétiques. Ces dispositifs RFID sont utilisés avec des lecteurs RFID pour saisir des informations et les traiter en conséquence pour une action spécifique comme l'autorisation pour l'accès. L'utilisation de la technologie RFID pour le contrôle d'accès permet aux organisations d'améliorer leur efficacité et d'appliquer des politiques concernant l'accès et la présence. Toutes les données d'identification sont stockées dans une base de données centrale et peuvent être mises à jour rapidement et facilement en cas de besoin, notamment en cas de changement de statut des autorisations ou de vol de cartes d'identité (ou de leurs données). Pour cela nous allons simuler et concevoir un système de sécurité et de contrôle d'accès à une zone sécurisée basé sur la RFID.

4.2 Description du projet

L'objectif principal de ce projet est d'assurer la sécurité d'une organisation en ne permettant qu'au personnel autorisé d'accéder à la zone sécurisée. Pour cette raison, seule la personne autorisée possédant un tag RFID valide est autorisée à pénétrer dans les locaux sécurisés. Ce tag contient un circuit intégré qui est utilisé pour stocker les informations dont un numéro d'identification unique. Notre système travaille automatiquement, en ouvrant la porte sans pression des boutons et sans utilisation des télécommandes. Les utilisateurs auront des cartes enregistrés pour accéder à une zone précise. Une fois que la personne présente le tag RFID au lecteur de carte, le numéro de série de ce tag est détecté et ainsi comparé à un numéro de série enregistré dans le logiciel ou dans une base de données. Si l'accès est accepté une LED verte va s'allumer avec une écriture « accès autorisé » sur l'afficheur et l'ouverture de la porte à l'aide d'un servomoteur. Si le cas contraire une LED rouge s'allume avec l'écriture « accès refusé » affichée. Pendant ce processus de rejet des utilisateurs, des bips caractéristiques seront émis sur un buzzer (tout comme une annonce sonore).

4.3 Méthodes et outils

4.3.1 Software

- **Arduino Software (IDE)**

L'environnement de développement intégré arduino ou arduino software (IDE) contient un éditeur de texte pour écrire le code, une zone de message, une console de texte et tous les outils nécessaires à l'activité de programmation. Aarduino IDE est le logiciel qui permet de programmer les cartes arduino. Vous pouvez donc saisir votre programme, l'enregistrer, le compiler, le vérifier et le transférer sur une carte srduino.

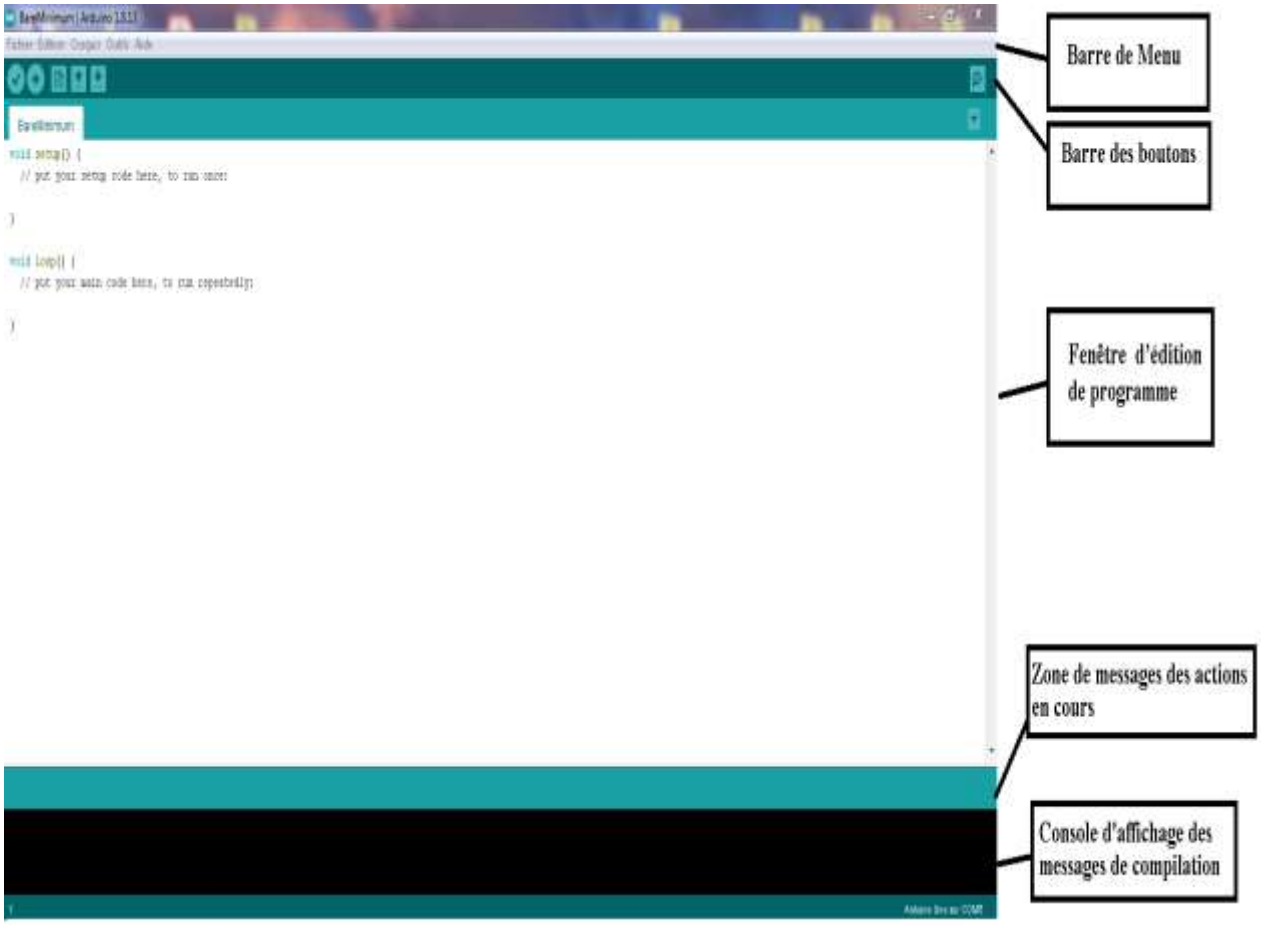


Figure 4-1 : Interface arduino IDE

- **Fritzing**

Fritzing software est un logiciel open-source intéressant pour aider les designers, les artistes, les chercheurs et les amateurs à travailler de manière créative avec l'électronique interactive et à développer des projets électroniques. Fritzing permet de concevoir de façon entièrement graphique le circuit électronique et de documenter les prototypes.

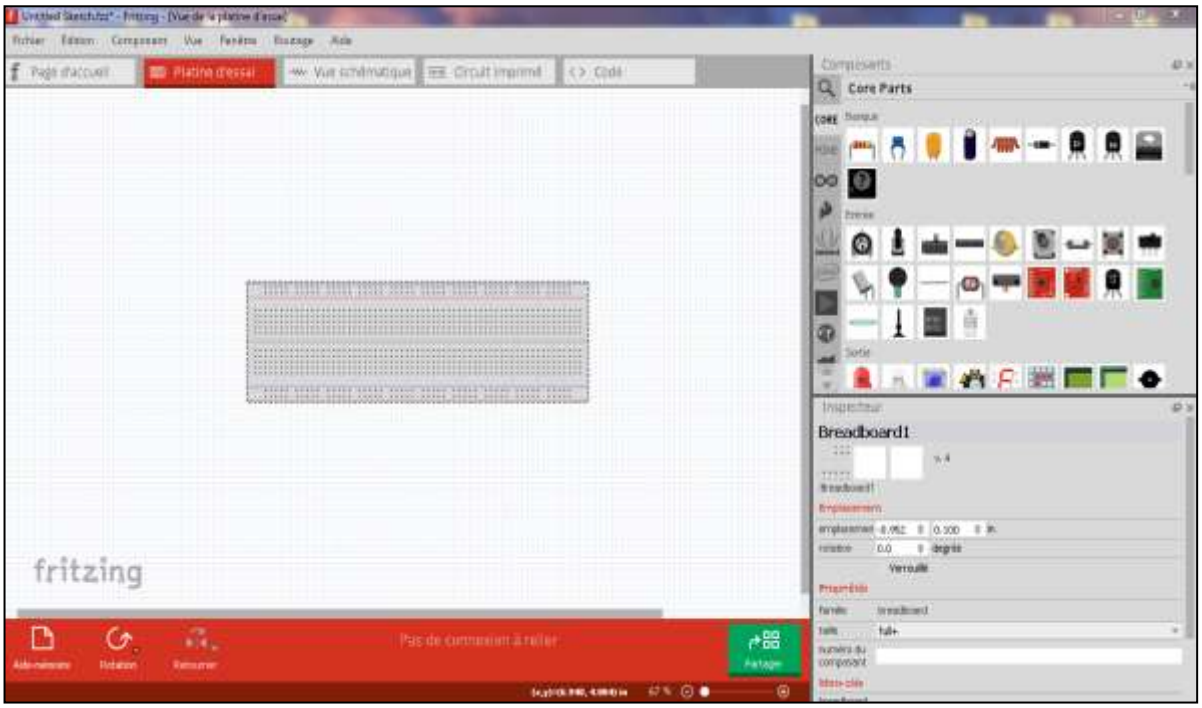


Figure 4-2 : Interface Fritzing

- **Proteus Professional**

Proteus Professional est une suite logicielle destinée à l'électronique, éditée par la société Labcenter Electronics. Les logiciels inclus dans Proteus Professional permettent la construction assistée par ordinateur dans le domaine électronique. Proteus est composé de deux logiciels principaux : ISIS, permettant la création de schémas et la simulation électrique, et ARES, destiné à la création de circuits imprimés.

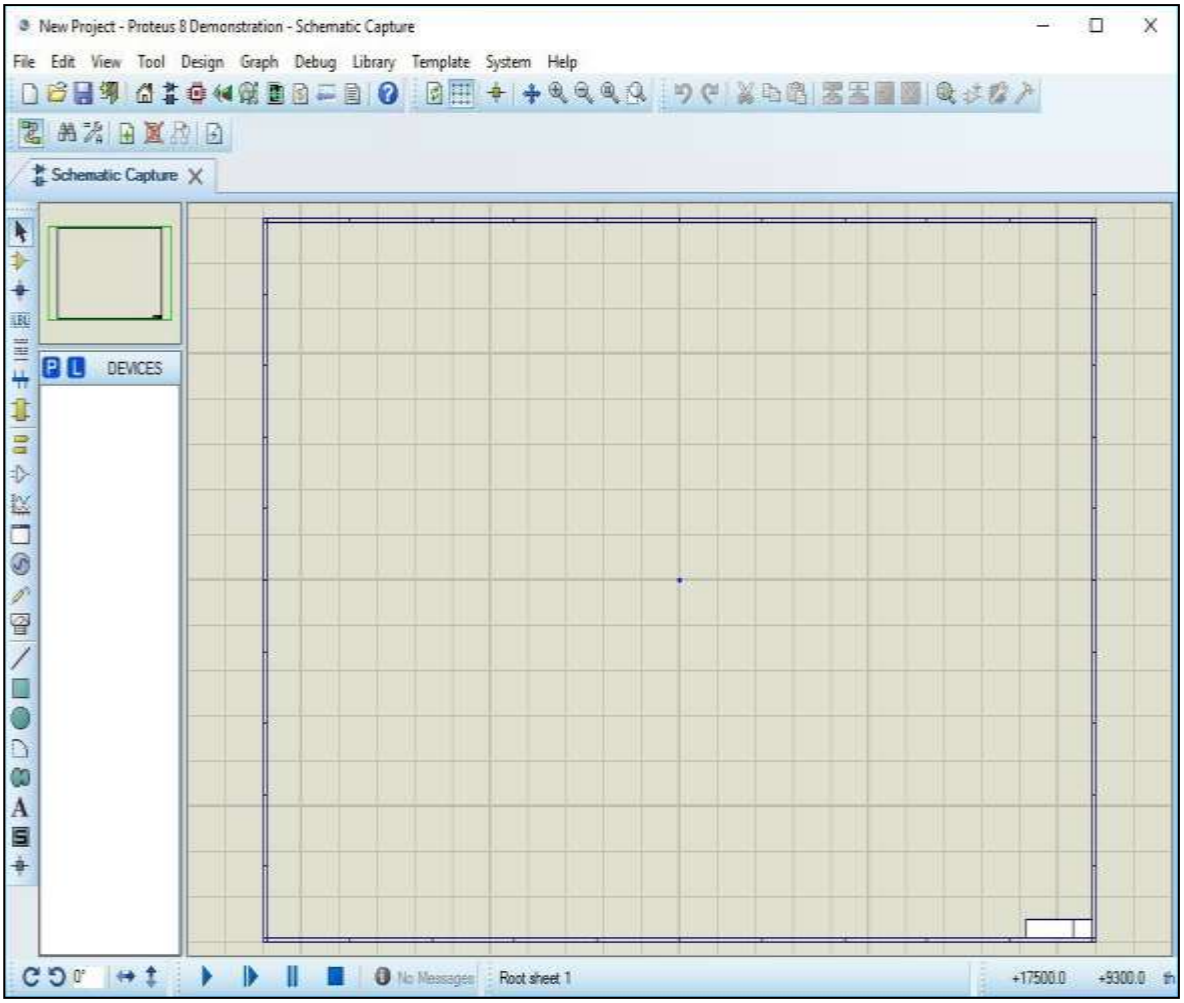


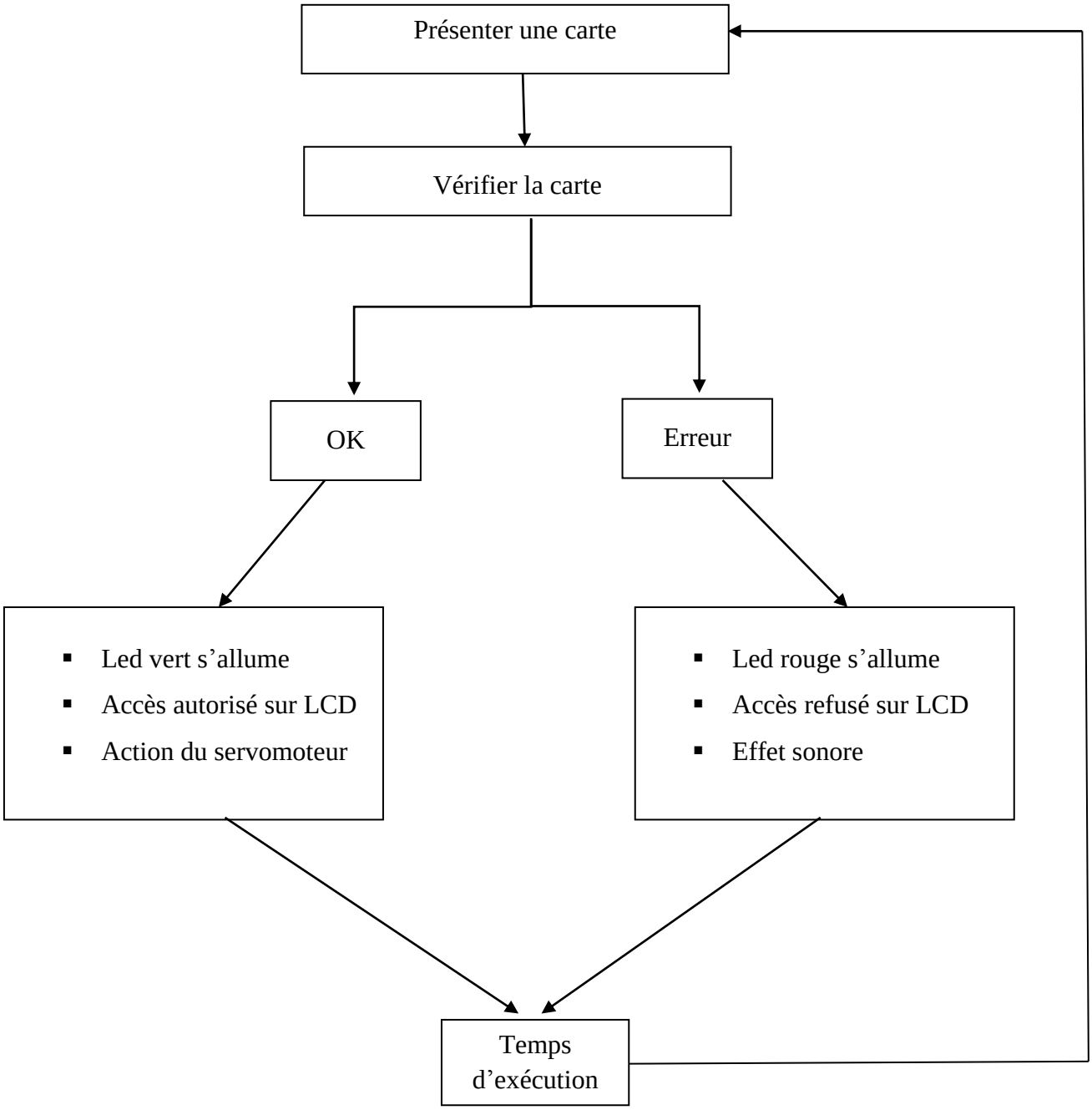
Figure 4-3 : Interface Proteus professional

4.3.2 Constitution du projet

Le système proposé se compose des sections suivantes :

- Entrée : Module RFID RC552
- Unité de contrôle : Arduino Uno (microcontrôleur ATmega328P)
- Sortie : Afficheur LCD, deux LED, buzzer et servomoteur.

❖ **Diagramme d'activité du système du contrôle d'accès**



4.4 Les composants

4.4.1 Arduino UNO

Arduino UNO est une carte de développement qui dispose d'un microcontrôleur ATmega328P. Elle possède 14 broches d'entrée/sortie numériques (dont 6 peuvent être utilisées comme sorties la modulation de largeur d'impulsions (MLI), 6 entrées analogiques, un résonateur céramique de 16 MHz, une connexion USB, une prise d'alimentation et un bouton de réinitialisation. Il contient tout le nécessaire pour supporter le microcontrôleur, il suffit de le connecter à un ordinateur avec un câble USB ou de l'alimenter avec un adaptateur CA-CC ou une batterie pour démarrer. La carte UNO est la carte idéale pour commencer, pour les personnes qui se lancent dans le développement sur la plate-forme arduino. Il s'agit d'une carte reconnue pour sa robustesse en matière d'expérimentation. Pour les utilisateurs plus expérimentés, elle reste la carte idéale pour le prototypage rapide. [28]

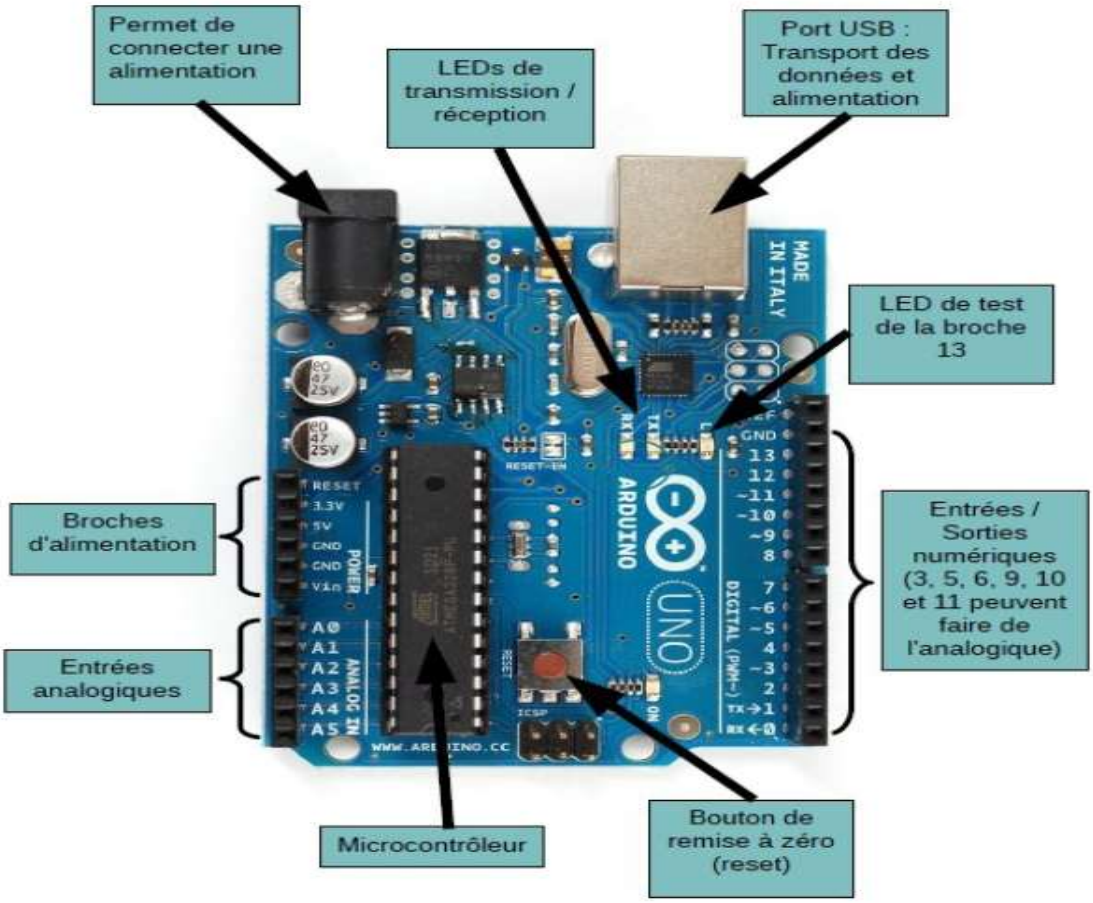


Figure 4-4 : Carte arduino uno

4.4.2 Le module RC522

Le RC522 est un module RFID à 13,56 MHz qui permet l'identification sans contact à partir d'un badge ou une clé RFID. Il est couramment utilisé dans les systèmes de présence et autres applications d'identification de personnes/objets.

Caractéristiques du RC522	
Fréquence de travail	13,56 MHz
Tension de fonctionnement	2,5V à 3,3V
Communication	Protocole SPI
Débit de données maximum	10Mbps
Portée de lecture	5 cm
Consommation de courant	13-26mA
Consommation en mode de mise hors tension	10uA (min)

Tableau 4-1 : Caractéristiques du module RFID [29]

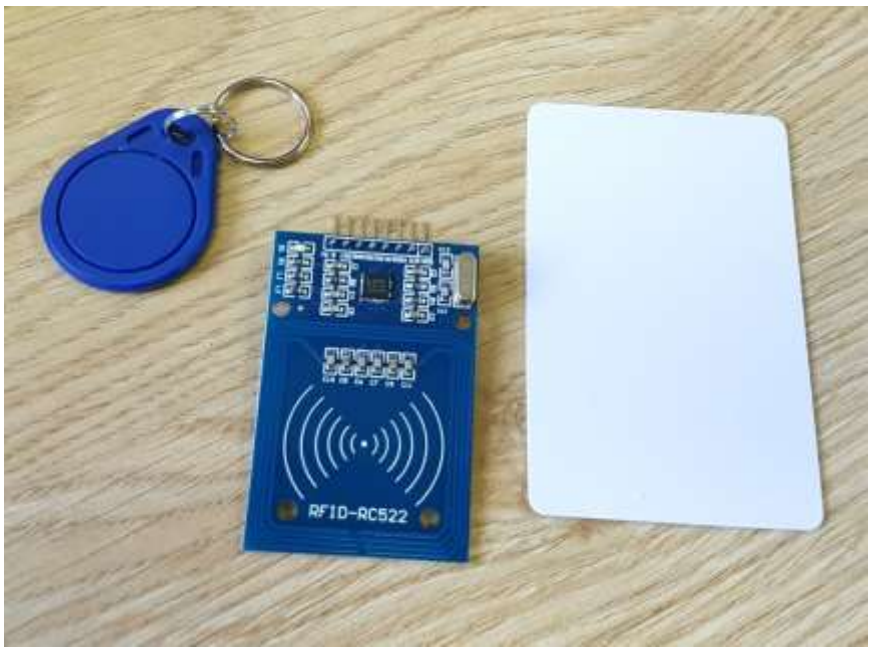


Figure 4-5: Lecteur RFID aves ses accessoires

4.4.3 Plaque d'essai

Une plaque d'essai permet de réaliser des montages électroniques sans soudure. Les composants sont insérés dans les prises de la platine d'assemblage et des fils isolants de cuivre de longueur et couleur variables sont utilisés pour établir les connexions.

Figure 4-6: Plaque d’essai et fils de connexion

4.4.4 Afficheur LCD

Un écran à cristaux liquides ou LCD tire sa définition de son nom même, il utilise un cristal liquide pour produire une image visible. Les écrans à cristaux liquides sont des écrans d'affichage de technologie ultra-mince qui sont généralement utilisés dans les écrans d'ordinateurs portables, les téléviseurs, les téléphones portables et les jeux vidéo portables.

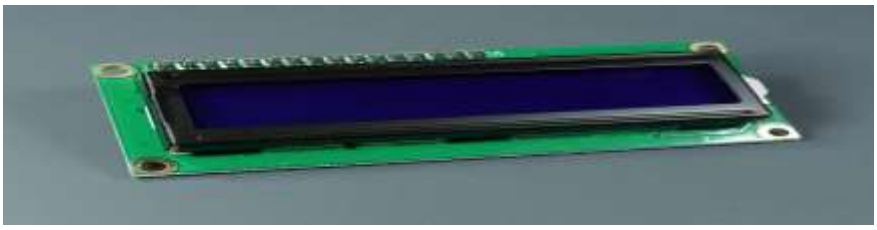


Figure 4-7: Afficheur LCD

4.4.5 La résistance

La résistance est un composant électronique ou électrique qui réduit le courant électrique. La capacité de la résistance à réduire le courant est appelée résistance et mesurée en ohms (symbole : Ω).

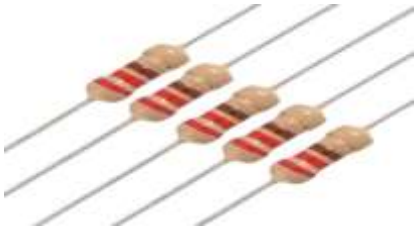


Figure 4-8 : Résistances

4.4.6 LED

LED diode électroluminescente est un dispositif qui convertit le courant électrique en énergie optique qui est utilisée ici comme indicateur pour différentes situations de système. Le connecteur le plus long du LED (anode) sera connecté à la borne positive du circuit, alors que le plus court (cathode) sera connecté à la borne négative

Figure 4-9 : LED

4.4.7 Buzzer

Un buzzer ou biper est un dispositif de signalisation audio, qui peut être mécanique, électromécanique ou piézoélectrique. C'est un composant qui émet un son lorsqu'une tension est présente à leurs bornes.

Figure 4-10 : Buzzer

4.4.8 Servomoteur

Un servomoteur est un actionneur rotatif qui permet un contrôle précis en termes de position angulaire, d'accélération et de vitesse. Le servomoteur est alimenté avec 3 fils: une entrée 5V, une masse et une entrée d'impulsion (la commande du servomoteur) qui désigne un signal numérique modulé en impulsions qui sera converti en un angle par un système électronique intégré dans le servomoteur.

Figure 4-11 : Servomoteur

4.5 Connexion et câblage

4.5.1 Câblage module RFID

RFID–RC522	**Arduino UNO**
SDA	Digital Pin 10
SCK	Digital Pin 13
MOSI	Digital Pin 11
MISO	Digital Pin 12
RST	Digital Pin 9
3.3 V	3.3 V
GND	GND

Tableau 4-2 : Connexion arduino et module RFID

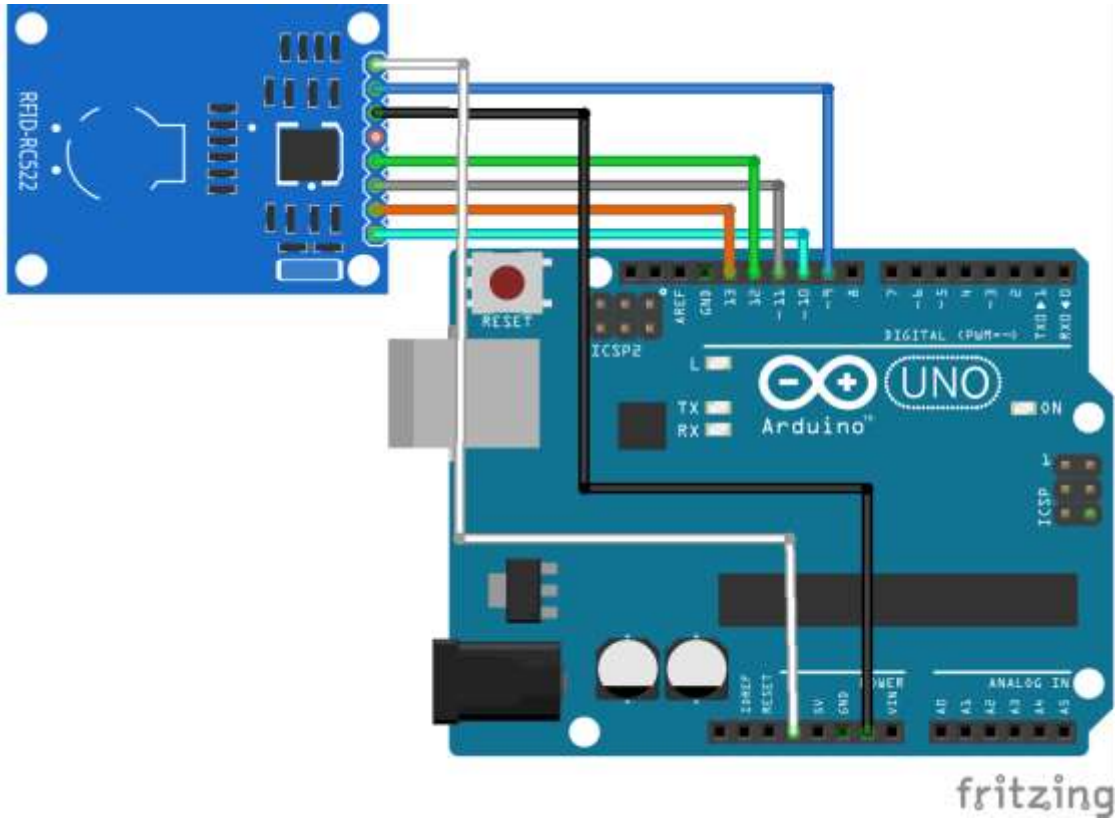


Figure 4-12 : Montage carte arduino+lecteur RFID

4.5.2 Câblage de LED

La connexion de la plaque à la broche GND de la carte. Puis l'emplacement des 2 LED rouge et verte en parallèle sur la plaque dont les anodes sont reliés avec deux résistances 220 Ohms. Les cathodes de LED rouge et LED vert sont attachés respectivement aux broches 4 et 5.

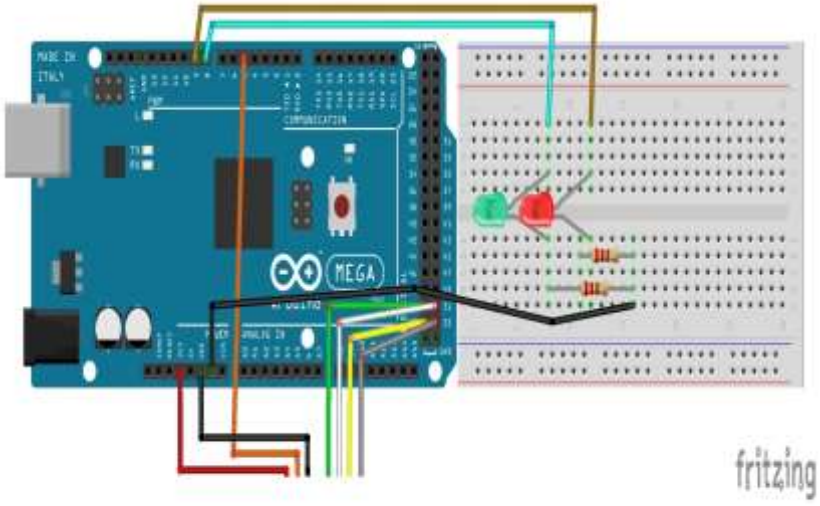


Figure 4-13 : Montage carte arduino+2 LED

4.5.3 Câblage du buzzer

L'entrée de buzzer est le port 9 de l'arduino via une résistance et la sortie est attachée à la masse GND.

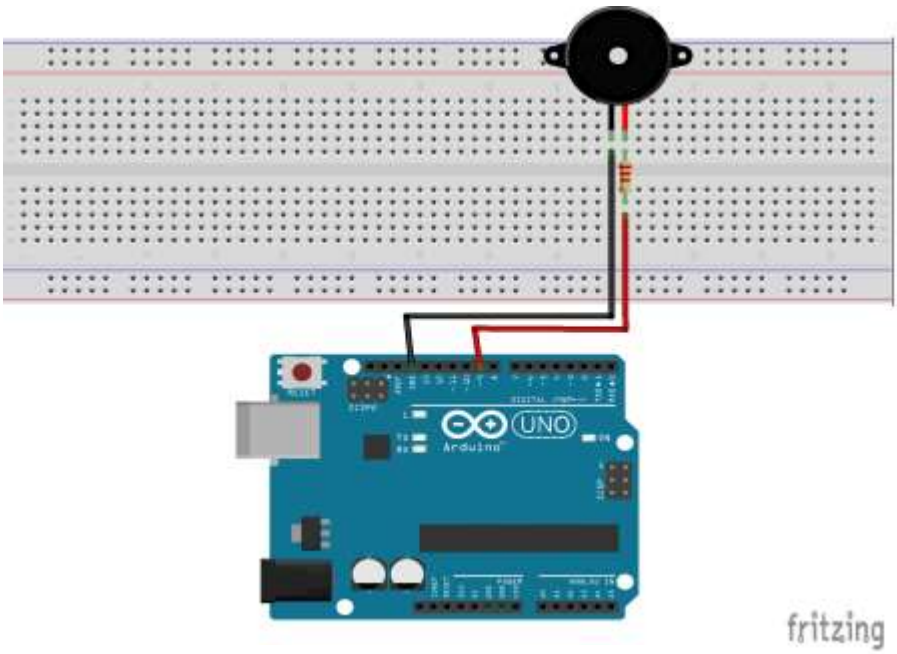


Figure 4-14: Montage catre arduino+buzzer

4.5.4 Câblage d'un afficheur LCD

L'afficheur LCD étudié est un écran permettant l'affichage de 16x2 caractères, c'est-à-dire deux lignes de 16 caractères, avec un potentiomètre pour ajuster le contraste. Le transfert des données sous forme de bits est pris en compte par la bibliothèque LiquidCrystal.

Arduino	**LCD**
La masse GND	La broche VSS
L'alimentation 5v	La broche VDD
port digital 12	La broche RS
RW	GND
Port Digital 11	La broche E
Port Digital 4	Les broches D4
Port Digital 5	Les broches D5
Port Digital 6	Les broches D6
Port Digital 7	Les broches D7

Tableau 4-3 : Connexion arduino et afficheur LCD [31]

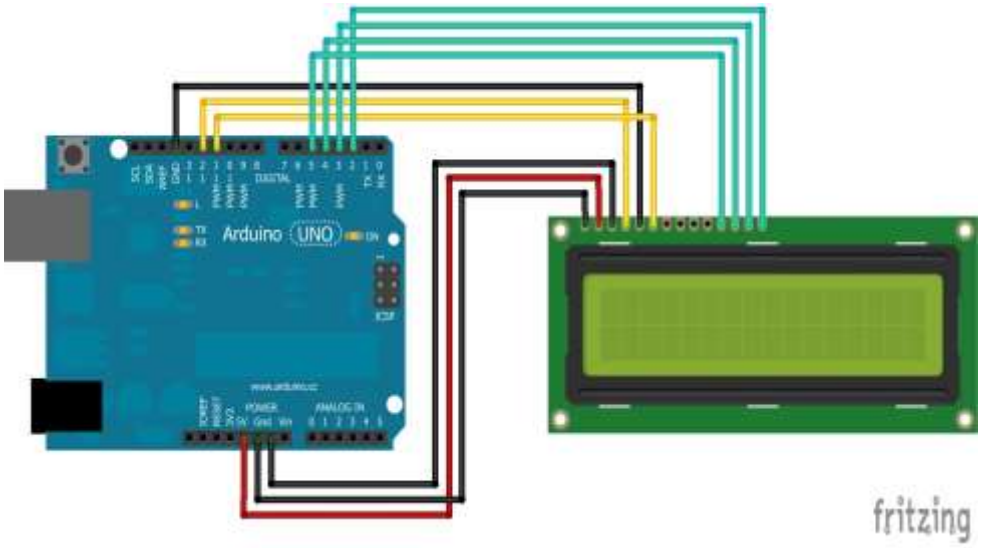


Figure 4-15: Montage carte aduino+afficheur LCD

4.5.5 Câblage du servomoteur

Le servomoteur a trois fils. La couleur des fils varie selon les servomoteurs, mais le fil rouge est toujours de 5V et le GND sera soit noir soit marron. L'autre fil est le fil de commande et il est généralement orange ou jaune.

Arduino	**Servomoteur**
GND	GND
+5 v	+5 v
Pin 9	Signal (fil de commande)

Tableau 4-4 : Connexion arduino et servomoteur [31]

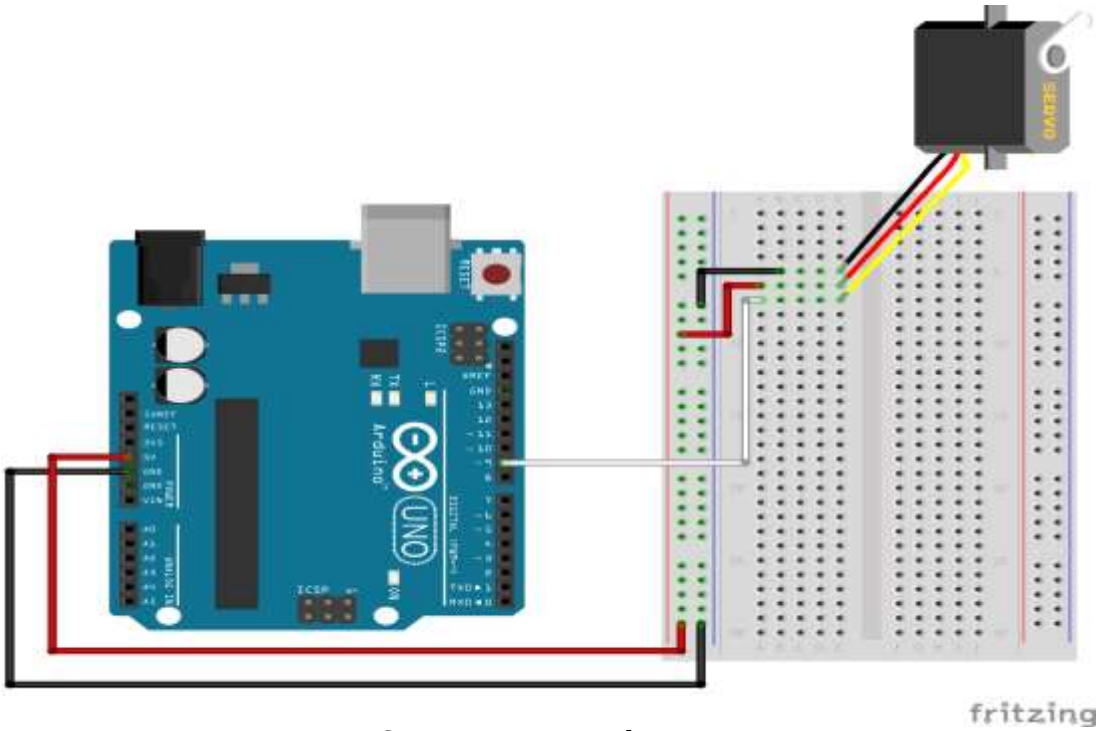


Figure 4-16: Montage carte aduino+servomoteur

4.6 Le schéma général (Fritzing)

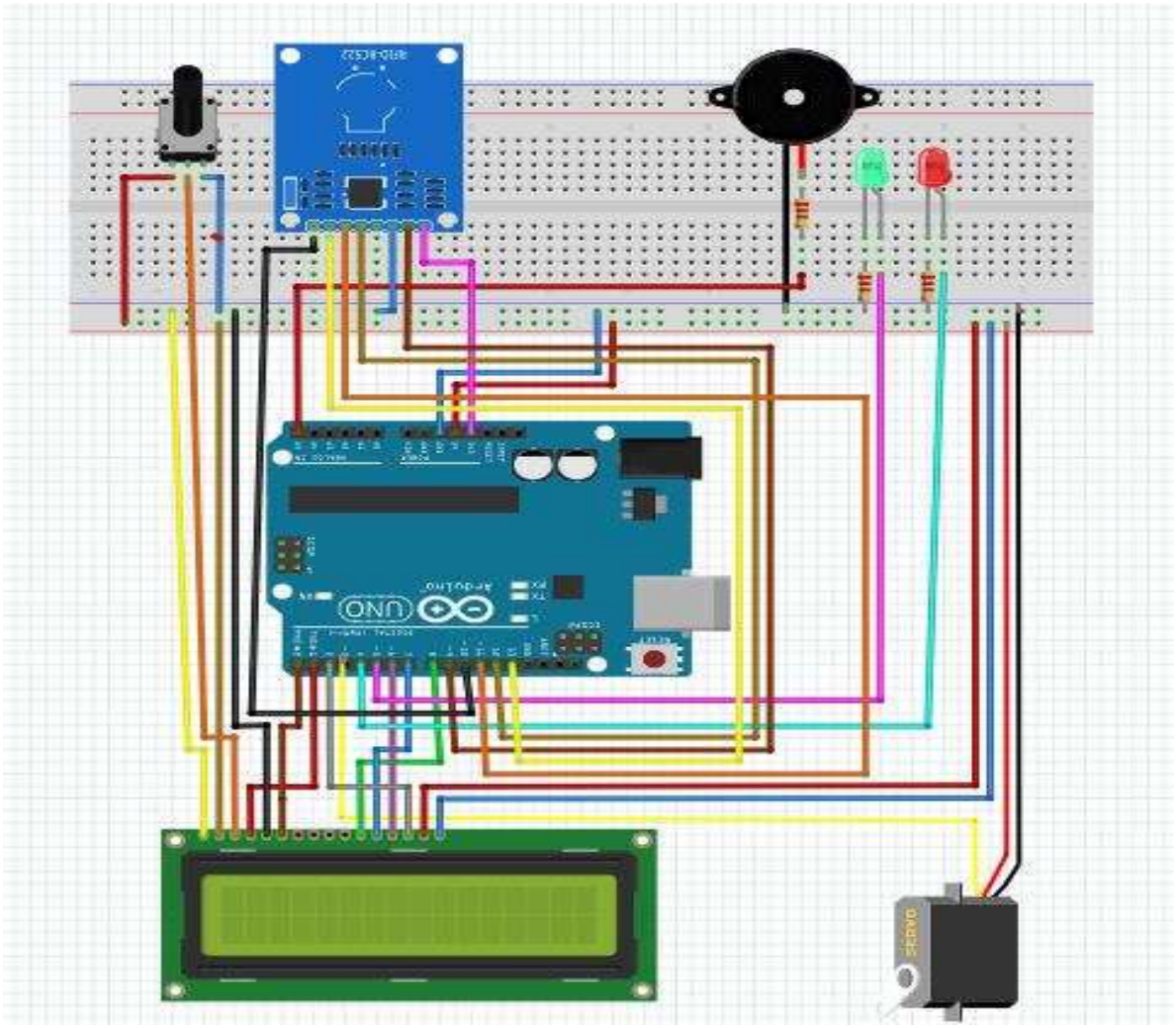


Figure 4-17: Schéma général en Fritzing

4.7 La programmation

La programmation de la carte arduino se fait par le logiciel arduino IDE qui est basé sur la programmation en langage C et C++. Le programme arduino est une série d'instructions élémentaires sous forme textuelle (ligne par ligne). La carte lit et exécute les instructions séquentiellement dans l'ordre défini par les lignes de code.

Le programme est en minimum composé des deux fonctions obligatoires :

- La fonction d'initialisation void setup () utilisé pour initialiser et fixer les variables, configurer les entrées, les sorties, le sens des broches et les bibliothèques. Elle est exécutée une seule fois au démarrage.
- La fonction void loop () est pour la définition des opérations à effectuer, elle est exécutée en boucle infinie une fois que la fonction setup () a été exécutée.

Bien noter que :

- Toutes les lignes commençant par // sont ignorées par le compilateur et sont appelées des commentaires.
- Le code de la fonction est compris entre des accolades qui sont des bornes délimitant la fonction.
- Chaque commande ou instruction est terminée par un point-virgule.

❖ **Bibliothèques**

- L'interface périphérique série (SPI): Cette bibliothèque permet de communiquer avec les appareils SPI, avec l'arduino comme appareil maître.
- MFRC522 : Permet de lire/écrire une carte ou un tag RFID.
- Servo : Permet aux cartes arduino de contrôler une variété de servomoteurs.
- LiquidCrystal : Cette bibliothèque permet à une carte arduino de contrôler des écrans à cristaux liquides (LCD).

4.8 Le programme général

```
// Programme : RFID - Contrôle d'accès
// --------------------------------------------
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <LiquidCrystal.h>
Servo microservo9g;
LiquidCrystal lcd(1, 0, 8, 7, 6, 2);
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);
int led_ok = 5;// LED d'accès autorisé est attachée au port num 5
int led_no = 4;// LED d'accès refusé est attachée au port num 4
const int buzzer = A5; // Buzzer branché au port pin A5
//-----------------------------------------------------
void setup()
{
pinMode(led_ok, OUTPUT);
pinMode(led_no, OUTPUT);
pinMode(buzzer, OUTPUT);
microservo9g.attach(3);// Servo est attaché au port num 3
microservo9g.write(90); // Angle du mouvement de servo
SPI.begin(); // Initialisation de SPI bus
mfrc522.PCD_Init(); // Initialisation de MFRC522
lcd.begin(16, 2);// Nombres de lignes et de colonnes de LCD:
lcd.print("SVP, INSERER LA ");// Message affiché sur LCD.
lcd.setCursor(4,2);//On place le curseur sur le caractère 4 de la ligne 2.
lcd.print(" CARTE ");// Message affiché sur deuxième ligne
}
```

```
//-------------------------------------------------------------
void loop()
{
// Attend le rapprochement des cartes
if ( ! mfrc522.PICC_IsNewCardPresent())
{
return;
}
// Lecture des cartes
if ( ! mfrc522.PICC_ReadCardSerial())
{
return;
}
String contenu= "";
for (byte i = 0; i < mfrc522.uid.size; i++)
{
contenu.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
contenu.concat(String(mfrc522.uid.uidByte[i], HEX));
}
contenu.toUpperCase();
// Procédures pour les cartes Autorisées
if (contenu.substring(1) == "EC 58 2F CB" || contenu.substring(1) == "B5 29 CF 65" )
{
lcd.begin(16, 2);
digitalWrite(led_ok, HIGH);
lcd.print("Accès Autorisé");
delay(1000);
microservo9g.write(-90);
delay(3000);

microservo9g.write(90);

digitalWrite(led_ok, LOW);

}
```

```
// Procédures pour les cartes refusées
if (contenu.substring(1) == "D6 3C F4 08" )
{
lcd.begin(16, 2);
digitalWrite(led_no, HIGH);
tone(buzzer, 1000); // Send 1KHz sound signal...
lcd.print("Accès refusé");
delay(1000);
lcd.noDisplay();
delay(500);
lcd.display();
delay(1000);
lcd.noDisplay();
delay(500);
lcd.display();
delay(1000);
digitalWrite(led_no, LOW);
noTone(buzzer); // Stop sound...
}
lcd.clear();
lcd.print("SVP, INSERER LA ");
lcd.setCursor(4,2);
lcd.print(" CARTE ");
delay(1000);
   }
```

4.9 Les étapes

4.9.1 La compilation

C'est la vérification du programme avec le logiciel arduino IDE. Si des erreurs sont signalées dans la console d'affichage, on modifie le programme.

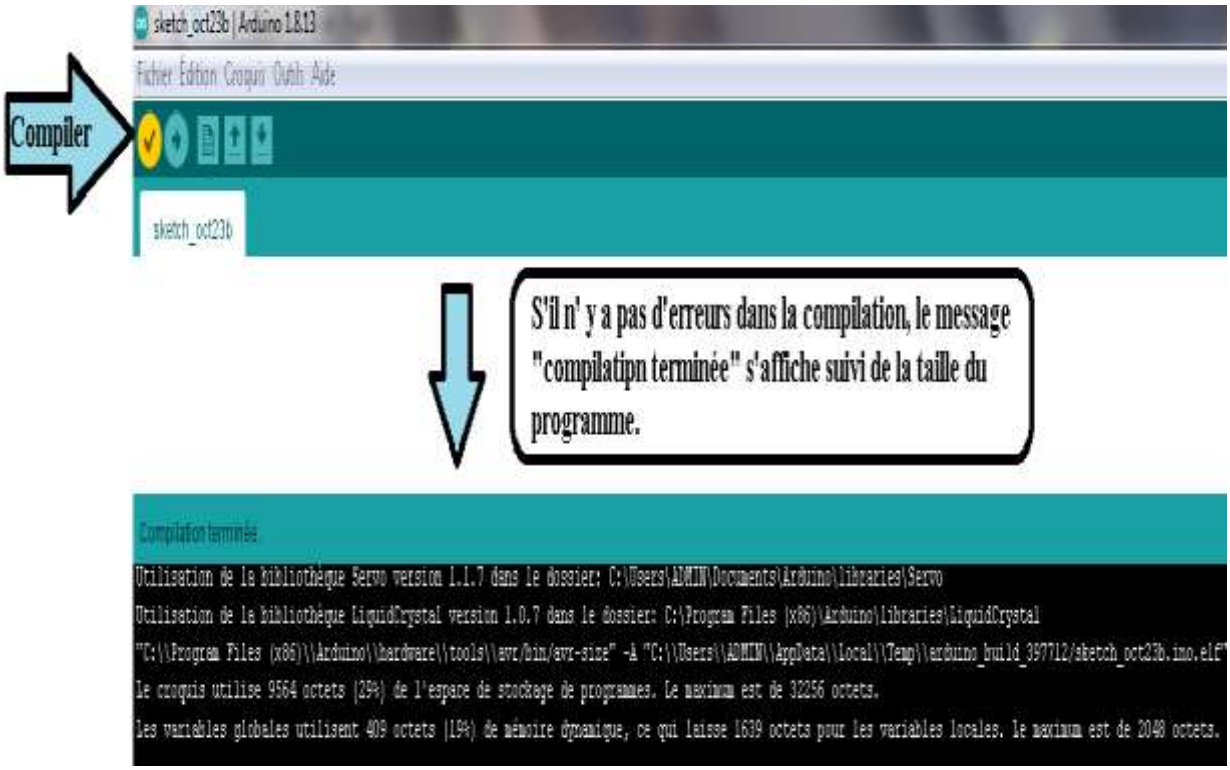


Figure 4-18: Compilation et vérification du programme

Après la compilation, le code source du programme est converti en code machine et généré par l'arduino IDE en un fichier HEX en sortie qui est indispensable pour la simulation et la programmation du microcontrôleur.

4.9.2 Simulation par Proteus Professional

Nous utilisons le logiciel Proteus pour la création d'un prototype virtuel, ce que nous permet de réduire les coûts matériels et logiciels lors de la conception d'un projet. Avant de commencer la simulation, nous devons d'abord charger et lier les différents composants que nous comptons utiliser. Une fois le schéma est saisi nous utilisons le fichier HEX pour lancer la simulation.

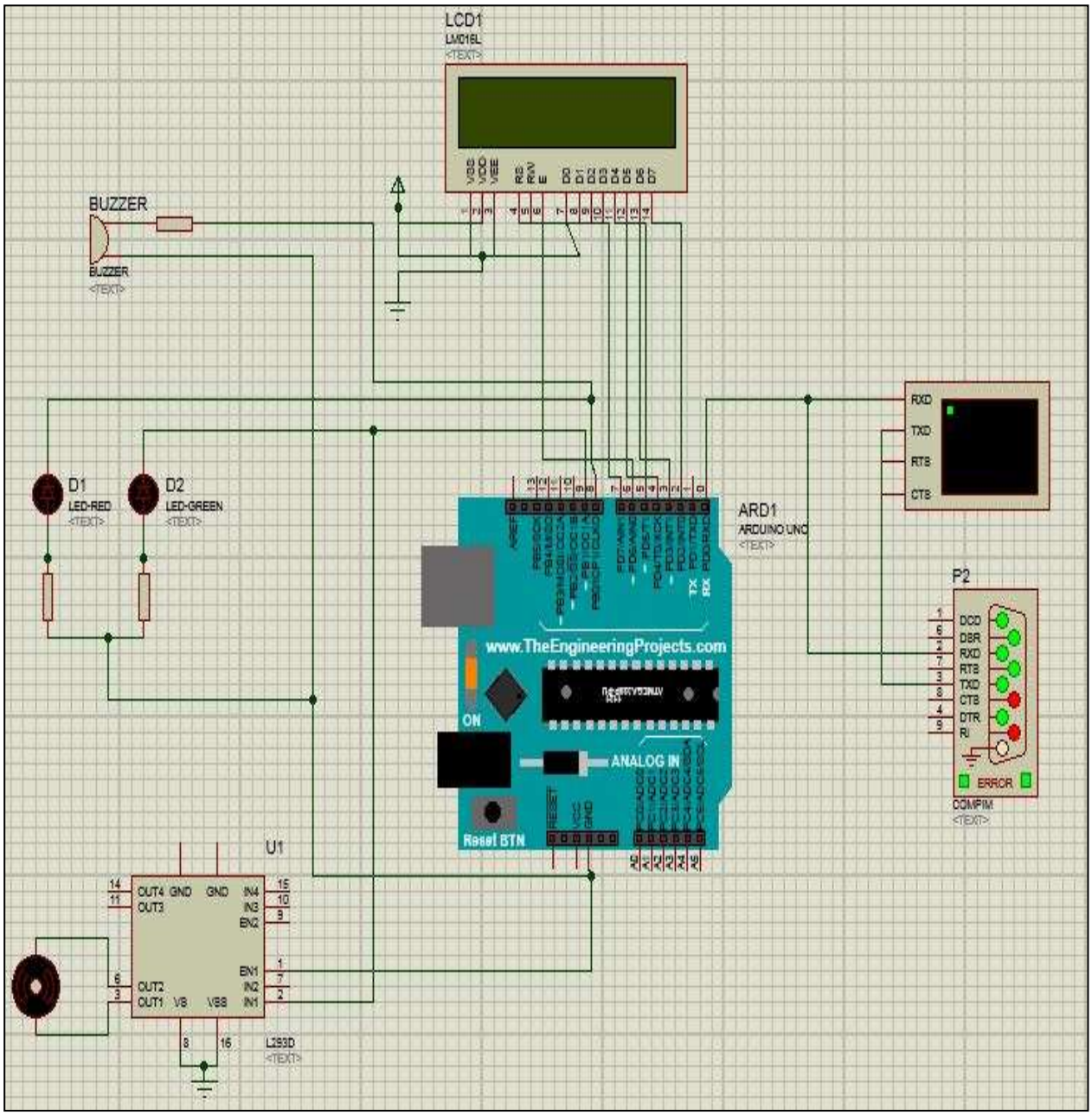


Figure 4-19: Simulation par Proteus Professional

4.10 Conclusion

Le système arduino, nous donne la possibilité de combiner les performances de la programmation et celles d'électronique. Le plus grand avantage de la programmation des équipements électroniques est qu'elle simplifie grandement les schémas électroniques et par conséquent, le coût de la réalisation. La connexion entre le système RFID et l'arduino se fait par un lecteur usb, permettant la communication avec les tags RFID à proximité, donc le contrôle d'accès. Durant ce projet nous avons simulé et conçu un système de RFID à base d'un lecteur RC522, un servomoteur qui sert à ouvrir une porte, un afficheur qui affiche si l'accès est accepté ou refusé, un buzzer et aussi deux LED rouge et verte pour la signalisation.

Conclusion générale et perspectives

Le travail présenté dans ce mémoire de master s'est porté sur la simulation d'un système RFID pour authentification par badges électroniques. Dans ce contexte nous avons abordé en détail les exigences des systèmes RFID dans les différents domaines, leurs principes de fonctionnement et les différentes fréquences de communication utilisés par les cartes RFID. Nous avons présenté la méthodologie d'extraction de l'information du capteur et l'authentification par RFID. En concluant les études sur la RFID par la simulation et la conception d'un système de contrôle d'accès en zone sécurisé avec une carte RFID, avec la présentation des phases nécessaires et les différents outils matériels et logiciels pour simuler et concevoir notre projet. Nous avons appris beaucoup de choses de ce projet même s'il n'a pas abouti à tous les résultats qu'on voulait atteindre et que le début fut un peu lent vu les besoins matériels requis.

Comme perspective concernant la technologie RFID, il est primordial de se préoccuper des problématiques de sécurité et de la vie privée, d'en comprendre les dangers car la technologie RFID n'est pas parfaite et les informations échangées par des radios fréquences durant une communication entre un tag et un lecteur peuvent être espionnées et prises clandestinement par des personnes extérieures.

La cryptographie s'avère en effet nécessaire pour deux raisons. D'une part parce que la RFID rend impossible le fait de savoir qui a eu accès à quelles données, quand et où, dans quel but, et qu'il convient d'éviter toute lecture ou interception furtives des données par un tiers non autorisé. D'autre part, puisqu'il est également nécessaire de limiter le risque d'altération ou de falsification des données, si d'aventure elles étaient néanmoins interceptées et clonées. Pour la fiabilité, il est recommandé de rendre chaque système basé sur la RFID publique, à la manière des logiciels open source, afin que la société civile puisse vérifier sa pertinence et son intégrité.

Finalement, on peut dire que l'identification par radio fréquence reste un domaine qui devrait encore être développé dans les prochaines années, et plusieurs ingénieurs et chercheurs travaillent déjà sur des standards pour mieux l'encadrer et pour parvenir aux modulations et techniques unifiées pour traiter les informations qui circulent s'appuyant sur ce système.

Bibliographie

[1] Weis, S. A. (2007). RFID (Radio Frequency Identification): Principles and Applications.

[2] González, G. Z. (July 2013). Radio Frequency Identification (RFID) Tags and Reader Antennas Based on Conjugate. Bellaterra (Cerdanyola del Vallès),.

[3] MAROUF, F. Z. (2013). Etude et Conception d'Antennes Imprimées pour Identification Radio Fréquence RFID UHF.

[4] KHIRANI, A. (2018). Securing & Tracking Homes In Smart Cities.

[5] Umar Farooq, M. u. (August 2014). RFID Based Security and Access Control System. IACSIT International Journal of Engineering and Technology .

[6] V. S. Hunt, A. P. (2007). A Guide to Radio-Frequency identification. NY.

[7] Aguirre, J. I. (2007, February). EPCglobal: A Universal Standard.

[8] International Organization for Standardization (ISO). (2003). Identification cards -. Contactless integrated circuit(s) cards .ISO/IEC 14443.

[9] Ibid. (2004). RFID for Item Management.ISO/IEC 18000.

[10] Finkenzeller, K. (2003). RFID Handbook 2nd edition. Wiley press.

[11] C.Ramasinghe, P. H. (2008). RFID Handbook Applications,Technology,Security and Privacy. CRC press.

[12] Motlagh, N. H. (2012, May). Near Field Communication A Technical Overview.

[13] Kuriakose, R. (2010). Automatic Student Attendance Registration Using RFID .

[14] Kheddam, R. (2014). Approches logicielles de sureté de fonctionnement pour les sysètmes RFID. Université Grenoble.

[15] Seriot, N. (2005, janvier). Les systèmes d'identification Radio-Fonctionnement,Applications et Dangers. Yverdon-les-bains.

[16] P.Krishna, (2007, semptembre) RFID Infrastructure. IEEE Communication Magazine .

[17]David Hanny, J. B. (2007). RFID Applied. John Wiley and sons . John Wiley and sons.

[18] Federal Office for Security in Information Technology. (2005). Security Aspects and Prospective Applications of RFID Systems. Bonn.

[19] Weis, S. A. (2003). Security and Privacy in Radio-Frequency Identification. Massachusetts, USA: Massachusetts Institute of Technology.

[20] Piramuthu, S. (2007). Protocols for RFID tag/reader authentication. Decision Support .

[21] H. Y. Chien. (2007). SASI: A New Ultra-Lightweight RFID Authentication Protocol Providing. IEEE Transactions on Dependable and Secure Computing .

[22] M. Ohkubo, K. S. (2003). Cryptographic approach to ‘Privacy-friendly. RFID Privacy workshop .

[23] S. Karthikeyan, M. N. (2005). RFID security without extensive cryptography. Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks , 63-67.

[24] Chien, H.-Y. (2009). The Study of RFID Authentication Protocols and Security of Some Popular RFID Tags. Department of Information Management, National Chi Nan University .

[25] P. Peris-Lopez, J. C.-C.-T. (2006). LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID. Proc. of 2nd Workshop on RFID Security .

[26] Weis., A. J. (2005). Authenticating Pervasive Devices with Human Protocols. Adv. in Cryptology .

[27] G. Avoine, E. D. (2006). Reducing time complexity in RFID systems. The 12th Annual Workshop on Selected Areas in Cryptography (SAC) .

[28] LILIA, G. (2017). Commande en position du a MCC par Arduino. Mémoire Master .

[29] Azad., M. A. (2018, December). Rfid Based Door Lock With Automatic Door Open And Close.

[30] Sándor USZKAI, B. P. (2018). Access Control System With Mobile Platform. Hungary.

[31] Amaury (s.d.). zestedesavoir. Récupéré sur https://zestedesavoir.com.