La cryptographie dans le monde de la monétique

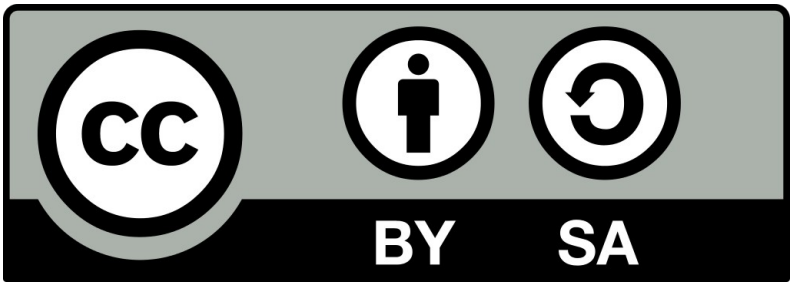
380, avenue Archimède
Parc Cézanne – Bâtiment B
13593 Aix-en-Provence

Ynov Aix-en-Provence
2 rue Le Corbusier
13090 Aix en Provence

Mickaël RIGONNAUX

Master Informatique : Expert Cloud, Sécurité & Infrastructure

2018 - 2020



1 Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au bon déroulement de mes trois années d'alternance et qui m'ont aidé lors de la réaction de ce mémoire de fin d'étude.

Premièrement je tiens à remercier mon tuteur en entreprise M. Grégoire Maux, expert en sécurité des systèmes d'information, pour sa confiance, ses conseils ainsi que le partage de son expertise. J'ai pu grâce à lui découvrir la sécurité informatique et m'accomplir dans ce domaine.

Je veux également remercier M. Eric Battistoni, mon professeur référent en Sécurité des Systèmes d'Information pour son expertise et ses conseils tout au long de la rédaction de ce mémoire.

Je remercie plus généralement toute l'équipe sécurité de la société Monext : Cindy, Quentin, Dylan, Philippe… Sans qui ces trois années n'auraient pas été aussi formatrices.

2 Table des matières

3 Problématique

Aujourd'hui, les méthodes et algorithmes cryptographiques utilisés dans le système monétique sont-ils suffisants ?

4 Introduction

4.1 Choix du sujet

Le présent rapport a pour objet la présentation de mes recherches dans le secteur de la cryptographie appliquée au monde de la monétique. Ces recherches ont été effectuées dans le cadre de mon Master réalisé en alternance au sein de la société Monext et du campus Ynov Aix-en-Provence.

Cette entreprise en pleine croissance a pour cœur de métier la monétique, avec toutes les problématiques qui l'accompagnent, notamment en matière de sécurité informatique.

Nous aborderons dans un premier temps la société Monext, dans en deuxième temps la monétique avec le système cryptographique actuel, dans un troisième les évolutions prévues au niveau de la cryptographie. Pour terminer nous aborderons l'informatique quantique et ses éventuels impacts sur la cryptographie et sur la monétique.

Il y a trois ans, j'ai intégré la cellule sécurité de cette société. Je m'occupe maintenant principalement de la gestion des certificats et des clés cryptographiques de l'entreprise ainsi que de la gestion des outils qui permettent de détecter les intrusions.

4.2 Présentation de la problématique

La problématique de ce mémoire est issue de plusieurs constats qui ont été faits tout au long de mes trois années d'alternance au sein de la société Monext. Notamment avec la mise en place de plusieurs services et l'observation du fonctionnement de la monétique, plus généralement avec les différents grands comptes du système français.

La question s'est donc posée naturellement avec les différentes informations que j'ai pu récolter tout au long de mes travaux et observations : « Aujourd'hui, les méthodes et algorithmes cryptographiques utilisés dans le système monétique sont-ils suffisants ? ». Surtout dans un secteur aussi sensible et fortement exposé à la fraude.

Plus précisément, est-ce que nous utilisons de la meilleure façon les outils à notre disposition pour protéger les données des utilisateurs comme leurs numéros de carte et leurs informations personnelles ? Ces solutions sont-elles pérennes dans le temps ?

Cette problématique est très large et nous permettra d'aborder plusieurs sujets, certains très techniques et d'autres purement organisationnels et humains.

5 Présentation de Monext

5.1 Présentation globale

Monext, société spécialisée dans la monétique est une filiale du groupe Crédit Mutuel Arkéa basée à Aix-en-Provence. Elle comporte environ 500 personnes sur trois sites, deux à Aix-en-Provence et un à Paris. Ses activités principales sont la fourniture de services de paiement en ligne ou physique. Depuis mai 2012 le directeur général de l'entreprise est Frédéric DIVERREZ.

5.2 Activités

Cette société a pour cœur de métier la monétique, c'est-à-dire tout ce qui concerne les paiements par carte bancaire. Ce secteur d'activité est très prometteur, essentiellement grâce aux développements des paiements en ligne. La diversification des moyens de paiement comme le paiement mobile avec ApplePay ou le sans contact a un impact important sur l'utilisation des paiements par carte bancaire.

Voici Monext en quelques chiffres :

- Chiffres d'affaires : 75.5 millions d'euros
- 3 milliards de transactions bancaires traitées
- Plus de 40 % de parts de marché sur les paiements en ligne
- 20 millions de cartes traitées, 4 millions en plus comparés à 2017

Cette entreprise innovante se positionne comme un des leaders sur le marché français avec 40 % de parts de marché en France. Les deux solutions phares de l'entreprise sont Payline et Payavenue. Ces logiciels interviennent au niveau de l'acceptation, c'est-à-dire au niveau du vendeur, que ça soit en ligne pour Payline ou physiquement pour Payavenue. De nombreux grands comptes utilisent les outils fournis par Monext comme PMU, la Banque de France, Amazon ou E. Leclerc.

La société travaille également avec des banques afin de leur fournir d'autres services comme des autorisations par exemple ou de l'émission de carte bancaire.

6 Partie 1 : Introduction à la monétique & à la cryptographie

6.1 La monétique

Avant tout, il est très important de définir la notion de monétique, qui s'avère être très complexe. La définition selon Wikipédia : « La monétique désigne l'ensemble des traitements électroniques, informatiques et télématiques nécessaires à la gestion de cartes bancaires ainsi que des transactions associées. ».

Pour simplifier cette notion, nous pouvons dire qu'il s'agit de tous les moyens liés à l'utilisation d'une carte bancaire. Nous utilisons donc presque tous les jours la monétique, avec le paiement sans contact, le paiement sur smartphone ou le paiement sur internet.

Il faut cependant ne pas confondre la monétique qui désigne les paiements électroniques avec le système monétaire, qui désigne les flux d'argent. Les virements SEPA ou les chèques par exemple ne font pas partie de la monétique.

La monétique est donc un métier ancien. Il a vu le jour avec l'invention de la « carte bleue » en 1967 et a fortement évolué en 1974 avec l'invention de la carte à puce. Depuis les paiements par cartes bancaires n'ont pas cessé d'augmenter jusqu'à dépasser le paiement par chèque en 2001. La même année le paiement par internet devient possible avec l'e-carte bleue. Depuis cette date les paiements en ligne ont bien sûr augmenté tout comme les paiements classiques, mais le métier en lui-même n'a pas grandement évolué. Dans l'ensemble des explications ci-dessous nous allons nous concentrer sur la monétique dans le marché français.

Les chiffres de 2018 pour les paiements par CB par le GIB CB[1] :

- Nombre de cartes CB : 70.4 millions
- Nombre de DAB : 54 milles
- Nombre de paiements : 12.7 millions
- Nombre de retraits : 1.3 millions

1 Groupement des cartes bancaires CB

Nous trouvons également un graphique du même groupe pour illustrer la forte hausse de l'utilisation des cartes bancaires :

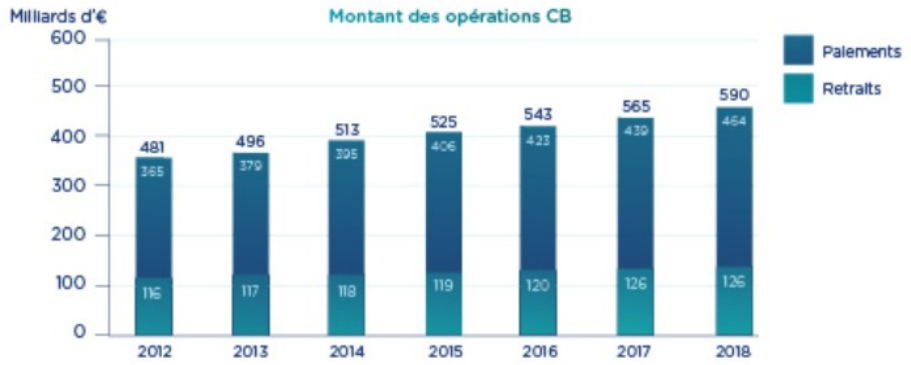


Figure 1. Source : cartes-bancaires.com. Evolution du montant des opérations CB en France entre 2012 et 2018

D'autres schémas sont disponibles en annexe I.

Il est aussi à noter que le milieu bancaire est très touché par la fraude. En 2018, les paiements par carte bancaire concernent 92.4% des transactions frauduleuses soit un peu moins de 440 millions d'euros, même si au niveau des montants la fraude par chèque est plus importante.

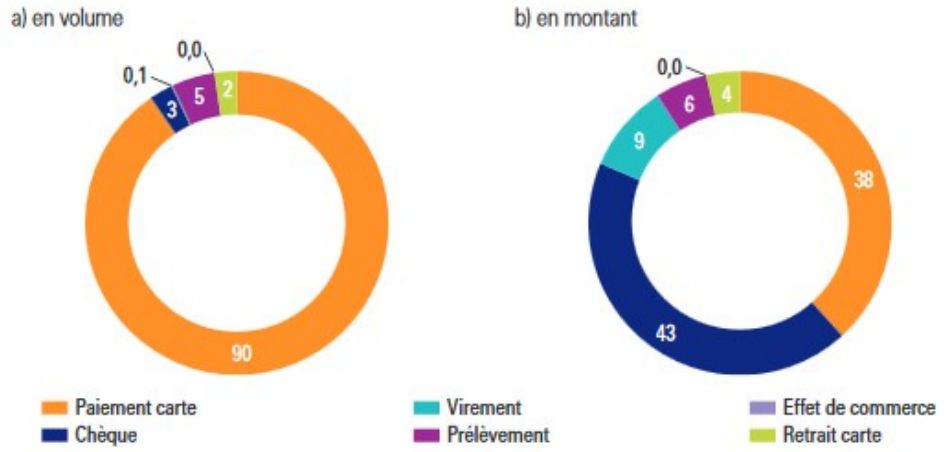


Figure 2. Source : banque-france.fr. Volume en % du nombre et des montants des transactions frauduleuses

6.1.1 Les schemes ou réseaux

Nous avons donc exposé ici les chiffres de 2018 du GIE CB qui est ce qu'on appelle un « scheme », c'est un réseau monétique. Un « scheme » est un réseau de paiement lié directement à des cartes et les banques peuvent en devenir

membre pour profiter de ce réseau. Elles peuvent donc émettre des cartes fonctionnant sur le réseau.

Les principaux réseaux dans ce milieu sont VISA, Mastercard ou encore American Express. La particularité de la France est le réseau GIE CB, ce dernier a été créé pour assurer l'interbancarité, afin que chaque personne puisse payer sans avoir un problème avec le réseau utilisé par le terminal de paiement. C'est pour cette raison que nous avons presque tous sur nos cartes deux logos, CB et VISA/Mastercard. Cela permet d'utiliser le réseau CB en et VISA ou Mastercard à l'étranger.

Le réseau CB va donc utiliser son réseau pour renvoyer les paiements vers les réseaux respectifs, tout ça sans intervention et sans problème pour l'utilisateur. De plus, ce réseau permet aux étrangers qui ne possèdent pas de carte issue du GIE CB de payer et également de router les transactions qui ne sont pas faites avec des cartes CB.

Les réseaux se matérialisent comme des réseaux classiques, c'est-à-dire par des liaisons en cuivre ou en fibre optique. Les réseaux les plus importants comme VISA et Mastercard utilisent leurs propres réseaux privés qui interconnectent les différents pays et les différentes banques directement, ils essaient d'éviter au maximum l'utilisation des réseaux publiques comme Internet.

Les points d'entrées sont eux généralement connectés à internet et les flux sont redirigés vers les différents réseaux.

6.1.2 Le modèle en quatre coins

Voici comment fonctionne la monétique avec son célèbre schéma en 4 coins :

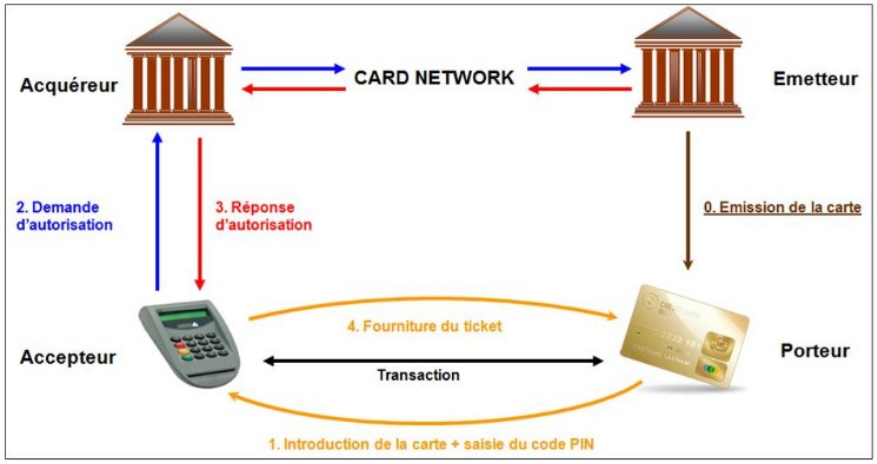


Figure 3. Source : capfi.fr. Schéma du modèle monétique à 4 coins

Un schéma avec trois coins existe également lorsque l'émetteur et l'acquéreur sont la même banque, il est disponible en annexe II.

Sur ce schéma simplifié, nous pouvons distinguer quatre parties : l'acquéreur, l'accepteur, le porteur et l'émetteur. Il est aussi possible de voir les réseaux de cartes ou les demandes d'autorisations.

Tout d'abord, l'émetteur qui est la banque du porteur. C'est à lui de délivrer une carte bancaire à son client, c'est ce qu'on appelle une émission de carte. Il peut s'agir par exemple de banque comme la BNP Paribas, le LCL ou encore des jeunes startups comme « Max » du Crédit Mutuel.

Ensuite le porteur. Aujourd'hui la majorité des individus possède une carte bancaire, toutes ces personnes sont des porteurs dans le monde de la monétique.

L'accepteur est de son côté, le commerçant ou la société qui va recevoir le paiement que ça soit en ligne ou physiquement, par exemple les magasins U, Auchan ou Amazon en version en ligne. Cette phase, est appelée acceptation. Nous remarquerons que les deux solutions de Monext Payline et Payavenue se positionnent ici.

La banque du commerçant ou de la société, qui reçoit le paiement est l'acquéreur ou banque acquéreuse. À ce titre, les paiements effectués par les porteurs arrivent chez l'acquéreur, on appelle cela l'acquisition.

En plus de ces quatre coins, nous pouvons observer sur ce schéma une demande d'autorisation. Ce système permet de vérifier auprès de la banque du porteur si la transaction est autorisée ou non.

Plus concrètement, lors d'un paiement chez un accepteur, le porteur va insérer sa carte et entrer son code pour payer. À ce moment-là, si le montant est supérieur à la limite fixée par l'accepteur, une demande d'autorisation va être envoyée à la banque acquéreuse. Cette dernière va renvoyer cette demande à l'émetteur qui donnera son accord ou non. Plusieurs vérifications seront alors faites pour accepter la transaction. Ce processus intervient au moment où le TPE[2] affiche « Autorisation en cours… » lorsqu'un paiement est effectué. Mais cette opération n'est pas automatique, elle n'est pas utilisée pour les petits montants par exemple ou pour les paiements sans contact.

2 Terminal de paiement électronique, aussi appelé point d'acceptation ou moyen d'acceptation

Et pour finir, nous pouvons aussi remarquer la présence des réseaux bancaires ou « schemes » déjà évoqué plus haut.

Ces fondements sont la base du système monétique, même si nous allons continuer à expliquer d'autres parties de ce secteur très vaste comme la télécollecte par exemple ou encore PCI DSS.

6.1.3 La télé-collecte et la compensation

La télé-collecte permet aux systèmes d'acceptations d'envoyer les transactions enregistrées à un système acquéreur. C'est-à-dire que toutes les transactions sont enregistrées par le TPE en attendant d'être envoyée à la banque acquéreuse en fin de journée généralement. Ce système se nomme la télé-collecte.

Lorsqu'une transaction est faite, elle n'est pas envoyée directement à l'acquéreur. Ce dernier n'a pas connaissance en temps réel des paiements effectués, sauf pour les autorisations mais l'information seule ne suffit pas. La transaction est stockée sur la mémoire du moyen d'acceptation.

Ce système intervient pour ne pas surcharger les serveurs monétiques lors d'une grosse journée par exemple, prévoir une heure fixe pour l'envoi de toutes les transactions permet également de mieux appréhender les flux et de les optimiser.

Ce mécanisme de télé-collecte est directement lié à un autre qui se nomme la compensation. La compensation n'est pas seulement valable pour les paiements classiques, le principe est le même pour les virements, les prélèvements et les retraits dans un distributeur.

Lors de la télé-collecte, les différents acquéreurs vont regrouper l'ensemble des actions réalisées par banque émettrice et vont faire les comptes. Par exemple, la BNP Paribas en fin de journée va faire ses comptes et va voir que des paiements des banques LCL et Crédit Agricole ont été réalisés dans des commerces de leurs clients.

La BNP Paribas va donc faire la somme des transactions que les autres banques lui doivent et demander un règlement. Dans le même temps, la BNPP va aussi recevoir des demandes de règlements des autres banques acquéreuses, car des paiements ont aussi été effectués par des clients porteurs. Une différence sera alors faite entre ce qu'une banque doit à la BNP Paribas et ce que la BNP Paribas

doit. Si le résultat est négatif pour une banque, elle devra verser de l'argent à la banque acquéreuse.

Ce système est valable pour l'ensemble des banques. Une fois la compensation réalisée, l'argent est redistribué par les banques acquéreuses sur les différents comptes bancaires.

6.1.4 La carte bancaire et la personnalisation

La carte bancaire est le cœur même de la monétique, nous allons donc aborder rapidement comment elles sont créées et les informations qu'elles contiennent.

Tout d'abord il faut savoir que les cartes sont soumises à un standard de sécurité appelé EMV[3]. Ce standard international est utilisé pour garantir la sécurité des cartes à puce. Il est utilisé en France depuis 2006, l'ensemble des cartes et des équipements utilisés aujourd'hui sont donc conformes à cette norme. En dehors de l'aspect sécuritaire l'utilisation d'EMV permet une interopérabilité entre les cartes à puce et les terminaux de paiement dans les pays partenaires.

Les cartes créées pour les porteurs sont donc soumises à EMV. Voyons maintenant les informations présentes sur et dans la carte bancaire. Sur les parties visibles, les informations classiques :

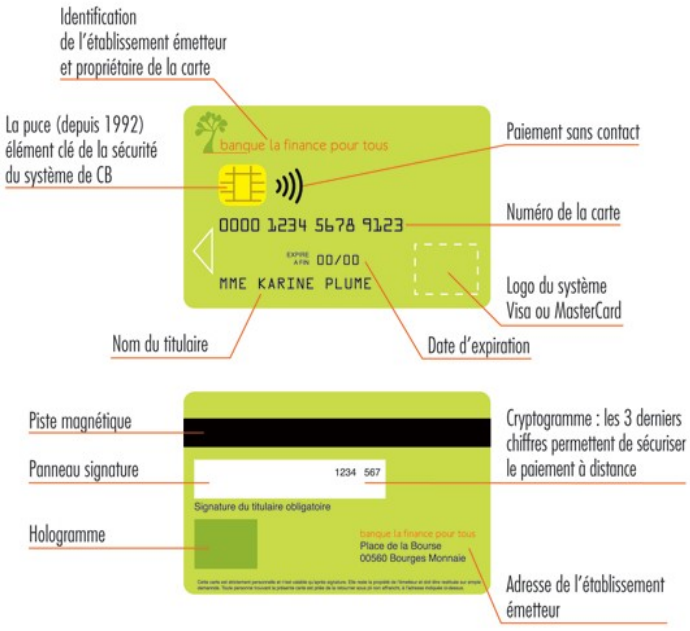


Figure 4. Source : inc-conso.fr. Schéma des éléments présents sur une CB

3 EMV : Europay, Mastercard et VISA forment EMVCo.

En plus de ce qui est visible sur l'illustration, le logo du GIE CB est à rajouter si le réseau CB est utilisé par la carte. Nous voyons donc sur ce schéma les différentes parties visibles sur une CB. Les plus importantes sont le PAN[4] qui est ici appelé numéro de carte ainsi que le cryptogramme. Ces deux informations sont créées lors d'un processus appelé personnalisation de carte, ce procédé fait partie intégrante de l'émission.

La personnalisation n'est pas là seulement pour générer ces deux composants. Elle permet aussi à une banque de mettre son logo ainsi que ses informations sur ses cartes. Mais l'aspect principal est la saisie des informations sur la puce ainsi que la piste magnétique de la carte. En plus des informations visibles, la puce et la piste de votre carte contiennent des informations comme votre adresse, nom & prénom, le PIN de la carte, le numéro de carte, la date d'expiration, le nombre de transaction réalisé ainsi que le dernier paiement réalisé en ligne.

D'autres composants sont présents comme un microprocesseur pour effectuer des calculs, des espaces mémoires pour stocker des clés de chiffrement ainsi que les informations listées. En plus, un capteur NFC peut être présent pour autoriser les paiements sans contact.

Volontairement oublié dans cette partie pour des raisons de compréhension, l'ensemble des actions et de générations des données sensibles lors de la personnalisation de la carte sont réalisées avec des moyens cryptographiques afin d'assurer la sécurité des éléments les plus importants. Comme le code PIN par exemple et les clés de chiffrement symétrique. Ces actions sont effectuées par un matériel spécifique appelé HSM[5]. Il permet de générer les codes PIN, les cryptogrammes ainsi que les clés secrètes déposée sur chaque carte.

Les HSM sont aussi utilisés dans d'autres cas comme les autorisations ou encore les retraits, dans les deux cas pour la vérification du PIN entré par le porteur. Des exemples d'utilisation des HSM sont présents en annexe III.

6.1.5 Les terminaux de paiement

Après la carte bancaire, nous pouvons maintenant parler du TPE ou Terminal de Paiement Electronique qui est le boitier utilisé pour les paiements physiques chez les commerçants. C'est le point d'acceptation, il est directement relié et distribué par les banques acquéreuses.

4 PAN : Primary Account Number
5 HSM : Hardware Security Module

Le TPE est la première entrée des différents flux monétiques générés et est directement connecté aux différents réseaux. Ils sont utilisés à travers toute la planète pour les paiements de proximités.

Mais ils ne servent pas que pour ce type de paiement. Ils permettent aussi de faire des ventes à distance, de payer en plusieurs fois et d'effectuer des préautorisations comme dans un hôtel par exemple.

Les différents services proposés par un TPE sont appelés des applications. Ils peuvent en contenir plusieurs comme l'application EMV pour l'acceptation des réseaux Mastercard, Visa et CB. Il y a aussi des applications pour des réseaux plus particuliers comme JCB ainsi que d'autres options comme les conversions de devises. Chaque fonctionnalité est associée à une application que l'accepteur choisit d'intégrer dans ses services.

Pour mieux situer les différentes parties présentées ci-dessus, un schéma plus détaillé de la monétique est disponible en annexe IV.

6.1.6 PCI DSS

Nous allons maintenant aborder le standard PCI DSS[6] qui est une norme de sécurité créée par les principaux groupes bancaires Visa, Mastercard, American Express, Discover Card et JCB. Cette norme créée par le PCI Security Standards Council a été mise en œuvre pour assurer un niveau de sécurité élevé pour la manipulation des données bancaires afin de protéger les porteurs et de réduire la fraude.

La première version a été publiée en 2004, actuellement la dernière version est la 3.2 sortie en 2016.

6 Le standard PCI DSS : Payment Card Industry Data Security Standard

Le PCI DSS est formé de six groupes appelés des objectifs de contrôles, divisés en douze conditions. Ces conditions sont-elles mêmes découpées en exigence comme réaliser des tests d'intrusion par exemple ou encore la gestion des mots de passe.

Objectif de contrôle	Conditions du PCI DSS
Création et gestion d'un réseau et d'un système sécurisé	1. Installer et gérer une configuration de pare-feu pour protéger les données du titulaire de carte
	2. Ne pas utiliser les mots de passe et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données du titulaire	3. Protéger les données stockées du titulaire
	4. Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts
Maintenir un programme de gestion des vulnérabilités	5. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes
	6. Développer et gérer des systèmes et des applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	7. Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître
	8. Identifier et authentifier l'accès aux composants du système
	9. Restreindre l'accès physique aux données du titulaire
Surveillance et test réguliers des réseaux	10. Suivre et surveiller tous les accès aux ressources réseau et aux données du titulaire
	11. Tester régulièrement les processus et les systèmes de sécurité
Maintenir une politique de sécurité des informations	12. Maintenir une politique qui adresse des informations de sécurité pour l'ensemble du personnel

Figure 5. Source : wikipedia.org. Organisation de PCI DSS

Plus largement, la norme PCI DSS est scindée en trois tiers, un premier purement organisationnel, un deuxième basé sur la documentation et un dernier sur la partie technique.

Cette norme n'est pas obligatoire même si elle devrait s'appliquer à toutes les entreprises gérant des données bancaires. Cependant, Visa et Mastercard obligent les commerçants et les prestataires à s'y conformer.

Même si pour les autres catégories ils n'imposent rien, ils se doivent d'avoir un niveau de sécurité à la hauteur des données traitées. L'émetteur par exemple est obligatoirement soumis à PCI DSS alors que l'acquéreur non. Sur la partie certification, le PCI Council utilise des prestataires agréés pour délivrer la certification PCI DSS. Ils sont appelés Auditeurs de Sécurité Qualifié ou QSA.

6.1.7 EMV

EMV[7] est un standard international chargé d'assurer la sécurité des cartes de paiement à puce. Son nom vient des groupes qui l'ont formé soit Europay, Mastercard & Visa. Il est aujourd'hui le plus répandu à travers la planète. Il est utilisé en France à travers les normes de CB, qui utilise essentiellement des cartes dites EMV. Plus largement en Europe les cartes concernent 98 % des paiements sur l'année 2019 avec à peu près 1 milliard de carte, soit plus de 80 % du volume. Plusieurs schémas sont disponibles en annexe V. Cela permet en plus de l'aspect sécuritaire, de former un système homogène ainsi que d'assurer une interopérabilité entre les cartes et les terminaux de paiement.

EMV traite l'ensemble des sujets relatifs aux paiements par carte à puce, que ça soit des paiements physiques comme abordé dans ce rapport mais également d'autres systèmes comme les paiements sans contact.

La dernière version de la norme qui concernant l'utilisation des cartes à puce est la 4.3, présentée officiellement en novembre 2011, très peu d'évolution ont été présentée depuis. Cette norme englobe les cartes et les traitements qui en sont faits au niveau de l'acceptation, c'est-à-dire le TPE.

Nous pouvons maintenant aborder la présentation de la cryptographie.

6.2 Présentation de la cryptographie

La définition de la cryptographie selon le Larousse :

« Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. »

En plus de cette définition je rajouterais que ses trois grands principes sont la confidentialité, l'authenticité et l'intégrité. Les différentes techniques cryptographiques servent ces trois fondements.

En d'autres termes, ça permet de rendre un message illisible pour les personnes qui n'ont pas autorité pour le lire. Pour le rendre illisible ou chiffré, plusieurs méthodes sont possibles. L'une des premières et des plus simples, consiste à modifier les données afin de les rendre incompréhensibles. Une seconde sera basée sur un système de clé, c'est cette clé qui nous permettra de protéger nos données et de les rendre illisibles.

7 EMV : Europay, Visa, Mastercard

La cryptographie, issu elle-même de la cryptologie permet de protéger des messages depuis la nuit des temps. De son côté la cryptologie est une science, appelé la science du secret qui contient la cryptographie et la cryptanalyse qui est tout simplement l'analyse de la cryptographie.

Une notion importante en cryptographie est le cycle de vie des algorithmes et de la taille des clés. Il est important de garder toujours une marge, c'est pourquoi nous arrêtons d'utiliser quotidiennement des algorithmes et des tailles de clés qui sont toujours surs, mais qui sont susceptibles de ne plus l'être d'ici peu. Les algorithmes et les tailles de clés sont donc choisies pour être durable dans le temps et non seulement assuré la sécurité à l'instant T. La notion du mot « aujourd'hui » en cryptographie à une durée beaucoup plus étendue que dans les autres domaines.

Voici un schéma avec les principales évolutions dans le monde de la cryptographie :

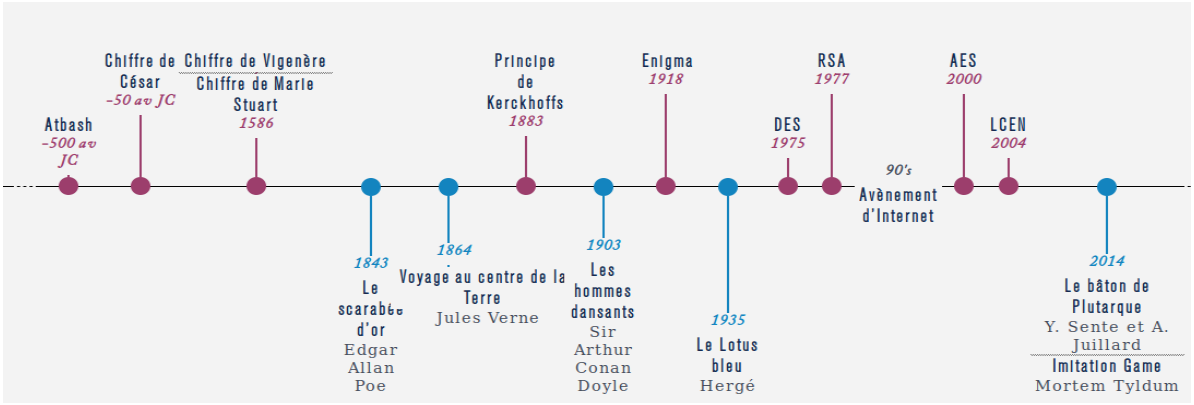


Figure 6. Source : ssi.gouv.fr. Evolution de la cryptographie à travers le temps

La cryptographie est utilisée depuis l'Antiquité pour échanger des messages sans qu'il puisse être lu par d'autres personnes que ceux connaissant la clé pour déchiffrer le message. On a donc toujours des notions de message chiffré, déchiffré et de clé.

L'une des premières utilisations de la cryptographie et également une des plus célèbres est celle du chiffre de César, utilisé par l'armée romaine pour échanger des messages chiffrés. Cette méthode très simple mais très efficace pour l'époque est fondée sur un simple décalage de lettres.

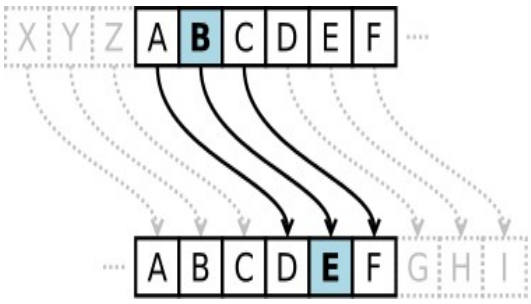


Figure 7. Source : wikipedia.org. Schéma du chiffrement par décalage

Tout au long de notre histoire la cryptographie a joué un rôle primordial. Les premiers textes chiffrés datent de l'Antiquité. Une recette de cuisine inscrite sur une tablette d'argile ou les consonnes ont été supprimées et l'orthographe des mots modifiés. Plus récemment et principalement dans le domaine militaire, la cryptographie et la cryptanalyse ont joué des rôles importants durant les grandes guerres de 14-18 et de 39-45.

Arriver à déchiffrer les messages de l'ennemi donnait un avantage certain. Notamment avec l'invention de la machine Enigma par les Allemands durant la deuxième guerre mondiale pour échanger des informations chiffrées, et par la même occasion, l'invention des « bombes », des machines électromagnétiques utilisées par les cryptologues britanniques afin de casser le code Enigma. Ces machines tout d'abord développée par les Polonais ont été grandement améliorées grâce au travail d'Alan Turing[8] et Gordon Welchman. Nous devons également à Alan Turing les fondements de l'informatique actuel, avec la machine de Turing.

Aujourd'hui, la cryptographie que nous utilisons est basée principalement sur des mathématiques. Sur des problèmes parfois très simples que les ordinateurs actuels ne peuvent pas résoudre comme la factorisation de deux nombres premiers.

Le chiffrement des données occupe donc aujourd'hui une grande part dans notre vie. Cet aspect s'est accentué fortement avec l'arrivée du tout numérique et des internets avec des besoins en sécurité très important. Paiement en ligne, consultation de notre compte en banque, messagerie instantanée, mail ou tout simplement la navigation. Toutes ces applications fonctionnent grâce à des méthodes de chiffrement afin de garantir la confidentialité et l'intégrité des

8 Célèbre mathématicien et cryptographe britanniques

données que nous échangeons. La cryptographie est donc un élément clé de la vie privée de chaque citoyen et de la société plus généralement.

Il y a notamment une prise de conscience générale sur ce sujet depuis la révélation d'Edward Snowden sur l'espionnage de masse des autorités américaines en 2016.

Nous allons maintenant aborder synthétiquement les trois systèmes les plus utilisés dans les systèmes actuels : la cryptographie symétrique, asymétrique et les fonctions de hachage.

Les principaux algorithmes et systèmes qui nous intéressent seront analysés plus en détail dans la suite du document.

6.2.1.1 Symétrique

Le chiffrement symétrique est la plus ancienne méthode de chiffrement utilisée. On peut la retrouver sous le nom de méthode à clé secrète. Ce nom vient du fait que l'ensemble du système est basé sur une clé partagée entre les différents acteurs de l'échange. Nous pouvons donc chiffrer et déchiffrer le message/fichier avec la même clé, là elle est la base des différents algorithmes.

Le principe est qu'une clé donnée, traitée par un algorithme permet de chiffrer et déchiffrer nos messages.

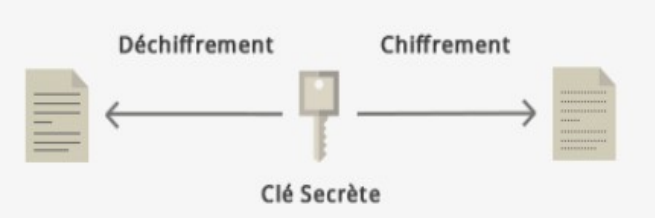


Figure 8. Source : cnil.fr. Schéma du chiffrement symétrique

Voici quelques-uns des principaux algorithmes de chiffrement symétrique :

- AES : Advanced Encryption Standard, lancé en 1997 par le NIST[9]. Il est aujourd'hui approuvé par les plus grosses entités comme la NSA, il est également le plus sûr et le plus utilisé.
- DES : Data Encryption Standard, publié en 1977 par « Federal Information Processing Standards » est un algorithme basé sur des clés de 56 bits.

9 NIST : National Institute of Standards and Technology

Aujourd'hui l'utilisation de cet outil est proscrite, il est plus couramment utilisé à travers 3DES.

- 3DES : Triple DES, créé en 1999 est simplement la répétition de l'algorithme DES trois fois avec deux ou trois clés différentes.
- Blowfish conçu par Bruce Schneier[10] en 1993, il est basé sur un principe utilisant de très grandes clés pseudo-aléatoires.

Dans les protocoles symétriques proposés deux grandes catégories sont utilisés, le chiffrement par bloc et le chiffrement par flux.

Le premier, comme son nom l'indique, doit découper les données en des blocs de tailles fixes pour permettre le chiffrement et le déchiffrement des données.

Le second, n'a pas besoin de découper le trafic et arrive à traiter les données de toutes les longueurs sans traitement supplémentaire.

La catégorie la plus répandue est celle du traitement par bloc, tous les algorithmes présentés ci-dessus sont utilisent le chiffrement par bloc.

En plus de ces aspects, il existe ce qu'on appelle le mode d'opération ou le mode de l'algorithme pour le chiffrement par bloc. Cela correspond à la manière dont sont traités les blocs dans l'algorithme. Il existe plusieurs modes comme ECB ou CBC, d'autres moins connus permettent de transformer un chiffrement par bloc en chiffrement par flux comme CFB ou CTR.

L'utilisation des protocoles symétriques est aujourd'hui démocratisée, nous en utilisons tous les jours sans nous en rendre compte avec GPG[11] ou SSL/TLS[12] par exemple. Ils ont l'avantage d'être très rapide et performant avec des clés relativement courtes, mais ils ont également des gros défauts au niveau de la transmission de ladite clé et de l'authentification des parties.

Comment pouvons-nous transmettre la clé à la personne avec qui nous échangeons de manière sécurisée ? Et comment être sûr que la clé est transmise à la bonne personne ?

10 Bruce Schneier est un célèbre cryptologue américain
11 GPG : GNU Privacy Guard
12 SSL/TLS : Secure Sockets Layer/Transport Layer Security

6.2.1.2 Asymétrique

Le chiffrement asymétrique, aussi appelé chiffrement à clé publique, est basé non pas sur l'utilisation d'une seule clé, mais sur des paires de clés, des clés privées et des clés publiques. Ce système permet lors d'un échange de ne pas partager la même clé.

Cette méthode créée en 1976 par Whitfield Diffie et Martin Hellman est révolutionnaire, elle est le cœur de la cryptographie que l'on connaît aujourd'hui. Même si ce principe a été publié en 1976, un exemple de système asymétrique a été donné seulement deux ans plus tard par les inventeurs du protocole RSA, Ronald Rivest, Adi Shamir et Leonard Adleman.

Ce système veut donc que pour des échanges chaque partie doit avoir deux clés. Une clé publique qui pourra être partagée sans problème et servira pour le chiffrement et une clé privée qui elle, ne doit être partagée sous aucun prétexte et servira à déchiffrer. Il ne doit pas être possible également de retrouver la clé privée avec la clé publique, mais l'inverse doit être possible.

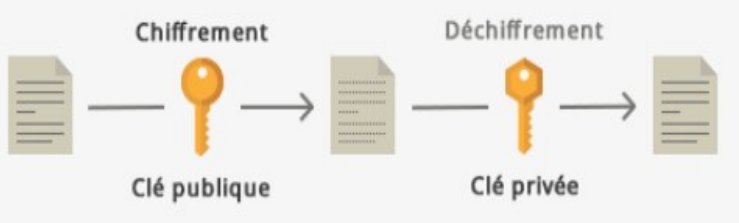


Figure 9. Source : cnil.fr. Schéma du chiffrement asymétrique

Voici les algorithmes les plus connus pour le chiffrement asymétrique :

- RSA issu des noms des trois inventeurs Rivest, Shamir et Adleman, il est aujourd'hui le protocole le plus utilisé dans les systèmes asymétriques.
- Diffie Hellman du nom des deux créateurs est la première version d'un système asymétrique créé en 1976. Ce dernier permet d'échanger des clés et est toujours utilisé aujourd'hui avec plusieurs variantes.
- ECC : Elliptic Curve Cryptography, est un ensemble de systèmes basés sur des courbes elliptiques. ECC utilisent des algorithmes comme ECDSA, ECDH, etc.

Les systèmes cryptographiques asymétriques sont aujourd'hui largement répandus, couplés avec des algorithmes symétriques et des fonctions de

hachage. Ils forment des systèmes très complets comme SSL/TLS par exemple. Ils sont la base des infrastructures de clés publiques ou PKI.

Avec l'aide des algorithmes de hachages il est possible, en plus du chiffrement asymétrique, de réaliser ce qu'on appelle des signatures.

6.2.1.3 Hachage (Hash)

Les fonctions de hachage sont très différentes des deux systèmes vus plus haut, tout simplement car une fonction de hachage est irréversible ou à sens unique. Elles sont conçues pour qu'avec la sortie de la fonction il ne soit pas possible de retrouver son entrée.

Les sorties de ces fonctions ont des tailles fixes, 160 bits pour SHA1 par exemple et 256 bits pour SHA256 et elles sont appelées hash ou empreinte. Le nom « empreinte » vient du fait que la sortie est censée être unique pour chaque entrée. C'est-à-dire que deux entrées différentes ne peuvent pas avoir le même hash en sortie. C'est une des conditions pour que l'algorithme soit considéré comme cryptographiquement sûr.

Même si tous les algorithmes ont des limites, par exemple avec SHA256, si on réalise des hashs avec l'algorithme SHA256 pour 2^{256+1} fichier, il y aura forcément deux entrées avec la même sortie, vu que la limite est de 256 bits.

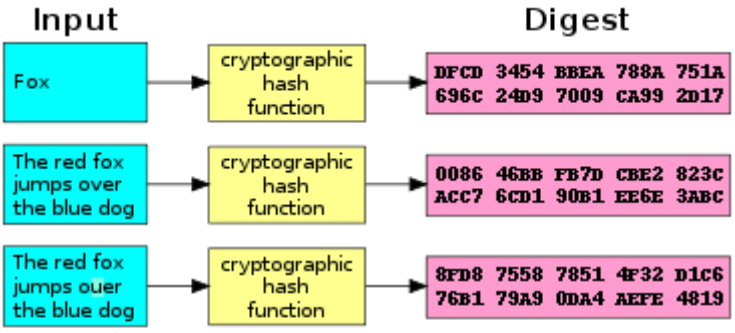


Figure 10. Source : wikipedia.org. Illustration de la méthode de hachage SHA-1

Voici quelques-uns des principaux algorithmes de hachage :

- MD5 : Message Digest 5, inventé par Ronald Rivers (un des créateurs d'RSA), qui était un algorithme très utilisé et qui est aujourd'hui obsolète mais encore présent dans certains cas. Il est le successeur de MD4.
- SHA-1 : Secure Hash Algorithm, lui a été créé par la NSA et est devenu un standard du NIST. Il était l'algorithme le plus utilisé pour les signatures et

est aujourd'hui obsolète, il reste cependant encore utilisé. Il fait partie de la famille SHA qui contient SHA-0 & SHA-1.

- SHA-256 issu de la famille SHA-2 est aujourd'hui l'algorithme le plus utilisé et recommandé, il est directement issu des algorithmes SHA0 et SHA-1. Dans la même famille il existe des algorithmes comme SHA-512.

Ces algorithmes sont utilisés dans le système asymétrique afin d'assurer l'authentification, l'intégrité et la non-répudiation des données échangées. Pour ce faire, une signature va être réalisée.

Plus concrètement pour signer un envoi il faut réaliser un hash des données à envoyer, et chiffrer avec la clé privée de l'envoyeur. C'est comme ça qu'une signature est construite. Le receveur pourra donc vérifier que le message vient bien de la bonne personne, car il est en possession de sa clé publique et il peut également comparer l'empreinte reçue à celle du fichier qu'il vient de recevoir.

Il y a donc deux actions différentes : le chiffrement qui se fait avec la clé publique du partenaire, et la signature qui se fait avec la clé privée de l'émetteur et l'empreinte du fichier ou des données à envoyer.

Voici un schéma d'un envoi de fichier chiffré avec signature :

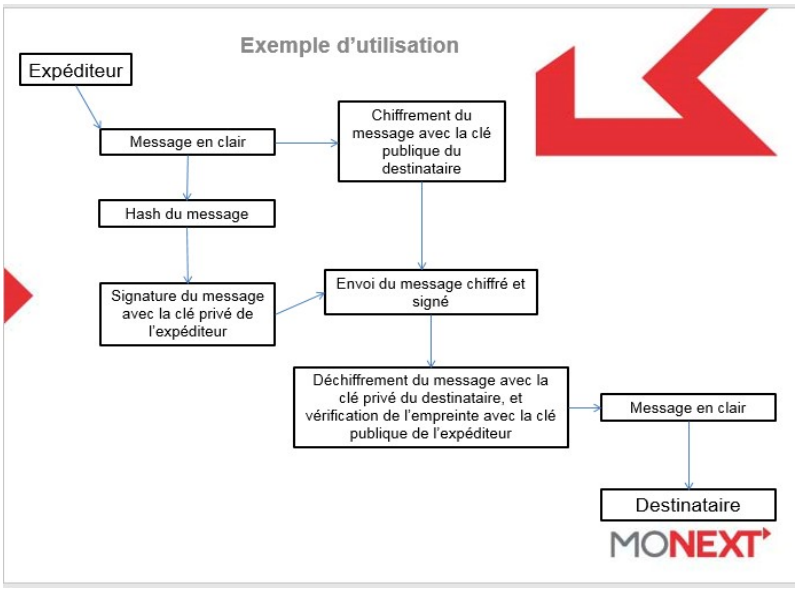


Figure 11. Source : intranet Monext. Illustration d'un envoi de message chiffré & signé

Les fonctions de hachage sont aujourd'hui indispensables dans un grand nombre de système comme SSL/TLS ou encore GPG/PGP.

6.2.1.4 SSL/TLS

Pour aborder rapidement SSL/TLS, c'est un protocole qui englobe un groupe d'algorithmes et de type de cryptographie. C'est ce processus qui est utilisé notamment pour assurer la sécurité des échanges Web avec HTTPS et également utilisé dans d'autres cas comme avec LDAPS ou encore FTPS.

L'ensemble du système est basé sur des certificats de norme X509. Ces certificats sont créés à partir de clé RSA dans la plupart des cas et sont signés par des tiers de confiance afin de prouver leurs provenances et leurs identités. Les tiers de confiance sont des autorités publiques comme GlobalSign ou Let's Encrypt. Ces derniers sont capables de vérifier des informations comme votre nom de domaine ou votre entreprise et de délivrer des certificats en fonction en ajoutant une signature issue de leurs propres certificats.

Un certificat est obligatoirement rattaché à une clé privée vu qu'il s'agit de cryptographie asymétrique. Il correspond à la « carte d'identité » d'une machine. Il comporte donc une date de validité, un ou plusieurs noms de domaine, une autorité racine appelée « issuer » et d'autres informations comme des extensions.

Le certificat est le cœur du protocole SSL/TLS. Il est à installer sur le serveur afin d'assurer les échanges.

Afin d'assurer ces mêmes échanges, le client voulant se connecter ainsi que le serveur recevant la connexion doivent avoir des listes avec les différents protocoles disponibles (SSLv3 à TLS1.3) ainsi que des algorithmes, appelé dans ce cas « cipher suites ».

C'est à travers tous ces éléments que la connexion pourra être établie, il faut que le client et le serveur se mettent d'accord sur la version à utiliser ainsi que la suite d'algorithmes. Dans ces algorithmes il y a des algorithmes, symétriques, asymétriques et de hachage comme abordé plus haut.

Nous pouvons donc aborder la partie principale de ce pré-mémoire, la cryptographie appliquée à la monétique et son fonctionnement plus technique.

7 Partie 2 : La monétique aujourd'hui

Comme nous avons pu le voir avec les deux premiers chapitres de ce document, la monétique est un secteur d'activité très compliqué avec beaucoup d'aspects différents, le constat est le même pour la cryptographie. De plus, certaines parties ont été ignorées volontairement dans ces deux mondes afin de simplifier les explications et ne pas surcharger le document.

L'ensemble des flux générés par les différents acteurs de la monétique dépendent entièrement de la cryptographie. Car les données échangées sont extrêmement sensibles et doivent donc transiter chiffrées, il est aussi très important que l'intégrité et l'authentification des pairs soient assurées. Sans la cryptographie actuelle, la monétique n'aurait pas pu exister.

Les flux transitent principalement par le réseau IP et le réseau X25. Le réseau X25 est utilisé par les concentrateurs de TPE car dans certains cas les TPE sont reliés à des concentrateurs pour ne pas surcharger les flux et identifier les points d'entrées. Les TPE peuvent aussi utiliser le réseau IP, c'est ce qui est fait principalement aujourd'hui, car le réseau X25 est obsolète même s'il reste très présent dans l'acceptation monétique entre les concentrateurs aussi appelés passerelles monétique et les fronts offices bancaires. Les canaux utilisés sont les mêmes que ça soit pour une autorisation ou dans l'acceptation. Pour les exemples de cas, nous aborderons principalement l'aspect physique.

7.1 Exemples de cas

7.1.1 Les cartes bancaires

Les cartes bancaires sont elles-mêmes basées sur la cryptographie. Elles intègrent d'ailleurs un microprocesseur afin de réaliser des calculs pour le chiffrement symétrique voire asymétrique dans certains cas.

La carte, lors de la personnalisation, reçoit toutes les informations nécessaires à son fonctionnement. Plusieurs données sont entrées dans plusieurs emplacements mémoire de la carte :

- Mémoire accessible en lecture seule (en clair) : les différentes clés publiques RSA selon les cas, le PAN, la date d'expiration, le nom & prénom du porteur, date d'expiration, signature des données

- Mémoire accessible avec le code pin en lecture et écriture : compteur de transaction, compteur de transaction en ligne, compteur d'erreur de saisie du code PIN
- Mémoire secrète, accessible seulement par la puce : stockage des clés privées, stockage de la clé secrète fournies par le HSM dérivée par une clé maître du personnalisateur/émetteur, PIN chiffré avec la clé secrète

En effet, la présence des clés asymétriques est différente selon les cas. En voici trois :

- Static Data Authentication (SDA) ou authentification statique des données.
- Dynamic Data Authentication (DDA) ou authentification dynamique des données.
- Combined Data Authentication (CDA) ou authentification combinée de données.

7.1.1.1 SDA

Le SDA est la première méthode historique d'EMV de vérification des données. Même si elle est dépréciée, elle est toujours utilisée aujourd'hui, car la méthode ne dépend pas seulement de la carte mais aussi de l'équipement d'acceptation.

Son fonctionnement est le suivant, lors de la phase de personnalisation les données statiques (PAN, nom, prénom, date d'expiration) sont identifiées et hachées avec l'algorithme SHA-1. L'empreinte est ensuite chiffrée avec la clé privée RSA de l'émetteur pour réaliser une signature ou SSAD[13]. Les tailles de clés RSA sont limitées à cause de l'espace de stockage des cartes EMV et du fonctionnement de ce standard. En effet, la taille maximale prévue est de 248 octets soit 1984 bits. Les clés RSA utilisées sont le plus souvent de 1024 bits, cependant depuis 2018, EMV oblige l'utilisation de clé 1408 bits. Cette limite sera portée à 1984 en 2025 mais à ce moment-là, la limite sera atteinte.

La signature ainsi que la clé publique de l'émetteur sont stockées dans la partie disponible en lecture de la carte afin qu'elles puissent être récupérées par un point d'acceptation dans une transaction. Lors d'un paiement, le TPE récupère toutes les informations disponibles sur la carte, il se sert de la clé publique pour vérifier la signature et récupérer la hache.

13 SSAD : Signed Static Application Data

Il génère ensuite un hash avec les informations statiques et le compare à celui trouvé en déchiffrant la signature. S'ils sont identiques, la carte est authentifiée.

De plus, dans ce mode d'authentification lors de la saisie du code PIN sur un TPE, ce dernier envoi le code sans méthode de chiffrement à la carte pour vérification.

7.1.1.2 DDA

La méthode DDA corrige les principaux problèmes de SDA, elle est aujourd'hui la plus communément utilisée. Elle nécessite cependant une modification de la puce EMV afin de pouvoir traiter les calculs cryptographiques asymétriques. Il y aura avec cette méthode l'authentification de la puce en plus des données.

Toujours durant la phase de personnalisation, l'émetteur crée une bi-clé RSA propre à la carte, la clé privée est stockée dans la zone secrète de la puce. La clé publique est signée par la clé privée de l'émetteur, afin d'attester de la provenance de la clé et de créer un certificat, ce dernier est stocké dans la zone en lecture seule. Les clés, dans ce cas, sont également sont limitées en taille.

En plus du SDA lors d'un paiement, le TPE récupère le certificat signé par l'émetteur et vérifie la signature de ce certificat avec la clé publique de l'émetteur. Les TPE ont toutes les clés publiques des émetteurs dans leurs magasins. Une fois vérifiée, le TPE envoie à la puce un nombre généré aléatoirement à la carte, de son côté la carte génère son ICC Dynamic Number (nombre aléatoire généré par le circuit intégré). Elle concatène ensuite les nombres aléatoires et les signes en réalisant un hash SHA1 et en chiffrant le résultat avec sa clé privée. La carte envoie par la suite au TPE la signature ainsi que son ICC Dynamic Number qui va vérifier la signature avec le certificat de la carte et réaliser un hash de la concaténation des deux nombres aléatoires. Si les résultats concordent, la carte est authentifiée.

Dans cette version, la transmission du code PIN du TPE vers la carte est chiffrée avec la clé publique de la carte.

7.1.1.3 CDA

La méthode CDA est la dernière en date pour EMV, elle se veut plus sécurisée et plus complexe que les deux autres méthodes. Le fonctionnement reste cependant proche de DDA, elle nécessite également la prise en compte de la cryptographie asymétrique par la carte à puce et le TPE.

Pour assurer un niveau de sécurité plus élevé la puce génère une signature au moment de la génération du cryptogramme. Cette action intervient au moment où le TPE demande à la carte de générer un cryptogramme (ARQC ou TC). La signature est réalisée grâce à plusieurs informations comme le nombre aléatoire générée par le terminal et les données de la puce.

Les données sont hachées puis signée avec la clé privée de la puce, le résultat de cette opération est envoyée au TPE. De son côté, point d'acceptation va déchiffrer les données envoyées par la puce avec la clé publique de la puce. Il va en suite recalculer l'empreinte des données et comparer aux résultats déchiffrés. Si les données sont identiques, la transaction est acceptée.

7.1.2 L'autorisation

L'autorisation, comme présentée ci-dessus est un système de questions-réponses de l'accepteur à l'émetteur de la carte qui permet de vérifier la saisie du PIN code en mode en ligne et pas hors ligne comme dans les cas précédents. Elle permet de vérifier l'approvisionnement du compte et les informations de la carte. L'autorisation n'est pas automatique pour chaque transaction, car elle rend la transaction plus longue. Elle intervient dans plusieurs cas :

- Retrait dans un distributeur (autorisation obligatoire)
- Pour les sommes dépassants le montant fixé par le commerçant (20/30€ généralement)
- Aléatoirement

L'autorisation intervient après la vérification des données du porteur et c'est la carte directement qui indique si une autorisation est nécessaire ou non. Après l'authentification le TPE demande à la puce de générer un cryptogramme qui sont les suivants :

- TC, Transaction Certificate : transaction acceptée (pas de vérification en ligne)
- AAC, Application Authentication Cryptogram : transaction refusée (pas de vérification en ligne)
- ARQC, Authorization Request Cryptogram : demande d'autorisation en ligne

La décision prise par la carte est calculée avec plusieurs facteurs. Le TVR[14] un champ sur 5 octets gérés par le TPE qui force l'autorisation dans les cas d'une nouvelle carte pour l'activer par exemple, ou lors de l'échec de la validation des données du porteur.

Ensuite l'IAC[15] qui garde la même forme que le TVR. L'IAC est stocké sur la carte et transmet la décision de l'émetteur, il peut avoir plusieurs valeurs comme refus si l'émetteur n'accepte pas l'autorisation, On-Line si l'émetteur demande la vérification en ligne et défaut en cas de problème de connexion avec la banque émettrice.

Enfin le TAC[16] qui garde le même principe que l'IAC mais avec l'acquéreur et non l'émetteur, les données sont donc stockées sur le TPE et non sur la carte.

Voici un exemple de transaction avec autorisation en ligne. Une fois la carte dans le TPE, ce dernier va lire les données de la carte et récupérer les données pour la vérification et également les trois IAC. Le TVR est mis à jour continuellement afin de suivre les différentes étapes.

Le TPE va maintenant vérifier s'il doit accepter la transaction ou non avec les données de la carte et du moyen d'acceptation, trois choix sont possibles :

- Refusé : comparaison faite entre le TAC et l'IAC. Si un bit est à 1, la transaction est refusée, les deux parties peuvent refuser la transaction (échec authentification, carte expirée, etc.), un cryptogramme AAC est généré.
- Online : après vérification des IAC & TAC refus par le TVR, la même opération est effectuée pour l'online, pour chaque bit à 1 une demande ARQC est créée.
- Offline : les cas de vérification hors ligne ont déjà été abordés dans la partie carte bancaire, ils sont utilisés après ces différents tests, un TC est alors envoyé par la carte.

Des schémas, étape par étape pour l'ensemble de ce système sont disponibles en annexe VI.

14 TVR : Terminal Verification Results
15 IAC : Issuer Action Code
16 TAC : Terminal Action Code

L'ARQC est donc générée par la carte. Ce dernier contient beaucoup d'informations comme le numéro de carte, la date d'expiration, le montant de la transaction ou encore le code pays.

Le code PIN est également fourni lors de l'échange chiffré avec l'algorithme Triple DES et des clés de 112 bits[17].

Les différentes données sont concaténées et sont chiffrées avec l'algorithme Triple DES avec deux clés de 56 bits (différentes de celle du PIN code). Le mode de l'algorithme utilisé est CBC-MAC[18], ce mode de chiffrement permet d'authentifier les messages envoyés avec Triple DES.

L'infrastructure côté émetteur peut maintenant recevoir la demande d'autorisation ARCQ en déchiffrant les flux sur son HSM avec les différentes clés Triple DES mise en place durant la personnalisation. Après vérification des données le HSM peut renvoyer une ARCP[19] toujours en utilisant l'algorithme Triple DES. La puce devra donc déchiffrer ce message afin de s'assurer que la réponse vient bien de sa banque. Ce n'est que maintenant que la carte reçoit la validation ou non de la transaction en ligne.

L'ensemble des flux générés par une autorisation sont aussi chiffrés. Les TPE sont connectées au réseau IP par différents moyens comme les réseaux MPLS ou les lignes dédiées pour les grandes enseignes, ou plus communément des simples liens ADSL ou encore le réseau GSM.

Les échanges entre les différents points d'acceptation et les serveurs d'autorisations sont chiffrés avec les protocoles SSL/TLS. Chaque TPE contient un ensemble d'autorités de certification dans sa mémoire afin de vérifier les certificats envoyés par les serveurs. En France, l'autorité utilisée par le GIE CB est PayCert.

Dans l'utilisation qui est faite aujourd'hui plusieurs versions sont utilisées, allant encore d'SSL v3 à TLS1.2. Plusieurs algorithmes sont donc utilisés pour assurer le fonctionnement, cette large utilisation de protocole est due au parc très hétérogène de TPE.

17 Très peu d'informations sont disponibles sur le transit du code PIN, il s'agit donc ici d'une déduction.
18 CBC-MAC : Cipher Block Chaining – Message Authentication Code
19 ARPC : Authorisation ResPonse Cryptogram

Cela implique donc l'utilisation de certificat SHA 1 par les émetteurs ainsi que le support de plusieurs ciphers suites comme MD5, RC4 ou encore DES. Le problème est le même pour l'utilisation de TLS1.0.

7.1.3 L'acceptation

Sur la phase d'acceptation pure, en dehors des autorisations en ligne et hors ligne, plusieurs données sont envoyées aux serveurs d'acquisitions qui sont différents de ceux utilisés pour les autorisations.

Les données sont utilisées dans le cadre de la télé-collecte, et dans cette partie le système est le même que sur la partie autorisation. Les flux sont chiffrés entre les TPE et les serveurs avec les protocoles SSL/TLS et des certificats délivrés par l'autorité PayCert.

Le problème est également le même sur l'aspect des versions des différents protocoles et des algorithmes.

De plus, dans ce mode de fonctionnement, les données comme :

- Le numéro de carte
- Nom & prénom du porteur
- Date d'expiration
- Montant de la transaction

Sont envoyées sans chiffrement supplémentaire entre les TPE et les machines chargées de l'acquisition.

7.2 Les technologies utilisées

Même s'il existe beaucoup d'autres cas qui n'ont pas été expliqués ici, nous allons voir plus en détail les différents protocoles et algorithmes principalement utilisés.

7.2.1 RSA

Utilisé dans plusieurs des cas ci-dessus, RSA du nom de ces trois inventeurs, est le protocole de chiffrement asymétrique le plus répandu aujourd'hui dans tous les domaines, que ça soit dans les échanges Web ou dans beaucoup d'autres cas, comme les VPN IPSec ou encore le protocole GPG/PGP.

Ce protocole est pourtant établi sur un principe extrêmement simple, il est basé sur la décomposition en facteurs premiers d'un entier n.

Il est très difficile de retrouver les facteurs pour n = p × q avec n connu, p et q étant des nombres premiers suffisamment grand. Ce problème est appelé le problème RSA, il a forcément une solution, mais elle reste difficilement retrouvable avec les ordinateurs actuels.

La compétition de factorisation RSA a mené à une factorisation réussie pour RSA-768 maximum en utilisant des nombres RSA ou nombres semi-premiers, c'est-à-dire un résultat de deux facteurs premiers.

Cependant, RSA est un protocole très fragile, une seule mauvaise configuration peut remettre en cause l'ensemble du chiffrement. De plus, la sécurité des échanges dépend directement de la taille des biclés utilisées.

Ces dernières années, la taille des clés n'a cessé d'augmenter. Même si par définition, il n'y a pas de limite à la taille des clés RSA, dans la pratique des limites sont très rapidement observées. Notamment au niveau de la vitesse des échanges, plus les clés sont longues plus le temps pour la génération est important. Et également le temps des échanges augmente en même temps que la taille des clés.

La taille des clés RSA recommandée par le NIST et l'ANSSI[20] est de 2048 bits, et de 3072 bits en 2030. On remarque alors que la monétique ne respecte pas les recommandations en utilisant toujours des clés de 1024 bits et en ayant d'ailleurs une limite maximum de 1984 bits. Dans le monde monétique un passage sur des clés 2048 bits et de 3072 est pour l'instant impossible.

7.2.2 3DES

Triple DES (Data Encryption Standard) ou 3DES lui est un algorithme de chiffrement symétrique par bloc, il est dérivé de l'algorithme DES en utilisant trois fois la fonction de chiffrement avec deux ou trois clés. Des recherches ayant été effectuées, l'utilisation de deux ou trois clés différentes assure le même niveau de sécurité. Dans les différentes utilisations dans le cadre monétique, seules deux clés sont utilisées.

DES comme 3DES utilisent des tailles de blocs de 64 bits et des clés de la même taille. Cependant, les clés ne font réellement que 56 bits car pour 64 bits il faut compter 8 bits pour assurer l'intégrité de la clé. Dans le fonctionnement avec deux clés la taille est donc de 112 bits et non 128.

20 ANSSI : Agence National de la Sécurité des Systèmes d'Information

Avec les trois tours de 3DES le fonctionnement est le suivant : tout d'abord un bloc est chiffré avec la clé n°1, puis déchiffré avec la clé n°2 et pour finir chiffré avec la clé n°1 ou 3 si utilisation de trois clés.

Comme présenté ici :

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

Figure 12. Source : wikipedia.org. Fonction mathématique de l'algorithme 3DES

Plus précisément, lors de chaque exécution de DES le message va être découpé en blocs de 64 bits qui vont être permutés. Les blocs vont être coupés en deux parties et 16 rondes seront effectuées sur ces moitiés de blocs avec des actions de permutation et de substitution.

L'algorithme DES initialement utilisé est obsolète aujourd'hui et il est également très lent. Par la même occasion, 3DES lui est tout de même trois fois plus lent que DES même s'il reste pour l'instant cryptographiquement sûr.

L'ANSSI indique qu'il est préférable d'utiliser 3DES comme dernier recours, car ce dernier utilise des tailles de blocs et de clés réduites. De ce fait, il faut renouveler les clés régulièrement, ce qui n'est pas le cas ici présent. De plus, le NIST indique que pour lui 3DES est déprécié depuis 2018 et sera interdit à partir de 2023.

7.2.3 SHA-1

SHA-1 lui est utilisé dans presque tous les cas vus ci-dessus. Cette fonction de hachage est utilisée pour assurer l'intégrité et pour signer les différents échanges. Il est le successeur de SHA-0, son fonctionnement est d'ailleurs exactement le même, sauf au niveau de la taille de la sortie qui est de 160 bits pour SHA-1.

SHA-1 est donc une fonction à sens unique, elle prend en entrée un message de 2^{64} bits maximum. Elle permet grâce à diverses opérations comme du bourrage et une série de 80 tours en transformant l'entrée et à d'autres actions de fournir en sortie un condensat. Ce condensat est censé être différent pour chaque fichier, et le clair ne doit pas pouvoir être retrouvé à partir de l'empreinte.

SHA-1 quant à lui, est un algorithme obsolète aujourd'hui et ça depuis 2011, cela est dû à plusieurs attaques par collision d'abord théorique et identifié par plusieurs grands noms de la cryptographie comme Bruce Schneier.

Théoriquement, il suffit à 2^{63} opérations pour créer une collision dans l'algorithme et plus concrètement, Google en 2017 a réussi à créer deux fichiers PDF avec seulement 2^{63} opérations. En plus de l'attaque initiée par Google, une recherche récente réalisée par des chercheurs français et singapouriens montre qu'il est désormais possible de réaliser des attaques avec préfixe choisi qui sont beaucoup plus importantes avec des moyens raisonnables.

Une attaque par préfixe choisi va beaucoup plus loin qu'une simple collision, elle permet de réaliser une collision en permettant le choix des données qui vont entrer en collision. Cela permet de remettre totalement en cause l'intégrité et la confidentialité du message et de réaliser des attaques importantes.

L'utilisation de cet algorithme est donc prohibée par l'ensemble des institutions, en particulier sur la génération de signatures électroniques. L'ANSSI ainsi que le NIST interdisent son utilisation et conseillent d'utiliser des algorithmes plus forts comme SHA256 ou SHA-3.

Dans le cadre de la monétique SHA-1 est encore principalement utilisé comme vu ensemble.

7.2.4 SSL/TLS

SSL/TLS sont eux différents, car ils intègrent tous les types de cryptographie à la fois, de la symétrique aux algorithmes de hachage. Dans l'utilisation de la monétique, plusieurs versions sont utilisées, comme SSLv3, TLS 1.0 ou encore TLS 1.2. TLS 1.1 n'est pas abordé, car il n'est que très peu utilisé.

Il n'y a que très peu d'écart entre les différentes versions citées ci-dessus, les principaux changements sont les algorithmes supportés. En effet, depuis les premières versions, il n'y a pas eu de changement majeur dans le système SSL/TLS. À chaque nouvelle version des protocoles plus forts sont ajoutés afin de suivre l'évolution et de rester sûr. Mais une des faiblesses est que très souvent, les protocoles faibles restent compatibles avec les nouvelles versions, et les anciennes versions d'SSL/TLS peuvent également rester activées.

Dans le monde de la monétique, SSLv3 et TLS1.0 sont toujours utilisés alors que ces derniers sont vulnérables à un grand nombre d'attaque. SSLv3 par exemple utilisent des « ciphers » très faibles pour aujourd'hui comme MD5, RC4, SHA-1 ou DES. L'utilisation de ces algorithmes peut remettre en cause le chiffrement ainsi que l'intégrité des échanges. Le constat est le même pour TLS1.0.

Ce dernier est d'ailleurs interdit par PCI DSS depuis 2018. De plus, l'ensemble des agences s'accordent à dire qu'il faut désactiver l'ensemble des versions de TLS inférieure à TLS1.2 car elles ne sont plus sûres cryptographiquement.

Les navigateurs ne supportent plus certaines de ces versions et interdisent les certificats SSL signés en SHA-1 par exemple, ce qui est une avancée. Firefox par exemple, ne supporte plus que les versions 1.2 & 1.3 de TLS.

Ci-dessous, un exemple de session avec le protocole TLS :

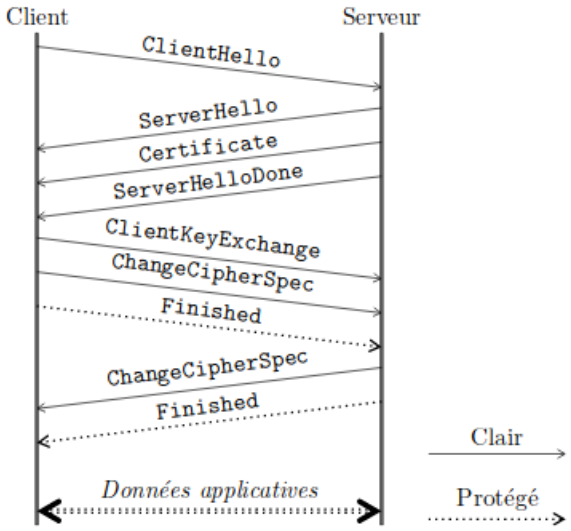


Figure 13. Source : ssi.gouv.fr. Schéma d'une session SSL/TLS

Lors du « client Hello » le client va envoyer plusieurs informations au serveur comme les différentes versions de TLS supportées ainsi que la liste des suites cryptographiques que le client est capable d'utiliser. Chaque suite est composée d'un algorithme d'échange de clé, d'un autre assurant l'authentification du serveur et enfin d'un algorithme symétrique pour l'échange des données et de hachage pour l'intégrité.

Voici un exemple de suite : TLS_RSA_WITH_AES_256_CBC_SHA2

On retrouve bien l'algorithme d'authentification avec RSA, AES-256-CBC comme algorithme de chiffrement symétrique par bloc avec une clé de 256 bits et enfin SHA256 pour assurer l'intégrité des données.

Enfin ce message comporte également un message « client_random » afin de générer une clé dérivée.

Le serveur renvoie dans un « serveur Hello » dans lequel est renseigné la version du protocole retenue par le serveur ainsi que la suite cryptographique.

Le serveur envoie également son certificat au client ainsi qu'un message l'invitant à répondre, « ServerHelloDone ».

Le client va alors vérifier de son côté le certificat. S'il est valide il va continuer les échanges et générer le « master-secret » qu'il va ensuite chiffrer avec le certificat et l'envoyer au serveur dans le « ClientKeyExchange ».

Le serveur peut alors déchiffrer le secret envoyé par le client avec sa clé privée. Le client et serveur peuvent maintenant utiliser les informations transmises dans le « Client Hello » et le « Serveur Hello » afin de créer une clé dérivée et de commencer les échanges.

Pour terminer, les échanges de type « ChangeCipherSpec » servent à activer et à vérifier les clés échangées.

TLS 1.3 a volontairement été écarté car c'est une version toute nouvelle du protocole sorti en 2018 qui change grandement son fonctionnement. Il n'est cependant que très peu utilisé, voire pas du tout dans le système monétique actuel.

7.3 Pourquoi cela ne suffit pas

Après avoir vu ensemble les algorithmes principalement utilisés dans le système monétique, il est facile de noter qu'ils sont bien souvent obsolètes ou non adaptés pour le traitement de données si importante.

L'utilisation de ces algorithmes et techniques entraîne un risque important sur les données, surtout dans un système où des données bancaires sont manipulées. La monétique devrait être l'inverse de ce qu'elle est aujourd'hui, et être l'exemple dans l'utilisation des algorithmes cryptographiques. Des attaques ont notamment été observées sur l'authentification des données SDA. Cette dernière ne protège pas la carte contre la copie, des fausses cartes ont ainsi pu être créées et étaient fonctionnelles en cas de vérification hors ligne des données.

De plus, avec l'évolution constante des technologies et de la puissance des machines, l'utilisation de protocole comme SHA-1 devient un danger réel et plus seulement théorique. Il en est de même pour la taille des clés RSA qui est trop faible par rapport aux données qui transitent.
Le problème est d'ailleurs le même sur tous les algorithmes utilisés, les moyens mis en œuvre ne sont pas à la hauteur.

Ils sont tous en fin de vie, et presque tous dépréciés ou interdits d'utilisation dans les autres cas. L'utilisation de ces algorithmes pourra être encore tolérée dans les années à venir, mais il va falloir trouver rapidement des alternatives et d'autres systèmes pour répondre à la demande toujours croissante en matière de cryptographie et de sécurité plus généralement.

Comment des systèmes si faibles, déjà vulnérable pour certains et probablement rapidement pour les autres peuvent être utilisés pour faire transiter des données aussi sensibles que les données bancaires ? Alors que ces algorithmes ne sont même plus utilisés pour du chiffrement de simple navigation Web.

La question est pourtant très simple mais la réponse reste très complexe, car elle dépend de plusieurs facteurs qui vont être abordés dans les points suivants.

7.4 Contraintes humaines

L'humain est au cœur du problème, car c'est à lui de choisir les différents algorithmes et de les mettre en œuvre au sein des différentes plateformes. Or, on se rend rapidement compte que dans la majorité des cas, la sécurité et la cryptographie plus précisément ne sont pas leurs priorités. Pour les équipes d'exploitation et de développement, l'essentiel c'est que l'application ou que le système fonctionne.

Le niveau de sécurité n'est pas primordial, et cela était encore plus vrai quand l'ensemble des systèmes ont été conçus. Car comme déjà évoqué, la monétique est un métier vieillissant, et les systèmes n'ont pas été conçus pour résister et s'adapter à l'informatique que nous connaissons aujourd'hui.

En plus du manque d'intérêt, la cryptographie étant une discipline complexe, les mêmes personnes n'ont pas dans certains cas le bon niveau de compétence dans le domaine pour assurer son fonctionnement dans les meilleures conditions.

Heureusement, les temps changent et les mentalités aussi. Nous avons aujourd'hui, tous une vision plus ouverte sur ces aspects-là. À ce jour, la cryptographie et la sécurité prennent des places de plus en plus importantes dans les entreprises.

Mais avec les infrastructures vieillissantes et les contraintes imposées par les différents organismes (CB, PCI DSS, EMV), les personnes en charge se contentent de l'aspect fonctionnel actuel et ne mettent en place des améliorations que quand cela est imposé.

7.4.1 Contraintes opérationnelles

En supplément des contraintes humaines, il en existe d'autres liées à l'aspect opérationnel de la monétique.

En effet, ce domaine est l'un des rares ou une interruption de service n'est pas possible, à chaque interruption les clients ne peuvent plus accepter de paiement, ce qui cause de gros préjudices pour l'entreprise fournissant le service et pour son client.

Il est donc très complexe de réaliser des modifications sur les infrastructures de production, elles ne sont donc que très peu modifiées dans leur cycle de vie. Cet aspect est également en cause dans la proposition des algorithmes faibles, car vu que l'application n'est que très peu modifiée et ne peut être arrêtée, si elle a été pensée pour utiliser des algorithmes spécifiques, il sera très compliqué de mettre à jour son fonctionnement. Cela inclut généralement des modifications côté client également, ce qui complique un petit plus la tâche.

De plus, les clients ne veulent généralement pas de changement de leur côté, ce qui oblige à laisser en activité des services historiques qui ne sont pas à la hauteur de l'informatique moderne. Lorsqu'un changement est planifié, il faut également prévoir l'ensemble des cas et réaliser énormément de test pour ne pas perturber la production. Ces raisons ralentissent encore les changements dans les applications.

7.5 Contraintes techniques & matérielles

Enfin, l'une des principales contraintes est que la sécurité des échanges dépend du point d'entrée, c'est-à-dire le point d'acceptation, car il est le client. Le parc de TPE est très important et très hétérogène, en France en 2018 le GIE CB a identifié 1 770 000 commerçants CB avec un ou plusieurs TPE.

Les terminaux de paiement sont fournis par les banques acquéreuses, qui se fournissent elles-mêmes chez les constructeurs. Mais le vrai problème est que la majorité des TPE utilisés sont anciens. Ils ne supportent pas les nouveaux algorithmes, il ne sert donc à rien de mettre en place des algorithmes forts sur les cartes et les serveurs si les terminaux ne peuvent pas les utiliser.

De plus, les nouveaux TPE, supportent toujours les algorithmes comme SHA-1 ou encore 3DES, ce qui ne pousse pas à l'utilisation d'algorithmes plus récents. Les commerçants ne veulent pas de leur côté changer de TPE, car ils ne sont pas sensibilisés à ces problématiques. De plus ce changement peut être onéreux pour eux.

Les différents organismes poussent les commerçants à changer de TPE mais ce changement est très lent.

8 Partie 3 : Les évolutions de la monétique

Pour renforcer la sécurité et l'aspect cryptographique des échanges, plusieurs changements sont prévus notamment au niveau de la certification PCI DSS et des standards EMV.

Les futures versions de PCI DSS devraient être plus strictes sur les algorithmes utilisés, comme les versions de TLS. Au niveau d'EMV, des améliorations sont également abordées, comme l'utilisation des courbes elliptiques, de l'algorithme AES ou encore de SHA-256. Ces améliorations sont prévues à tous les niveaux, que ça soit sur les cartes ou sur les différents protocoles autour de cette dernière.

Ces changements sont également amenés grâces aux nouvelles recherches effectuées par les mêmes chercheurs français et singapouriens. Elles démontrent qu'il est officiellement possible de réaliser une attaque avec préfixe choisi sur l'algorithme SHA-1 avec des moyens raisonnables.

En plus de ces changements que l'on qualifiera d'obligatoires, la monétique fait face depuis peu à une démocratisation de ces services, ce qui amène des changements profonds, que ça soit au niveau de la sécurité mais également au niveau organisationnel et technique.

8.1 L'évolution du métier

Comme nous avons pu le voir dans ce document, la monétique est un « vieux » métier. Cependant, il existe depuis quelques années un renouveau dans ce secteur. Des nouveaux acteurs sont arrivés ce qui permet des améliorations notables, au niveau de la sécurité, de la mobilité et des technologies utilisées principalement.

8.1.1 Les nouveaux moyens de paiement

Cette évolution passe également par le changement des habitudes des consommateurs et donc de nouveaux moyens de paiement.

L'évolution des paiements est forte, chaque année de nouveaux moyens de paiement arrivent sur le marché. Étonnamment, certains ne sont pas initiés par les grands groupes bancaires mais par des grands fabricants de matériel ou des jeunes start-ups par exemple.

Il y a notamment les paiements qui se font sans contact, que ça soit sur mobile via des applications et des protocoles dédiés comme Google Pay ou encore Apple Pay, ou les paiements sans contacts plus classiques avec votre carte bancaire. Ses protocoles sont totalement nouveaux et peuvent donc se permettre d'utiliser les dernières technologies disponibles ainsi que d'avoir une sécurité maximale.

Ces moyens de paiement permettent de moderniser l'ensemble de la monétique. Ils obligent les banques, les commerçants et les différents organismes à s'adapter et donc à moderniser les outils et les différents matériels utilisés.

Les paiements ne se font plus par carte directement avec une authentification par code, mais ils se font via votre smartphone ou via votre montre connectée. L'authentification est assurée par ce dernier, avec une empreinte digitale ainsi que la reconnaissance faciale. Les paiements restent toujours basés sur votre carte bancaire et ils utilisent toujours les différents réseaux mais l'expérience cliente est différente car simplifiée.

Les cas de fraudes sont particulièrement faibles sur ces moyens de paiement et même sur les paiements sans contact. La mise en place d'une telle attaque, même si elle paraît simple au premier abord, reste très compliquée.

Cela pose cependant d'autres problèmes, car les paiements ne sont plus traités par des organismes reconnus comme les banques, mais par des entreprises du secteur privé et plus particulièrement les leaders en matière de technologie et de traitement des données. De plus, ces nouveaux moyens de paiement impactent l'acceptation, car des évolutions arrivent de ce côté-là pour améliorer cette l'expérience du paiement.

8.1.2 Les nouveaux acteurs

Ces nouveaux moyens de paiement sont proposés généralement par des nouveaux acteurs. Jusqu'à maintenant, la monétique était dédiée aux entreprises historiques qui dominaient fortement le marché. Mais depuis peu, avec la croissance des services dit « Cloud » et les évolutions importantes de la technologie, le marché s'ouvre.

Nous voyons donc l'émergence de ce qu'on appelle des « fintech », des start-ups qui révolutionnent la finance grâce à la technologie. Rien qu'en France, il existait 352 fintechs actives fin 2019. Ce chiffre démontre l'importante mobilisation des entreprises pour le milieu bancaire, réservé jusqu'ici à des élites.

Pour accompagner ces fintechs, les principaux fournisseurs de services du milieu se sont mis à proposer des solutions clés en main à ces entreprises. C'est-à-dire des services et des hébergements qui sont certifiés PCI DSS et conformes aux normes EMV.

Cela permet aux entreprises désirant se lancer dans la monétique d'économiser de l'argent et du temps afin d'ouvrir fortement ce marché jusqu'à maintenant très fermé. Les principaux fournisseurs sont des grands noms comme Amazon Web Services ou encore OVH. Pour la norme PCI DSS les demandes vont jusqu'aux accès des différents centres de données. La partie infrastructure est le premier centre de coût pour les entreprises historiques et l'arrivée de ce genre de service est une révolution dans ce secteur.

L'avantage avec ce type de solution est que la partie infrastructure est entièrement évolutive, c'est-à-dire que vous payez seulement ce que vous consommez et qu'il est possible de la faire évoluer rapidement en cas de forte demande.

L'entreprise devra faire certifier seulement la partie applicative restant dans son périmètre. Selon les offres, le reste de la chaîne peut être externalisé vers des services tiers. Elle n'a plus à se soucier de la partie infrastructure, ce qui facilite grandement le lancement d'une application qui serait basée sur le paiement. Cela permet de s'affranchir d'un grand nombre de contraintes.

L'arrivée des nouveaux acteurs et des nouvelles solutions permet d'améliorer indirectement la sécurité de ces services.

Ces acteurs, s'ils sont nouveaux, n'ont aucun historique et ne doivent pas continuer à maintenir des services vieillissants. Ils utilisent directement les derniers services disponibles avec les meilleures normes en termes de sécurité informatique et de cryptographie. De part ce fait, ils sont également beaucoup plus libres sur leurs actions.

Au niveau purement infrastructure, ces acteurs se basent principalement sur des solutions hébergées qui sont soumises aux contraintes de sécurité misent en avant par les différentes institutions.

Pour reprendre l'exemple d'AWS[21], ils proposent une multitude de services conforme nativement au PCI DSS. Cela peut aller d'un simple service de stockage

21 Amazon Web Services

de fichiers à des machines dédiées ou même des équipements très spécifiques comme des HSM pour la gestion de la partie cryptographie.

Ces nouveaux acteurs, que cela soit Max, Apple avec Apple Pay ou encore Linxo n'améliorent pas seulement la monétique en termes de sécurité. Ils se concentrent principalement sur l'expérience client, c'est-à-dire comment faciliter la vie d'un client désireux de payer avec sa carte bancaire. Ces améliorations sont également notables pour les acquéreurs, il est aujourd'hui beaucoup plus facile pour les commerçants de se procurer des terminaux de paiements. Ces derniers ne sont plus proposés seulement par des banques car aujourd'hui il suffit d'avoir un accès Internet pour recevoir de l'argent.

L'arrivée de ces nouveaux acteurs permet à l'ensemble du secteur de progresser et d'accélérer le changement chez les fournisseurs historiques. Ces derniers sont obligés de changer les méthodes de fonctionnement et de pousser le changement au niveau de leurs clients et partenaires pour rester compétitif. Cela implique d'accélérer la transition au niveau des services historiques, et donc l'amélioration de la sécurité et de la cryptographie.

8.1.3 L'évolution des protocoles

L'arrivée des nouveaux moyens de paiement et des nouveaux acteurs amène automatiquement des améliorations au niveau des paiements par carte à puce. Mais comme nous l'avons déjà abordé avec EMV, le standard utilisé date de 2011. Des modifications et des corrections ont été adoptées mais cela ne révolutionne pas le fonctionnement expliqué en première partie de ce document.

Les protocoles utilisés sont identiques dans l'ensemble, cependant ils ont fait des améliorations au niveau de la cryptographie en permettant l'utilisation de l'algorithme AES en remplacement de DES et de 3DES. Des implémentations plus strictes sont également en cours de déploiement sur la partie des flux SSL/TLS.

Le groupe EMV travaille sur des améliorations bien plus importantes, notamment pour prendre en compte des nouveaux algorithmes aujourd'hui essentiel comme SHA-256 un algorithme de hachage ou encore la cryptographie basée sur les courbes elliptiques. Ils ont déjà publié des documents concernant leurs utilisations. Ces fonctionnalités sont déjà adoptées par les autres moyens de paiement, qui eux n'ont pas de problématiques liées à l'historique. Apple Pay par exemple utilise conjointement la cryptographie basée sur RSA ainsi que celle basée sur les courbes elliptiques. Il intègre bien entendu l'utilisation d'algorithme

de chiffrement plus fort comme SHA-256 ou encore Blake. Une notion importante est l'utilisation de TLS 1.3 sur la partie des flux réseaux, cela permet de manière assez simple d'améliorer considérablement le niveau de sécurité.

Concrètement, aujourd'hui aucune amélioration fondamentale n'est déployée sur la partie paiement physique avec l'utilisation de carte à puce. EMV prépare avec beaucoup d'importance le futur du standard, tout en prenant en compte les problématiques liées aux matériels et aux services historiques. L'utilisation dans les autres systèmes de paiement de technologie plus avancée devrait permettre un retour d'expérience à EMV.

8.2 L'amélioration de la cryptographie

Plusieurs changements sont prévus ou abordés dans le système cryptographique du standard EMV, nous allons voir ensemble plus en détails les principales évolutions.

8.2.1 Courbes elliptiques

Une des améliorations notables est le changement d'algorithme de chiffrement asymétrique avec l'utilisation des courbes elliptiques à la place du chiffrement RSA. Ce changement n'est pour l'instant pas encore déployé, mais il est étudié depuis plusieurs années par EMV. L'utilisation de cet algorithme, à certes des avantages indéniables, mais également de nombreuses contraintes.

Le chiffrement basé sur les courbes elliptiques est un ensemble de méthodes cryptographiques qui utilise les propriétés des courbes elliptiques pour le chiffrement des données.

Ce système, comme pour le problème RSA, est basé sur des problèmes mathématiques complexes, impossible à réaliser aujourd'hui par un ordinateur classique. Le système en question est basé sur le problème du logarithme discret.

Le principal avantage des courbes elliptiques est que pour une taille de clé égale, la sécurité est plus forte qu'avec l'algorithme RSA.

Comme le démontre cette illustration avec des chiffres tirés d'un rapport du NIST :

Symmetric	DH or RSA	ECC
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Figure 14. Source : net-security.fr. Tableau d'équivalence des différentes tailles de clés de chiffrement

Nous pouvons voir que l'utilisation des courbes elliptiques permet de réduire jusqu'à plus de 10 fois la taille des clés. Cela permet d'avoir un niveau de sécurité plus important en utilisant un stockage réduit. C'est idéal dans le cadre de l'utilisation sur des objets connectés et principalement sur les cartes bancaires, surtout avec les limites au niveau de la mémoire déjà abordée dans ce document.

Plus techniquement, les courbes elliptiques sont basées comme leurs noms l'indiquent sur des courbes, cela peut se matérialiser sous cette forme :

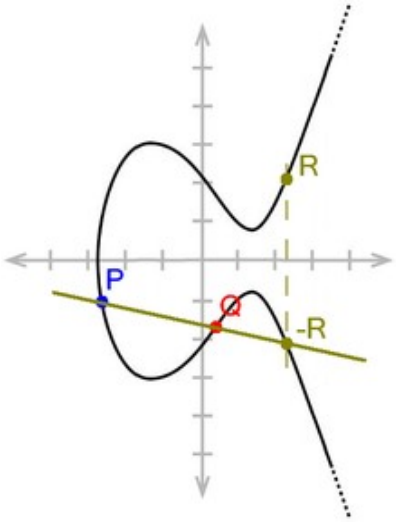


Figure 15. Source : wikipedia.org. Additions de points sur une courbe elliptique

Ce système est plus complexe sur le plan mathématique que RSA. Le but ici est de présenter ce système dans son ensemble et d'en comprendre les grands

principes. Les informations sont volontairement simplifiées pour faciliter la compréhension.

Une courbe elliptique est un cas particulier de courbe algébrique. Elles ont de nombreuses applications et utilités dans le monde des mathématiques et dans notre cas, de la cryptographie. Une courbe elliptique est un ensemble fini d'éléments, avec laquelle nous sommes capables de faire des opérations simples comme l'addition, la multiplication, la soustraction et la division. L'équation la plus simplifiée pour une courbe elliptique est la suivante :

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

Où a et b sont les coefficients de la courbe et appartiennent à l'ensemble K.

Les calculs les plus importants dans notre cas sont l'addition ainsi que la multiplication :

- Quand on a deux points P et R sur une courbe K, on peut calculer Q = P + R, Q appartient également à K.
- Quand on a un point P sur une courbe K, on peut additionner k fois ce même point. Par exemple si k = 2, on peut calculer P + P. Ce qui revient à multiplier les points Q = k×P. Q appartient également à K.

Cette illustration permet de visualiser ces opérations :

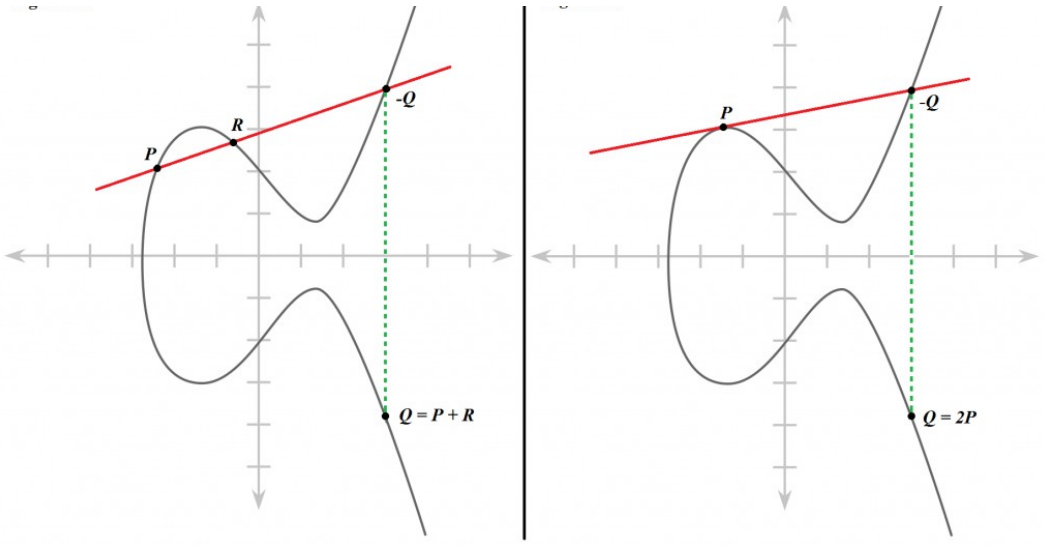


Figure 16. Source : www.smalsresearch.be. Illustration d'addition (gauche) et de multiplication (droite) sur des courbes elliptiques

Sur l'illustration de gauche nous voyons une addition de deux points P et R. Sur celle de droite, une multiplication du point P pour k = 2.

Pour définir l'addition du point P avec lui-même ou la multiplication de deux points pour k = 2, il faut tracer une tangente au point P. Cette droite est en rouge sur nos illustrations, elle coupe la courbe en un point -Q. La symétrique de ce point, comme pour l'addition, est le résultat Q.

Pour en venir à l'essentiel, comme pour RSA il est essentiel de trouver deux nombres : un pour la clé privée et un autre pour la clé publique. Avec un point P sur une courbe elliptique, il est très facile de calculer Q = k×P pour un entier k, mais il est difficile de retrouver la valeur de k quand seulement P et Q sont connus.

Avec ces propriétés nous avons un système de chiffrement asymétrique ou à clé publique. La clé privée est un entier k et la clé publique correspond au point Q, résultat de l'opération k×P ou P est un point publiquement connu.

Comme vous avez pu le voir, l'utilisation des courbes elliptiques est complexe et cela ne se limite pas qu'à la théorie. Contrairement à RSA, ce système n'est pas complet, c'est-à-dire que les courbes elliptiques ne permettent pas de chiffrer des messages, de réaliser des signatures ou d'échanger des clés. La cryptographie basée sur les courbes elliptiques utilise d'autres algorithmes pour réaliser ces tâches.

Par exemple :

- ECDH : Elliptic Curve Diffie-Hellman pour l'échange de clé. ECDH reprend le protocole DH initial en se basant sur le problème du logarithme discret.
- ECDSA : Elliptic Curve Digital Signature Algorithm pour réaliser des signatures. ECDSA permet de réaliser ces actions en ajoutant le support des courbes elliptiques à l'algorithme DSA.
- ECIES : Elliptic Curve Integrated Encryption Scheme permet de chiffrer des données. C'est un système hybride qui permet de réaliser des actions de chiffrement avec plusieurs mécanismes basés sur les courbes elliptiques.

L'utilisation d'algorithme externe rajoute une couche de complexité à l'environnement ECC, notamment sur son implémentation. Il est très compliqué d'implémenter correctement ces différentes méthodes, la problématique est exactement la même qu'avec RSA, bien qu'encore plus complexe. Cela se traduit par de nombreuses attaques sur la cryptographie basée sur les courbes elliptiques. La dernière notable est la possibilité d'usurper une autorité de

certification reconnue au sein des systèmes Microsoft[22]. La vulnérabilité permettait de générer des certificats qui étaient reconnus par les systèmes d'exploitations Windows, et donc de réaliser des abus de confiance, que ça soit au niveau Web en utilisant un certificat SSL ou avec une application en usurpant la signature de l'autorité.

Un autre débat, très important pour les mathématiciens et les chercheurs, est le choix des courbes. En effet, il existe un grand nombre de courbes, elles sont adaptées en fonction des besoins et des algorithmes qui vont les utiliser. Plusieurs grands groupes ou entités proposent leurs propres courbes comme le NIST ou encore la NSA. Nous ajoutons donc à toutes les problématiques existantes, la notion de confiance. Il est impératif d'avoir confiance en l'entité qui fourni la courbe qui va être utilisée dans tel ou tel programme ou application.

Voici une liste non exhaustive des principales courbes elliptiques et de leurs utilisations associées :

- Curve25519, créée par Daniel J. Bernstein, un mathématicien américain. Elle est utilisée essentiellement pour l'échange de clé Diffie-Hellman basé sur les courbes elliptiques.
- Ed25519, issue de la suite précédente, mais adaptée pour la signature avec ECDSA.
- NIST-P-256, NIST-P-384, publiées en 2005 par la NSA dans le cadre de « Suite B ». Cette suite est formée de plusieurs algorithmes cryptographiques validés par le NIST dans le cadre des échanges d'informations internes ou externes du gouvernement des États-Unis. Elles peuvent être utilisées avec les algorithmes ECDH et ECDSA.
- FRP256v1, publiée en octobre 2011 au journal officiel est une suite française préconisée et créée l'ANSSI.

Bien que complexe, l'utilisation de cette technologie est démocratisée dans certains domaines, notamment celui de la blockchain. Le Bitcoin utilise par exemple des courbes elliptiques et plus précisément la courbe secp256k1. Cette technologie est connue pour être l'avenir de la cryptographie asymétrique, elle est également présente dans plusieurs logiciels ou protocoles tel que OpenSSH et

22 Référence : CVE-2020-0601

TLS. Dans la dernière version de TLS, les suites de chiffrement sont principalement basées sur ce système.

Bien qu'il soit vieux de plus de trente ans, ce système peine à être massivement utilisé, cela est dû au fait qu'il a été protégé durant de longues années par des brevets détenus par des sociétés privées.

8.2.2 AES

AES ou Advanced Encryption Standard est déjà utilisé en parallèle de 3DES. Les standards et les protocoles du groupe EMV ont été modifiés pour permettre son utilisation. Il se veut plus rapide et plus sécurisé que 3DES avec des tailles de clé similaires. AES est à peu près trois fois plus rapide que 3DES, il est donc similaire à DES dans sa version la plus simple au niveau de la rapidité, vu que 3DES est trois fois plus lent que DES.

AES est un algorithme de chiffrement par bloc lancé en 2000 par le NIST, il est notamment reconnu et utilisé par les différents états à travers le monde. Il est approuvé par la NSA à travers la publication de sa suite B et est aujourd'hui l'algorithme symétrique le plus sûr et le plus répandu. Il est également le remplaçant officiel de 3DES.

Cet algorithme utilise exclusivement des blocs de 128 bits et son fonctionnement est basé sur des tours, c'est-à-dire que l'algorithme répète plusieurs fois les mêmes actions pour chiffrer le message. Le nombre de tour est très important car ce dernier assure la sécurité de l'algorithme.

Plusieurs tailles de clés sont disponibles pour cet algorithme, ces tailles ont un impact sur le nombre de tours qui seront effectués par l'algorithme :

- AES-128 : 10 tours
- AES-192 : 12 tours
- AES-256 : 14 tours

Plus techniquement, ces tours correspondent à des calculs mathématiques basés principalement sur de la permutation, des matrices et des opérations « xor » avec des clés dérivées de la clé « maître ».

Pour expliquer simplement son fonctionnement, l'algorithme découpe les données en blocs de 128 bits soit 16 octets. Ces derniers sont permutés selon la table définie dans l'algorithme et sont placés dans une matrice de 4×4

éléments, soit 1 octet par case. Les lignes subissent ensuite une rotation vers la droite et les colonnes sont mélangés selon des règles strictes.

Des clés sont dérivées de la clé maître, une clé pour chaque tour. Elles servent à réaliser des opérations « xor » entre la matrice issue des opérations précédentes et la matrice correspondant à une des clés dérivées.

Les opérations sont répétées autant de fois qu'il y a de tour, 10 fois pour AES-128 par exemple. Sauf pour le dernier tour, le dixième pour AES-128, qui n'effectue pas le mélange des colonnes.

Chaque bloc de 16 octets est traité dix fois pour être chiffré. Pour déchiffrer, les opérations sont les mêmes mais dans le sens inverse.

Voici un schéma qui vous permettra de mieux appréhender le fonctionnement de cet algorithme :

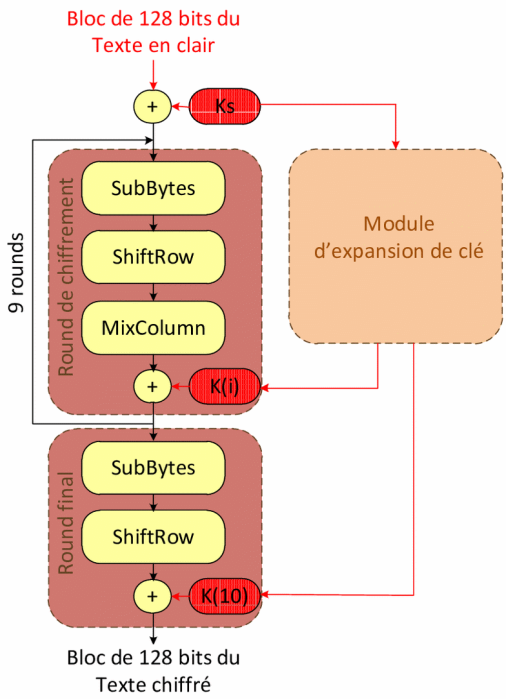


Figure 17: Source : researchgate.net. Illustration du chiffrement d'un bloc avec AES-128

L'opération « SubBytes » correspond au découpage du bloc, « ShiftRow » au décalage par ligne et « MixColumn » au mélange des colonnes.

Dans le système monétique actuel, la version utilisée est AES-128 bits en remplacement de 3DES. Cette version est aujourd'hui cryptographiquement sûre, il n'existe aujourd'hui aucune attaque pratique qui remette en cause la confiance

accordée à AES-128. Les clés de 256 bits sont cependant conseillées par le NIST et l'ANSSI bien qu'AES-128 soit toujours reconnu comme une alternative acceptable.

Plusieurs attaques ont été présentées sur les différentes versions d'AES mais elles comportent à chaque fois les mêmes techniques, c'est-à-dire la réduction du nombre de tours. AES-128 est « cassé » à partir de sept tours par exemple, mais l'attaque n'est pas possible en un temps acceptable avec dix tours.

AES-128 est donc aujourd'hui utilisé comme algorithme de chiffrement symétrique au sein des cartes à puce EMV. Cependant son déploiement reste progressif, à terme il devrait remplacer totalement 3DES.

8.2.3 SHA-2 & SHA-256

Une amélioration abordée pour le standard EMV est le remplacement de l'algorithme SHA-1 qui est aujourd'hui officiellement vulnérable aux attaques par collision. Son remplaçant sera l'algorithme SHA-256 de la famille SHA-2.

SHA-2 est une famille de fonction de hachage, elle a été créée par la NSA en se basant en grande partie sur les fonctions SHA-1 et SHA-0. Par défaut, elle comprenait les fonctions SHA-256 et SHA-512, les algorithmes sont strictement similaires, seul la taille des mots diffère ainsi que la longueur des résultats ou hashs. D'autres algorithmes ont été ajoutés dans cette famille comme SHA-224 et SHA-384, ils ne sont que des versions tronquées de SHA-256 et SHA-512.

SHA-256 est aujourd'hui le remplaçant officiel de SHA-1. Il est la référence en termes de fonction de hachage et est reconnu par les plus grandes institutions comme le NIST ou l'ANSSI en France.

SHA-256 est basé en grande partie sur SHA-1, son fonctionnement a déjà été expliqué dans ce document. Ses caractéristiques sont cependant différentes, car le condensat ou hash est de 256 bits. Il peut gérer des messages jusqu'à 2^{64} bits en entrée, il travaille avec des blocs de 512 bits, des mots de 32 bits et il faut réaliser 2^{128} opérations avant de trouver une collision sur SHA-256 en utilisant le paradoxe des anniversaires, alors qu'il en faut seulement 2^{63} pour SHA-1.

Le nombre de tour avec les différentes opérations mathématiques est également plus grand sur SHA-256, il est de 64 tours, contre 80 pour SHA-1.

C’est aujourd’hui l’algorithme choisi pour remplacer SHA-1 dans la plupart des cas et notamment dans le cadre de la monétique.

8.2.4 SSL/TLS

L’évolution de la sécurité des paiements par carte passe obligatoirement par une meilleure implémentation des protocoles TLS.

Pour la France l’autorité de certification Paycert, rattachée au GIE CB, délivrait toujours des certificats SHA-1 aux processeurs de paiement. Ces certificats étaient alors exposés et les différents TPE pouvaient se connecter à l’interface SSL/TLS rattachée, souvent avec des protocoles obsolètes comme SSLv3 ou TLS 1.0. Cependant, à partir de 2020 l’autorité ne délivrera plus de certificat signé en SHA-1, même en demandant une dérogation, ce qui obligera les commerçants à changer leurs parcs de TPE s’ils ne sont pas capables de gérer un autre protocole de hachage au niveau du certificat.

Le PCI DSS, avec les différents audits menés par les QSA, se veut plus strict sur l’application des standards, notamment l’interdiction d’utiliser les protocoles antérieurs à TLS 1.1. Ces points, jusqu’à maintenant essentiel pour les processeurs de paiement, seront bientôt bloquants pour les processeurs de paiement car ils ne se verront plus attribuer de certification PCI DSS en cas d’implémentation trop faible de TLS. Ils devront mener des actions conjointes avec leurs clients pour mettre à jour le parc de TPE et assurer un niveau de sécurité suffisant. TLS 1.0 et 1.1 seront bientôt rendus obsolètes par l’IETF[23], cela vient du fait que ces versions ne supportent que des algorithmes de hachages obsolètes comme SHA-1 et MD5.

Plus généralement, les configurations TLS se durcissent et les principaux navigateurs ont prévu de ne plus supporter les algorithmes inférieurs à TLS 1.2. Cela permet l’utilisation globale de TLS 1.2 et force les différents acteurs à mettre en place TLS 1.3, qui est aujourd’hui le plus avancé en termes de sécurité informatique et est recommandé par des agences comme l’ANSSI.

8.2.4.1 TLS 1.3

TLS 1.3 comporte des évolutions majeures, jusqu’ici jamais expérimentées. Elle permet d’utiliser exclusivement des algorithmes conformes à l’état de l’art. Les

23 Internet Engineering Task Force est un organisme qui promut et élabore des standards pour Internet.

autres versions de TLS, et même TLS 1.2, restent complexes à mettre en œuvre, car la configuration permet d'utiliser des algorithmes obsolètes et non sûrs.

Plus concrètement, TLS 1.3 ne permet pas d'utiliser des algorithmes obsolètes. Il est impossible d'utiliser SHA-1, MD5 ou encore DES. C'est d'ailleurs cette particularité qui fait qu'il est si peu utilisé aujourd'hui car beaucoup de clients ne permettent pas d'utiliser ce protocole.

En dehors de l'aspect sécuritaire, TLS 1.3 se veut 30 % plus rapide que ses prédécesseurs, cela est possible grâce à une simplification des échanges. Voici une illustration qui permet de visualiser les différences. Sur l'illustration ci-dessous, les échanges en rouge représentent les échanges en clair.

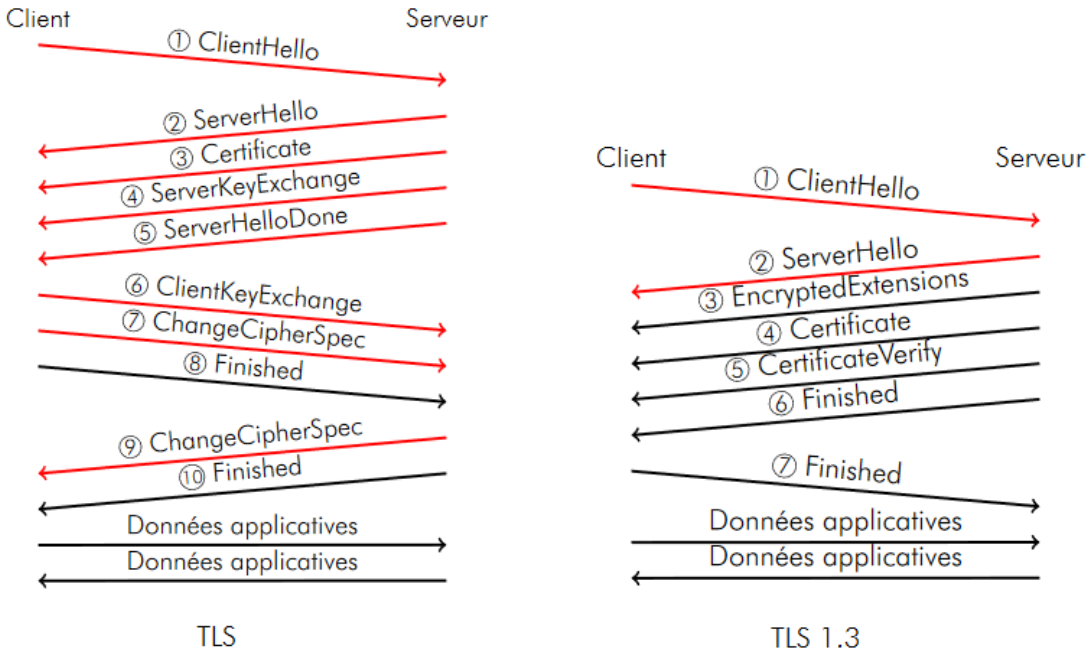


Figure 18. Source : www.ssi.gouv.fr. Illustration de sessions TLS. TLS inférieur à 1.3 (gauche) et TLS 1.3 (droite)

Il comporte donc trois étapes de moins que les autres versions d'SSL/TLS. Voici le détail de ces échanges.

Le client commence par envoyer une requête « ClientHello ». Cette dernière contient des informations comme les suites cryptographiques qu'il peut prendre en charge ainsi que les extensions. Le client peut également ajouter certains paramètres relatifs aux courbes elliptiques qu'il peut gérer.

Le serveur renvoi ensuite un message « ServerHello » qui contient la suite retenue par le serveur ainsi que les extensions sélectionnées pour l'échange de clé.

Ensuite un message « EncryptedExtensions » contient les extensions qui ne sont pas en rapport avec l'échange de clé.

Le certificat du serveur est envoyé également avec la requête « Certificate ». Cette dernière contient principalement la clé publique.

Pour terminer le serveur, à travers le message « CertificateVerify », transmet des données signées avec sa clé privée pour prouver l'authenticité du certificat.

Le serveur et le client s'envoient mutuellement des messages « Finished » signifiant que la négociation TLS est terminée et les échanges chiffrés peuvent commencer.

Cette version de TLS nécessite un échange aller-retour en moins que les précédentes pour la négociation. Cela permet au client de transmettre des données dès le troisième paquet envoyé, ce qui rend le système plus rapide.

Les échanges ont été réduits grâce à la suppression et à la mutualisation des différentes phases. Les messages de signalisation « ChangeCipherSpec » et « ServerHelloDone » sont supprimés, tout comme les messages « KeyExchange » utilisés pour échanger les valeurs Diffie-Hellman. Les données relatives à Diffie-Hellman sont maintenant échangées dans les messages « ClientHello » et « ServerHello ». Cela permet de chiffrer les échanges plus tôt, car les valeurs sont envoyées dès les premiers échanges. Le premier message chiffré de l'échange est « EncryptedExtensions ».

La phase d'authentification du serveur est faite avec les messages relatifs au certificat. Le dernier message contient une signature du condensat des messages échangés au préalable. Contrairement aux autres versions, cette phase est chiffrée.

Les suites cryptographiques utilisées dans TLS 1.3 sont formées de la même façon qye les autres versions. Elles sont cependant indépendantes, car elles ne peuvent pas utiliser les algorithmes supportés par TLS 1.2 par exemple. Les algorithmes utilisés sont pour beaucoup issus du chiffrement basé sur les courbes elliptiques pour la partie asymétrique. Pour le chiffrement symétrique AES et ChaCha sont utilisés. Pour terminer, au niveau des fonctions de hachages, la

famille SHA-1 est interdite et seule la famille SHA-2 est utilisable, c'est-à-dire SHA-2 256 ou SHA-2 384 par exemple. Il n'existe pas aujourd'hui d'implémentation de TLS 1.3 avec des algorithmes issus de la famille SHA-3, cela peut-être dû aux nouvelles découvertes sur l'algorithme Blake qui se veut, selon plusieurs chercheurs, plus performant et sécurisé.

8.3 L'évolution du matériel

Les évolutions de la monétique, plus précisément celles des protocoles et des services, ont également un impact sur le matériel utilisé qui se doit d'être conforme et compatible avec les améliorations amenées.

Les principaux équipements concernés par ces changements sont également les plus utilisés et les plus exposés comme les distributeurs automatiques de billets et les terminaux de paiement.

Les terminaux de paiement sont aujourd'hui le cœur de la monétique et les paiements réalisés par carte bancaire passent forcément par un de ces équipements. Les mesures prises par le groupe EMV, plus largement l'évolution de l'état de l'art de la sécurité informatique, pousse vers le remplacement de l'ensemble des terminaux obsolètes. Cela passe par exemple par la limite initiée par le GIE CB au niveau de l'utilisation des certificats SHA-1. Ces nouveaux terminaux proposés par des grands groupes comme Ingenico supportent désormais les derniers algorithmes et protocoles. Ils permettent d'avoir un niveau de sécurité correct au niveau des données traitées. Ces changements sont cependant lents, car il faut que les différents commerçants ou accepteurs se rapprochent de leurs banques acquéreuses ou de leurs fournisseurs pour s'équiper de nouveaux équipements.

Ce changement devrait devenir obligatoire dans les années à venir. Les entreprises qui proposent des services de paiements avec les différentes contraintes liées au PCI DSS, à EMV ainsi qu'au GIE CB en France ne seront plus capables de gérer les flux générer par les anciens TPE. Ce changement est conséquent pour les acteurs de la monétique, cela devrait enfin permettre la mise en place d'un système homogène et une sécurisation accrue au niveau des différents flux.

Un autre changement majeur dans le domaine des TPE est la facilité pour les accepteurs de s'en procurer. Il est aujourd'hui très facile d'acquérir un TPE, peu importe la taille de son entreprise. Ils ne sont plus seulement fournis par des

banques mais également par des entreprises privées ou des start-ups. Cette nouveauté permet une nouvelle fois d'accentuer la présence des paiements par carte et de renouveler le parc historique des TPE.

Un autre élément, rendant ce changement plus important et nécessaire, est la baisse d'utilisation de l'argent liquide par les différentes personnes, notamment en France. Cela induit forcément une hausse des paiements par carte bancaire. Les banques commencent progressivement à retirer les distributeurs automatiques de billets, ce qui va accroître de fait, ce changement. Pour donner des chiffres, la France a fermé en 2018 un millier de distributeurs automatiques et plus largement le nombre de ces équipements a reculé de 5 % en trois ans.

En dehors des évolutions liées à la consommation des Français, cela permet de réduire fortement l'exposition des équipements qui sont directement connectés aux réseaux des banques.

8.4 Les limites

Nous avons, à travers cette troisième partie, abordé les différentes évolutions prévues dans le système monétique sur le moyen terme mais des limites sont cependant présentes.

Aujourd'hui, les changements ne sont que théoriques au niveau des paiements par carte. Dans les sujets que nous avons étudiés, seul l'algorithme AES est réellement implémenté sur les systèmes actuels. SHA-1 est toujours largement utilisé, ce qui comporte des risques importants en termes de sécurité.

La multitude de problèmes abordée dans ce document fait que les changements à réaliser sont lents. Il faut les traiter sur le long terme car l'impact peut-être potentiellement désastreux.

Ce changement est accompagné par les nouveaux acteurs et les nouveaux moyens de paiement qui adoptent dès leur création un aspect sécuritaire important.

Une autre limite est l'exposition grandissante de ce système avec l'arrivée de ces mêmes acteurs. Jusqu'à maintenant, le système monétique était isolé et transitait essentiellement sur des réseaux gérés par les schemes, limitant l'exposition.

Aujourd'hui, avec la démocratisation des accès haut débit, la quasi-totalité de la population est en capacité de payer ou d'être payé. Ces facteurs sont facilités par l'arrivée de nouveaux acteurs, de nouveaux moyens de paiement et de nouveaux moyens d'acceptation pour les commerçants. Bien que cela soit une bonne chose au niveau commercial ainsi que pour l'expérience client, les flux sont en majorité envoyés vers Internet que ça soit via les réseaux fibres, cuivres ou mobiles. L'exposition et les risques sont donc beaucoup plus importants.

D'autres limites sont également observées et plus spécifiquement au niveau de la cryptographie. Les changements anticipés par le groupe EMV ne permettent pas de répondre à une menace grandissante : l'arrivée de l'informatique quantique.

9 Partie 4 : L'arrivée de l'informatique quantique

Dans cette dernière partie nous allons aborder un sujet majeur de la cryptographie de ces dernières années : l'informatique quantique et les ordinateurs quantiques. Ce sujet dépasse largement le système monétique car il pourrait impacter l'ensemble des communications réalisées aujourd'hui sur Internet.

Ce sujet est d'autant plus important qu'il est traité par les plus grandes entreprises technologiques comme IBM, Google ou encore Microsoft. La mise au point d'un ordinateur quantique suffisamment puissant pourrait remettre en cause l'ensemble des systèmes informatiques.

Le but de ce chapitre n'est pas de comprendre totalement le fonctionnement de l'informatique quantique ou de la physique quantique, car ce n'est tout simplement pas possible.

Il faudrait bien plus qu'un chapitre de mémoire pour traiter ce sujet vaste comme en témoigne les citations de Richard Feynman. Ce physicien américain, prix Nobel de physique en 1965 ayant travaillé une grande partie de sa carrière sur la physique quantique :

« Je pense pouvoir dire sans trop me tromper que personne ne comprend la mécanique quantique. » Richard Feynman

C'est un sujet ou il faut accepter de ne pas comprendre totalement les concepts car ils ne sont comparables à rien de ce qui est connu à l'heure actuelle et ne sont souvent pas applicables à des règles de mathématiques.

Le but de cette partie est d'appréhender le fonctionnement général de ces systèmes, les impacts que cela pourrait avoir sur l'informatique que nous connaissons aujourd'hui et indirectement sur la monétique et pour terminer les éventuelles solutions. L'impact le plus important qui sera abordé se situe au niveau de la cryptographie.

Ce sujet a volontairement été simplifié dans le présent rapport pour des raisons de compréhension et pour ne pas surcharger ce document.

9.1 Définitions

Avant tout, il est important de définir les différents termes relatifs à l'informatique quantique pour mieux comprendre ce sujet.

9.1.1 La physique et la mécanique quantique

La mécanique quantique intervient au moment où la physique classique ne suffit plus, c'est-à-dire dans l'infiniment petit. Contrairement à la physique classique, la mécanique quantique intervient au niveau des atomes et des particules subatomiques pour comprendre les particules de matières constituant les différents objets de l'univers.

La mécanique quantique est cependant remise en cause par une partie de la communauté scientifique et comporte d'énormes difficultés de compréhension.

Elle est le regroupement de l'ensemble des domaines de la physique ou les règles de la mécanique sont utilisées.

9.1.2 L'informatique quantique

L'informatique quantique est une autre branche de l'informatique traditionnel. Cette dernière est basée sur l'utilisation de calculateur quantique également appelé ordinateur quantique. Contrairement aux ordinateurs classiques, ils n'utilisent pas l'électricité et des transistors pour fonctionner. La technologie de ces calculateurs permet d'utiliser des propriétés de la physique quantique. Ils utilisent principalement la superposition et l'intrication quantique.

Ces ordinateurs permettent de manipuler des qubits qui peuvent être dans plusieurs états simultanément, 0 et 1 par exemple, contrairement à des simples bits qui peuvent être seulement à 0 ou 1.

9.1.3 La cryptographie quantique

La cryptographie quantique est l'utilisation des propriétés de la physique quantique pour établir des algorithmes cryptographiques, elle n'est donc plus basée sur des propriétés mathématiques. Elle est très différente de la cryptographie post-quantique qui sera abordée par la suite et ne doit pas être confondue avec cette dernière.

Elle permet d'atteindre des niveaux de sécurité plus important qu'avec les technologies non quantiques utilisées actuellement, notamment au niveau des

algorithmes d'échanges de clés. L'utilisation des propriétés de la physique quantique pourrait révolutionner ce système et permettre d'échanger facilement et de façon sécurisée des clés secrètes.

Cependant, elle reste limitée car elle ne permet pas de chiffrer concrètement des données. Elle se limite au niveau des échanges de clé, qui eux permettront de chiffrer ses données.

9.1.4 La cryptographie post-quantique

La cryptographie post-quantique est une section particulière de la cryptographie classique. Son but est de garantir la sécurité de l'information face à des attaquants utilisant un calculateur quantique ou ordinateur quantique.

Elle reste donc basée sur des propriétés mathématiques comme la cryptographie actuelle mais les algorithmes sont différents, car ils ne doivent pas être basés sur les mêmes problèmes mathématiques.

9.2 Pourquoi l'informatique quantique

L'informatique quantique pourrait révolutionner l'informatique actuel par sa puissance de calcul. Il peut résoudre des problèmes que nos ordinateurs ne savent pas résoudre et qu'ils ne seront peut-être jamais capables de résoudre. Il s'agit principalement des problèmes exponentiels, ou la quantité de données à traiter fait augmenter exponentiellement la difficulté du problème à résoudre.

Cette théorie n'est pas nouvelle. Dans les années 90, des chercheurs avaient déjà démontré que l'utilisation d'une machine de ce type pouvait calculer beaucoup plus rapidement.

Nous pouvons prendre par exemple la création d'un itinéraire entre deux positions géographiques. Plus nous éloignons le point de départ de l'arrivée, plus les données à prendre en compte sont importantes. Il faut analyser les différentes routes, les travaux, les embouteillages, etc.

Ces ordinateurs pourront, pour certains problèmes, dépasser les plus puissants supercalculateurs qui sont utilisés aujourd'hui. Pour illustrer ces propos nous pouvons imaginer des problèmes très complexes pour nos ordinateurs classiques. Ces problèmes pourraient prendre des millions d'années pour être résolus, voir même dépasser l'âge de l'univers et cela même avec l'ensemble des supercalculateurs.

Alors que les ordinateurs quantiques pourraient, en théorie, ramener la résolution de ces problèmes à l'échelle d'une vie humaine, en mois ou en années.

Cela est possible car la façon de calculer d'un ordinateur quantique est différente de ce qui était fait jusqu'à présent. Il est capable, grâce à des principes comme l'intrication et la superposition, de calculer l'ensemble des résultats possibles en une seule opération contrairement aux ordinateurs actuels.

L'informatique quantique ne permettrait pas juste d'aller plus vite, mais de traiter des problèmes qui sont impossibles à résoudre avec les technologies actuelles. Elles arrivent à leurs limites en termes d'évolution même en prenant en compte les évolutions perpétuelles de la loi de Moore.

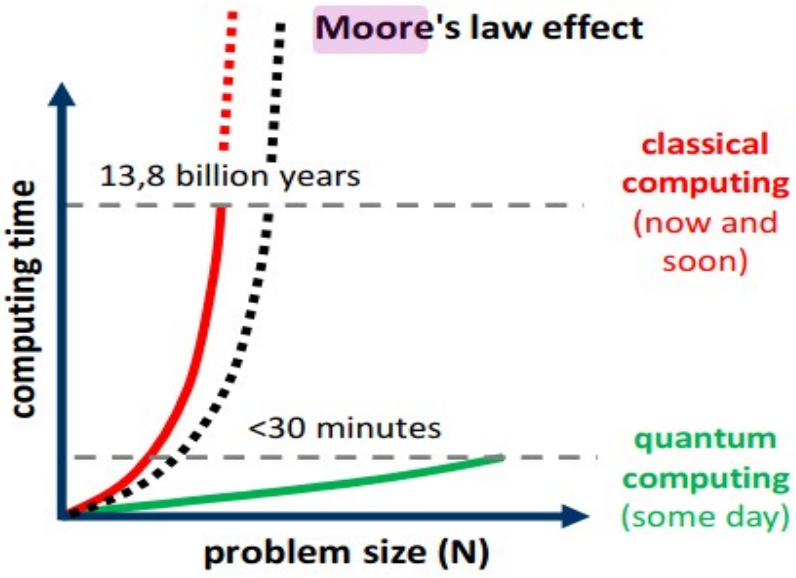


Figure 19. Source :www.oezratty.net. Graphique de la loi de Moore illustrant la différence de traitement en temps de l'informatique quantique et l'informatique actuel selon la taille d'un problème

Un grand nombre d'applications sont possibles pour cette technologie, dans la science, la finance ou encore la santé. Tous les domaines ou les systèmes actuels peines à traiter les données de façon efficace.

Plus concrètement, il serait possible de factoriser n'importe quel nombre entier en utilisant un calculateur quantique suffisamment puissant avec l'algorithme de Schor. Pour réaliser ces calculs les ordinateurs quantiques sont basés sur des

qubits. Ces éléments utilisent eux-mêmes des principes quantiques comme la superposition d'états ou l'intrication. Ces éléments seront traités dans la partie suivante.

Toutes les raisons évoquées font que l'intérêt envers cette technologie ne cesse d'augmenter. Notamment au niveau des géants de l'informatique comme Google et IBM qui investissent des sommes colossales pour développer un ordinateur quantique fonctionnel et suffisamment puissant.

L'ensemble des éléments sont à prendre au conditionnel car aujourd'hui l'ordinateur quantique n'est toujours pas utilisable, de nombreuses contraintes et limites sont présentes dans ce système. Elles seront également abordées dans les points suivants.

9.3 Les grands principes

Pour essayer de comprendre le fonctionnement des calculateurs quantiques, il est important d'aborder les principaux principes qui sont l'intrication, la superposition et l'utilisation des qubits.

9.3.1 La superposition

Un calculateur quantique utilise des lois issues de la mécanique quantique pour fonctionner. Une de ces lois permet à une particule, un photon ou une molécule de se trouver dans différents états et cela en même temps. Les états sont dits « superposés ».

Plus précisément, l'état est indéterminé et rien ne permet de le déterminer avant la mesure comme la position d'une particule. Elle ne se situe pas à un point A ou à un point B car il y a une infinité de possibilités au niveau de sa localisation. Il faut obligatoirement réaliser une mesure pour connaître l'état de cette particule, mais une fois mesurer, l'état quantique de la particule n'est plus car nous avons pu voir si elle était au point A ou bien au B. Nous pouvons dire qu'avant la mesure la particule était au point A et au point B par superposition.

Pour schématiser cette explication, nous pouvons reprendre la très célèbre expérience du chat de Schrödinger. Il faut également savoir qu'il est très compliqué de démontrer les principes de la physique quantique car rien n'est comparable. Cette problématique donne lieu à des explications de ce type.

Cette expérience, pensée par Erwin Schrödinger, a pour but de présenter la superposition quantique, tout en mettant en avant le problème lié aux mesures et à la complexité d'expliquer les différents principes.

L'expérience est simple. Vous enfermez un chat dans une boite avec un système qui tue le chat avec du poison en cas de détection d'un élément particulier comme la désintégration d'un atome. L'atome est donc dans un état superposé, intact et désintégré à la fois. Cet état se répercute directement sur le chat, qui se retrouve également dans les deux états, mort et vivant.

Il est impossible de savoir si l'atome est intact, et donc que le chat est vivant sans faire de mesure. Il y a juste des probabilités, tant pour que le chat soit vivant, tant pour qu'il soit mort.

Pour illustrer la superposition, il est aussi possible de dire que l'état change très rapidement. Même si ce n'est pas exact au sens de la physique, c'est une façon d'aborder ce point très particulier.

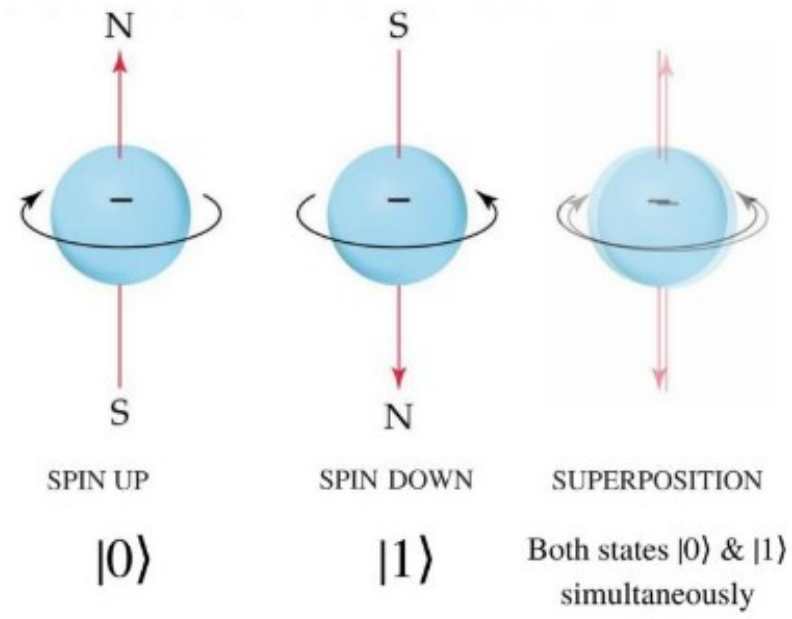


Figure 20. Source :www.oezratty.net. Illustration de la superposition quantique.

Ce principe est un des plus importants de la physique quantique et plus précisément des calculateurs. C'est l'utilisation de ces états superposés avec les qubits qui permet à ces ordinateurs d'avoir une telle puissance de calcul.

9.3.2 L'intrication

L'intrication est également essentielle à la compréhension de ces calculateurs. Cette propriété permet, grâce à des propriétés quantiques, de lier deux particules indépendantes. C'est-à-dire qu'il est possible de forcer l'état d'un objet quantique lorsque l'on en mesure un autre, ces objets sont donc intriqués.

Plus précisément, si l'on prend deux particules, séparées et indépendantes l'une de l'autre et que l'on modifie l'état d'une de ces particules, l'état de l'autre sera automatiquement modifié, et cela très rapidement, presque instantanément.

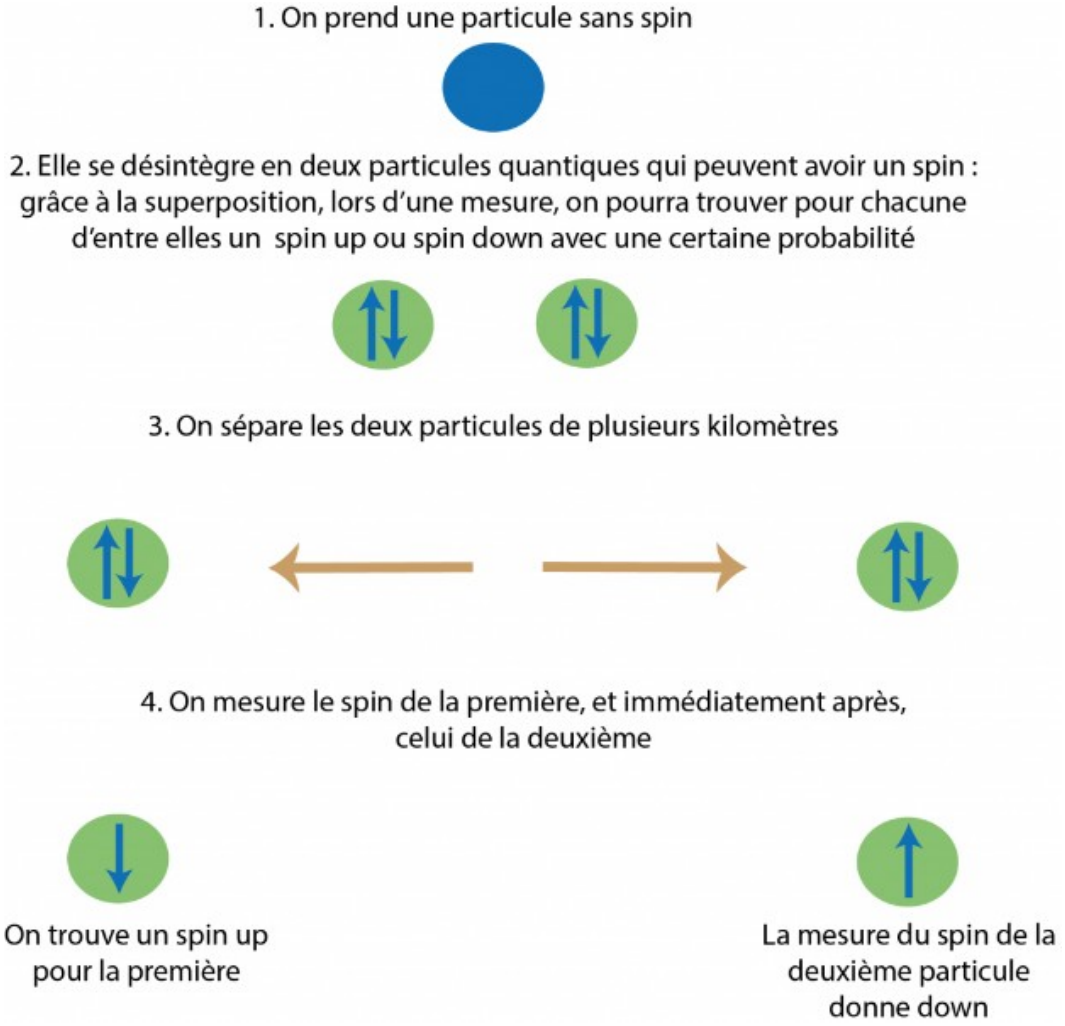


Figure 21. Source : www.institut-pandore.com. Illustration de l'intrication de deux particules.

Cette propriété correspond à l'intrication, elle peut s'illustrer de la façon suivante. Nous prenons deux ampoules dans deux maisons différentes. Deux états sont possibles pour chaque ampoule, allumée ou éteinte. Il serait alors possible de déterminer l'état de la seconde en observant la première. Si la première ampoule est éteinte, alors la deuxième est allumée, et si la première est allumée, la deuxième s'éteint automatiquement.

Si nous revenons au niveau des particules, elles sont généralement liées par un évènement et c'est la mesure qui a un impact sur les états. Cela peut se faire à des kilomètres, grâce au principe quantique de non localité. Les deux particules, même distantes, font partie intégrante du même système physique. Aucune donnée n'est donc échangée pour le changement d'état.

Ce système a été prouvé dès l'année 1982 par Alain Aspect lors d'une de ses expériences. Ce système permet donc de lier des objets quantiques entre eux. Cette fonctionnalité est utilisée dans l'informatique quantique pour lier les qubits entre eux conjointement à la superposition.

9.3.3 Les qubits

La présentation de la superposition et de l'intrication nous amène à l'élément principal des calculateurs quantiques : les qubits ou les bits quantiques. Ils sont la base de l'informatique quantique, comme les bits classiques pour l'informatique traditionnel.

Les qubits, grâce à la superposition, peuvent être dans deux états à la fois, c'est-à-dire 1 et 0 car même dans l'informatique quantique le binaire est utilisé. L'état 0 ou 1 n'est retrouvé que lors de la mesure du qubit, mais la mesure n'est pas l'élément le plus important. La véritable valeur du qubit est utilisée lors des différents calculs.

Ces qubits sont utilisés à travers des portes quantiques qui sont l'équivalent des portes logiques pour des bits classiques. Ces portes peuvent utiliser un ou deux qubits permettant de réaliser les différents calculs d'un ordinateur quantique et de modifier l'état de ces qubits. Il en existe des différentes et certaines peuvent être réversibles contrairement aux portes logiques classiques.

L'utilisation des propriétés quantiques et des qubits font que l'ordinateur quantique est sensiblement plus rapide. Pour donner un exemple un ordinateur utilisant quatre qubits est seize fois plus rapides qu'un ordinateur classique à

quatre bits. La capacité double à chaque ajout de qubit sur l'ordinateur, ce qui n'est pas le cas des ordinateurs utilisant des bits.

Des algorithmes quantiques sont également disponibles pour effectuer des calculs sur ces machines. Ils fonctionnent sur le même principe que les algorithmes classiques, leurs particularités sont qu'ils utilisent spécifiquement des caractéristiques de l'informatique quantique comme l'intrication ou la superposition.

Parmi les plus connus nous avons l'algorithme de Shor qui permet de factoriser des nombres, ou encore l'algorithme de Grover qui permet de rechercher des éléments dans une liste.

Il faut également faire la différence entre les qubits logiques et physiques. Les premiers sont ceux utilisés sur des ordinateurs classiques, par exemple émulé par des processeurs utilisant des bits. Les seconds sont des qubits au sens physique du terme, c'est-à-dire la réelle implémentation d'un qubit sur un calculateur quantique.

9.4 L'impact de l'informatique quantique

L'arrivée des calculateurs quantiques peut avoir des impacts importants sur l'informatique, sur notre façon de communiquer et être particulièrement destructeurs au niveau de la cryptographie.

9.4.1 Sur la cryptographie

Déjà abordé dans ce document, l'ensemble des méthodes et des algorithmes cryptographiques utilisés aujourd'hui pour chiffrer nos communications sont basés sur des principes mathématiques. Leurs particularités sont que les problèmes utilisés sont extrêmement compliqués pour nos ordinateurs classiques. Ces problèmes, principalement basés sur le logarithme et sur la factorisation, ne peuvent pas être résolus à l'échelle d'une vie humaine à la condition que les clés soient suffisamment grandes.

Cependant, l'arrivée de l'informatique quantique pourrait remettre en cause une grande partie du système cryptographique actuel et pas seulement dans le monde de la monétique.

L'algorithme de Shor, nommé en l'honneur de son créateur Peter Shor, permettrait, s'il était implémenté sur un calculateur quantique suffisamment

puissant, de factoriser un nombre N en un temps qui serait exponentiellement plus rapide qu'avec des supercalculateurs. Il serait alors possible de retrouver les clés privées des différentes biclés RSA en un temps qui sera acceptable à l'échelle d'une vie humaine.

L'utilisation de cet algorithme pourrait remettre en cause l'ensemble du système bancaire actuel, tout comme la quasi-totalité des échanges chiffrés de la planète.

Cet algorithme n'épargne pas non plus la cryptographie basée sur les courbes elliptiques, car il est capable de calculer des logarithmes discrets et de remettre en question la confidentialité et l'intégrité des données. Ce type de cryptographie est d'ailleurs une cible plus facile pour cet algorithme car il nécessitera un nombre de qubits et de portes logiques inférieurs à la cryptographie basée sur RSA.

Avec un seul algorithme il est donc possible de rendre inutilisable les deux plus grands systèmes de cryptographie asymétrique.

Les systèmes symétriques sont également vulnérables aux attaques des ordinateurs quantiques. L'algorithme utilisé est celui de Grover découvert par Lov Grover. Ce dernier est un algorithme de recherche basé sur des qubits et des systèmes de boites noires. Il est capable de rechercher très rapidement des données grâce à un système de comparaison et cela même si la liste est énorme. Il permet dans la finalité de rendre la recherche de clé secrète plus rapide, mais cette fois-ci sans remettre en cause l'ensemble du système. Selon les différents experts, il suffirait de doubler le taille des clés qui sont utilisés actuellement pour limiter l'impact. Les fonctions de hachages sont également vulnérables à l'algorithme de Grover mais le constat est le même, il suffit d'augmenter les tailles de « clé » pour les rendre sûres.

Les calculateurs quantiques sont pour l'instant capables de rendre obsolète les systèmes asymétriques mais pas les symétriques.

Pour la cryptographie, les fonctionnalités offertes par l'informatique quantique ne se limitent pas aux attaques sur les différents systèmes. L'arrivée de cette technologie pourrait également révolutionner le fonctionnement des échanges de clé, un point majeur en termes de cryptographie.

La distribution de clé quantique ou QKD[24] en anglais regroupe un ensemble d'algorithmes et de fonctionnalités permettant d'échanger des clés, c'est-à-dire un protocole cryptographique permettant de partager des clés secrètes entre deux parties. La particularité de ces algorithmes est qu'ils utilisent des propriétés de la physique quantique pour échanger les informations de manière sécurisée et non pas des mathématiques. La sécurité des échanges est assurée par plusieurs principes en fonction des différents protocoles, comme le théorème de non clonage qui rend impossible la reproduction des données par un attaquant ou encore l'intrication quantique.

La QKD peut théoriquement remplacer l'utilisation des protocoles RSA ou DH au niveau de l'échange des clés. Il faudra toujours s'assurer au préalable que les deux parties sont authentifiées. L'intérêt principal de cette technologie est d'offrir un nouveau moyen d'échanger des clés en dehors des systèmes mathématiques, ce qui permettrait de rendre ce système invulnérable aux attaques mathématiques.

9.4.2 Sur l'informatique

En dehors de l'aspect destructeur au niveau de la cryptographie, l'arrivée des calculateurs quantiques permettrait d'améliorer sensiblement plusieurs domaines.

Grâce aux différences fondamentales de ces machines, il sera possible de trouver des réponses à des questions qui sont pour l'instant restées sans réponses avec nos ordinateurs classiques. Les différents domaines de la science pourront tirer profit de cette technologie.

Au niveau de l'informatique comme nous le connaissons aujourd'hui, l'impact sera minime. L'utilisation de ces machines se fera en complément des serveurs que nous utilisons. Bien que les ordinateurs classiques ne soient pas capables de réaliser les calculs d'un ordinateur quantique, la même chose est vraie dans le sens inverse. Les calculateurs quantiques ne sont pas capables d'effectuer les opérations faites aujourd'hui avec des ordinateurs classiques.

Vous n'aurez sans doutes jamais d'ordinateur quantique chez vous car ils comportent un grand nombre de limites et de contraintes qui seront expliquées dans la prochaine partie.

24 Quantum Key Distribution

De plus, les calculateurs quantiques sont considérés comme des modules externes pour nos ordinateurs. Il est donc nécessaire d'utiliser un ordinateur classique pour le contrôler.

9.5 Les limites

La mise en place et la création de systèmes informatiques basées sur des propriétés quantiques comportent un grand nombre de contraintes.

Les grands noms de l'informatique développent des ordinateurs ou des simulateurs quantiques et sont confrontés à des problèmes dès la conception.

Une des problématiques est que pour fonctionner, les ordinateurs quantiques actuels ont besoin de températures très basses. Cela est nécessaire pour que les qubits puissent garder leur état quantique et éviter les erreurs. Pour donner un exemple, la température des qubits doit être proche du zéro absolu[25] soit −273 °C.

Cette température rend l'utilisation et l'installation de ces machines complexes et coûteuses, c'est pour cela qu'il sera probablement impossible d'avoir un jour des ordinateurs quantiques personnels.

Cela nous amène à la seconde limite, qui est de garder notre qubit dans un état quantique car c'est seulement dans cet état-là qu'il est utile pour réaliser des calculs complexes. Il est très difficile de manipuler ces qubits sans les détruire totalement et donc les faire devenir des simples bits. Le prix Nobel de physique 2012 à d'ailleurs été donné à des chercheurs[26] ayant réussi a mesuré des qubits sans altérer leur état.

Comme pour les processeurs avec une architecture classique qui utilisent des bits et portes logiques, les processeurs quantiques utilisent des qubits et des portes quantiques. Pour réaliser des calculs importants, il faut pouvoir utiliser un grand nombre de qubits et de portes quantiques, ce qui est impossible actuellement.

Les entreprises les plus importantes du domaine comme IBM, Google ou encore DWave arrivent à créer des ordinateurs avec plus ou moins 53 qubits, ce qui n'est pas encore suffisant pour dépasser les supercalculateurs actuels.

25 Température la plus basse qui puisse exister.
26 David Wineland et Serge Haroche

Cependant le nombre de qubits et de portes quantiques ne suffit pas. Un facteur essentiel est le pourcentage d'erreur lié à la manipulation des qubits, c'est le problème le plus important lors de la création d'un ordinateur quantique.

Aujourd'hui, il est de plus ou moins 0,5 % soit une erreur toutes les deux cents manipulations. Pour que cela soit efficient, il faudrait que le taux d'erreur soit de 0,01 % voire 0,0001 %. Cela est évalué au niveau de la stabilité de deux qubits avec une porte quantique. La méthode est différente selon les entreprises, certaines préfèrent augmenter le nombre de qubit alors que d'autres préfèrent améliorer le taux d'erreur avec un nombre de qubit moins important.

Pour limiter ces problèmes, plusieurs qubits physiques sont utilisés pour former un qubit logique. Cela permet de réduire les problèmes en utilisant de la redondance.

Pour revenir à la cryptographie asymétrique, pour une clé de 1024 bits RSA il faudrait par exemple 166 millions de qubits physiques avec un taux d'erreur à 0,1 % et plus ou moins 7 semaines de calcul. Il est possible de descendre à 5,5 millions de qubits physiques mais le taux d'erreur doit être de 0,01 %.

Des employés de Google ont cependant publié un algorithme pour factoriser des clés de 2048 bits plus rapidement. Il faut tout de même 2,3 millions de qubits physiques avec un taux de 0,1 % pour un calcul réalisé en moins de 10 heures.

Bien qu'inférieur, les résultats sont sensiblement les mêmes. En utilisant des clés de 256 bits il faudrait à peu près 2330 qubits logiques, il faut multiplier ce chiffre de 200 à 20 000 pour avoir le résultat en qubits physiques selon le taux d'erreur et les conditions.

Ces chiffres sont bien loin des performances actuelles de ces calculateurs. Selon certains experts du domaine, des ordinateurs quantiques assez puissant pourraient arriver d'ici une quinzaine d'années. D'autres sont moins optimistes et pensent que cela soit impossible à l'échelle de notre vie.

Dans tous les cas, l'informatique quantique est une réelle menace pour la cryptographie que nous connaissons. Les plus grandes entreprises et groupes du monde entier se sont donc mis depuis plusieurs années à chercher des algorithmes et des techniques post-quantique pour mieux appréhender ce phénomène.

9.6 Les solutions

Il existe des solutions pour contrer l'arrivée de l'informatique quantique au niveau de la cryptographie. Elles peuvent être très simples comme doubler la taille des clés pour les algorithmes symétriques ou encore utiliser des algorithmes de hachage plus fort comme SHA-3.

Pour le chiffrement asymétrique plusieurs groupes ont déjà abordés le sujet comme Atos Wordline et EMV pour la monétique. Ils travaillent en collaboration avec des universitaires et des organismes comme le NIST pour trouver des solutions et développer des solutions post-quantiques.

L'ANSSI admet également qu'il est nécessaire de développer des solutions cryptographiques post-quantiques, preuve que la menace est grandissante. La NSA, de son côté, a appelé en 2015 les administrations à anticiper cette bascule.

À ce jour plusieurs algorithmes asymétriques ont été développés mais aucun n'est encore reconnu par les différentes instances. Le NIST a pour cela lancé un concours en 2017 pour sélectionner les nouveaux standards en la matière.

Sur les soixante-neuf propositions acceptées par l'institut, vingt-six ont été retenues pour être étudiées plus profondément. Les protocoles analysés permettent soit la signature numérique, soit l'échange de clé.

Tous les éléments sont repris et traités par une communauté mondiale d'experts et de cryptographes, les résultats de ce concours ne sont pas attendus avant au moins l'année 2022.

Pour ces algorithmes, il a fallu trouver des nouveaux problèmes mathématiques que l'informatique quantique ne pourrait pas résoudre. Ils peuvent être basés sur les réseaux euclidiens ou encore les graphes d'isogénies.

La monétique, plus précisément avec EMV, essai d'anticiper ces problématiques avec le développement d'applications sur mesure. Une solution pour les cartes, qui ne sont pas agiles au niveau de la cryptographie est le remplacement du système par Global Plaform[27]. Cette solution applicative se positionne au niveau des cartes à puce, elle pourrait permettre à EMV de faire évoluer fortement ses cartes et leur niveau de sécurité et de les rendre résistantes.

27 GP : Global Platform, solution applicative Java pour administrer un parc de carte à puce https://globalplatform.org/

10 Conclusion & ouverture

Après avoir abordé les différents secteurs comme la monétique, la cryptographie, l'état de l'art, les évolutions possibles et finalement l'arrivée de l'informatique quantique nous pouvons conclure ce mémoire de fin d'études.

Aujourd'hui, nous avons démontré que les moyens cryptographiques mis en œuvre dans le système monétique ne sont pas suffisants pour diverses raisons. La cause principale est la conception de ce système qui à la base n'a pas été pensé pour évoluer. Il est monolithique et peu agile, causé d'une part par les systèmes physiques comme les cartes et les terminaux de paiement. D'autre part par les systèmes applicatifs qui ne sont pas capables de gérer les derniers protocoles et les contraintes opérationnelles.

Aujourd'hui, la plupart des algorithmes utilisés dans le secteur de la monétique et par les standards EMV sont dépréciés par les principales institutions.

Cependant, à l'heure actuelle aucune attaque contre ces systèmes n'est disponible mais cela devrait changer dans un futur proche, notamment avec les récents évènements liés à l'algorithme SHA-1 qui est toujours massivement utilisé. L'exposition des différents services avec l'arrivée des fintechs ainsi que l'utilisation des réseaux classiques[28] seront des facteurs importants. Ce secteur, critique et exposé à la fraude, sera une cible de choix pour des attaquants.

Au vu des limites rencontrées pour réaliser des simples changements au niveau des tailles de clés ou des algorithmes, il sera très compliqué d'anticiper l'arrivée de l'informatique quantique. Néanmoins, même si cette technologie n'arrivera peut-être jamais, il est important d'évoquer ce sujet et plus particulièrement pour un secteur comme la monétique.

28 Fibres, cuivres, mobiles.

11 Bibliographie

FRARY, Mark. Fous de codes secrets. 1ère édition. Paris : Flammarion, 2017. 192p. (SCIENCE POPULAI).

IVINZA LEPAPA, Alphonse. Monétique et Transactions électroniques. 1ère édition. Aix-en-Provence : Bookelis, 2018. 288p. (BO.MONDE VF).

PLATEAUX, Aude. Solutions opérationnelles d'une transaction électronique respectueuse de la vie privée [en ligne]. Thèse de Doctorat. Cryptographie et sécurité. Caen : Université de Caen, 2013. [Consulté le 24 Juin 2019]. 171p. Disponible à l'adresse : https://tel.archives-ouvertes.fr/tel-01009349/document

LEURENT Gaëtan, PEYRIN Thomas. From Collisions to Chosen-Prefix Collisions Application to Full SHA-1 [en ligne]. Rapport de recherche. France : INRIA, Singapour : Nayang Technological University, Temasek Laboratories. 06 Mai 2019. [Consultation le 03 Juin 2019]. 30p. Disponible à l'adresse : https://eprint.iacr.org/2019/459.pdf

SOLAT, Siamak. Security of Electronic Payment Systems : A Comprehensive Survey [en ligne]. Rapport de recherche. France : Sorbonne Universités, UPMP Unversity of Paris VI, CNRS. 12 Janvier 2017. [Consultation le 05 Juin 2019]. 29p. Disponible à l'adresse : https://arxiv.org/ftp/arxiv/papers/1701/1701.04556.pdf

ANSSI. Référentiel Général de Sécurité : Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques [en ligne]. Version 2.03. Paris : ANSSI, 2014. 63p. [Consulté le 12 Juillet 2019]. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

BARKER, Elaine, NIST. Recommandation for Key Management, Part 1 : General [en ligne]. Part 1 Revision 4. Gaithersburg : NIST, 2016. 160p. [Consulté le 13 Juillet 2019]. Disponible à l'adresse : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

EMVCo. EMV Integrated Circuit Card Specifications for Payment Systems : Book 2 Security and Key Management [en ligne]. Version 4.3. Purchase, Harrison : EMVCo, Novembre 2011, 162p. Disponible à l'adresse : https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

LEVILLAIN, Olivier. SSL/TLS, 3 ans plus tard. SSTIC [en ligne]. Conférence. 2015. [Consulté le 02 Juillet 2019]. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2015/06/SSTIC2015-Article-ssltls_soa_reloaded-levillain_cObDbqp.pdf

Kévin, Jérémy (noms non disponibles). Paymon.fr [en ligne]. (Créé en 2011, mis à jour le 21 Juin 2019). [Consulté le 6 mai 2019]. Disponible à l'adresse : https://paymon.fr

DUNJIC, Milos. The Current State Of EMV Cryptography. Financial IT Blog [en ligne]. 20 Novembre 2017. [Consulté le 18 Mai 2019]. Disponible à l'adresse : https://financialit.net/blog/current-state-emv-cryptography

EMVCo. A Guide to EMV Chip Technology [en ligne]. Version 2.0. [Consulté le 12 Juillet 2019]. Purchase, Harrison : EMVCo, 2014. 36p. Disponible à l'adresse : https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf

MIMOSO, Mike. SDA Protocol Payments Cards Remain a Target for Cybercriminals. Flashpoint Blog [en ligne]. 05 Mars 2018. [Consulté le 19 Mai 2019]. Disponible à l'adresse : https://www.flashpoint-intel.com/blog/sda-protocol-payment-cards-remain-target-cybercriminals/

CAPFI. Carte bancaire – Introduction fonctionnelle et technique à l'interbancarité. Capfi Blog [en ligne]. 13 Juin 2017. [Consulté le 23 Mai 2019]. Disponible à l'adresse : https://www.capfi.fr/blog/techno-digital/carte-bancaire-introduction-fonctionnelle-et-technique-linterbancarite

PEREZ, Ben. Seriously, stop using RSA. Trailofbits Blog [en ligne]. 08 Juillet 2019. [Consulté le 11 Juillet 2019]. Disponible à l'adresse : https://blog.trailofbits.com/2019/07/08/fuck-rsa/

MARTIN, Tania. Elliptic Curve Cryptography for dummies 1. Smals Research [en ligne]. 25 Février 2015. [Consulté le 15 avril 2020]. Disponible à l'adresse : http://www.smalsresearch.be/elliptic-curve-cryptography-tutoriel1/

MARTIN, Tania. Elliptic Curve Cryptography for dummies 2. Smals Research [en ligne]. 12 Août 2015. [Consulté le 16 avril 2020]. Disponible à l'adresse : http://www.smalsresearch.be/elliptic-curve-cryptography-tutoriel2/

Grayblock. Elliptic-Curve Cryptography. Medium [en ligne]. 29 Juin 2018. [Consulté le 30 Mars 2020]. Disponible à l'adresse : https://medium.com/coinmonks/elliptic-curve-cryptography-6de8fc748b8b

Cryptographie sur les courbes elliptiques. Wikipédia [en ligne]. 2020. [Consulté le 8 Avril 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Cryptographie_sur_les_courbes_elliptiques

GASPAR, Emilien. Standardisation des courbes elliptiques : à qui faire confiance ? MISC [en ligne]. Avril 2016. [Consulté le 10 avril 2020]. HS N°13. Disponible à l'adresse : https://connect.ed-diamond.com/MISC/MISCHS-013/Standardisation des-courbes-elliptiques-a-qui-faire-confiance

ANSSI. Recommandations de sécurité relatives à TLS [en ligne]. Version 1,2. Paris : ANSSI, 26/03/2020. 72p. [Consulté le 12 Avril 2020]. Disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

Planet Fintech. Cartographie 2020 des Fintech françaises. Planet-Fintech [en ligne]. 29 Janvier 2020. [Consulté le 25 mars 2020]. Disponible à l'adresse : https://www.planet-fintech.com/Cartographie-2020-des-Fintech-francaises_a1300.html

Advanced Standard Encryption. Wikipédia [en ligne]. 2020. [Consulté le 20 Avril 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

SHA-2. Wikipédia [en ligne]. 2020. [Consulté le 3 Mai 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/SHA-2

Cryptographie Quantique. Wikipédia [en ligne]. 2020. [Consulté le 15 Mai 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Cryptographie_quantique

BENNETT Charles, BRASSARD Gilles, EKERT Artur. La cryptographie quantique. Pour la Science [en ligne]. 1 Juillet 2002. [Consulté le 18 Mai 2020]. Disponible à l'adresse : https://www.pourlascience.fr/sr/article/la-cryptographie-quantique-4779.php

Cryptographie Post Quantique. Wikipédia [en ligne]. 2020. [Consulté le 19 Mai]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Cryptographie_post-quantique

INRIA. Cryptographie post-quantique : forte présence d'Inria au NIST. INRIA Blog [en ligne]. 14 Mai 2019. [Consulté 25 Mai 2020]. Disponible à l'adresse : https://www.inria.fr/fr/inria-au-nist

PERRET Ludovic, FAUGERE Jean-Charles. Le grand défi du post-quantique. MISC [en ligne]. Avril 2016. [Consulté le 11 avril 2020]. HS N°13. Disponible à l'adresse : https://connect.ed-diamond.com/MISC/MISCHS-013/Le-grand-defi-du-post-quantique

Vincent (nom non disponible.). L'ordinateur quantique : tout comprendre en partant de zéro. Institut Pandore [en ligne]. 23 Janvier 2020. [Consulté le 02 Juin 2020]. Disponible à l'adresse : https://www.institut-pandore.com/physique-quantique/informatique-ordinateur-quantique/

Calculateur Quantique. Wikipédia [en ligne]. 2020. [Consulté le 23 Mai]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Calculateur_quantique

SACCO, Laurent. Ordinateur Quantique. Futura Science [en ligne]. [Consulté le 1 Juin 2020]. Disponible à l'adresse : https://www.futura-sciences.com/sciences/definitions/physique-ordinateur-quantique-4348/

EZRATTY, Olivier. Comprendre l'informatique quantique. Édition 2019. Ebook, 2019. 504p. [Consulté le 10 Février 2020]. Disponible à l'adresse : https://www.oezratty.net/wordpress/2019/comprendre-informatique-quantique-edition-2019/

Mécanique Quantique. Wikipédia [en ligne]. 2020. [Consulté le 29 Mai]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/M%C3%A9canique_quantique

CEA. La mécanique quantique. CEA [en ligne]. 15 Mai 2019. [Consulté le 14 Avril 2020]. Disponible à l'adresse : http://www.cea.fr/comprendre/Pages/physique-chimie/essentiel-sur-mecanique-quantique.aspx

Physique Quantique. Wikipédia [en ligne]. 2020. Consulté le 29 Mai]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Physique_quantique

Futura Science. Physique Quantique. Futura Science [en ligne]. [Consulté le 26 Mai]. Disponible à l'adresse : https://www.futura-sciences.com/sciences/definitions/physique-physique-quantique-13197/

BOURDET, Julien. Ordinateur : les promesses de l'aube quantique. CNRS [en ligne]. 6 Janvier 2020. [Consulté le 26 Mai]. Disponible à l'adresse : https://lejournal.cnrs.fr/articles/ordinateur-les-promesses-de-laube-quantique

Informatique Quantique. Wikipédia [en ligne]. 2020. [Consulté le 27 Mai 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Informatique_quantique

SACCO, Laurent. Le secret bancaire résistera-t-il à un algorithme quantique ? Futura Science [en ligne]. 09 Mars 2016. [Consulté le 27 Mai 2020]. Disponible à l'adresse : https://www.futura-sciences.com/sciences/actualites/ordinateur-quantique-secret-bancaire-resistera-t-il-algorithme-quantique-61903/

ASPECT, Alain, LAMBRECHT, Astrid, BOUTON, Fanny, et. al. Technologies quantiques : cryptographie quantiques et post-quantiques. Sénat [en ligne]. Juillet 2019. [Consulté le 06 juin 2020]. Disponible à l'adresse : http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2019_0071_note_cryptographies_quantiques_postquantiques.pdf

ANSSI. L'avenir des communications sécurisées passe-t-il par la distribution quantique des clés ? ANSSI [en ligne]. 4 Mai 2020. [Consulté le 10 Juin 2020]. Disponible à l'adresse : https://www.ssi.gouv.fr/publication/lavenir-des-communications-securisees-passe-t-il-par-la-distribution-quantique-de-cles

Distribution quantique de clé. Wikipédia [en ligne]. 2020. [Consulté le 10 Juin 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Distribution_quantique_de_cl%C3%A9

La recherche. Le NIST a annoncé les protocoles qui seront examinés pour devenir les nouveaux standards de cryptographie post-quantique. La recherche [en ligne]. 5 Février 2019. [Consulté le 11 Juin 2020]. Disponible à l'adresse : https://www.larecherche.fr/informatique-cryptographie/le-nist-annonc%C3%A9-les-protocoles-qui-seront-examin%C3%A9s-pour-devenir-les

12 Table des figures

13 Glossaire et liste des abréviations

PCI DSS : Payment Card Industry Data Security Standard

PCI SSC : Payment Card Industry Security Standard Council

QSA : Qualified Security Assessors

HSM : Hardware Security Module

Serveur : Dispositif informatique offrant des services à différents clients. Mail ou Web par exemple.

EMV & EMVCo : Europay, Mastercard & Visa forment l'EMVCo

GIE CB : Groupement des cartes bancaires CB

CB : Carte Bancaire

SSL/TLS : Secure Sockets Layer / Transport Layer Security

SHA : Secure Hash Algorithm

RSA : Du nom des trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman.

DES : Data Encryption Standard, notamment utilisé trois fois pour former 3DES

PAN : Primary Account Number est le numéro de votre carte bancaire.

TPE : Terminal de paiement électronique également appelé moyen d'acceptation ou point d'acceptation.

Chiffrer : Procédé cryptographique visant à rendre impossible la lecture d'un message aux personnes qui n'ont pas la clé.

Clair : Un message en clair est le texte original.

Déchiffrer : Retrouver le texte original d'un message chiffré dont on possède la clé.

Signature : Mécanisme permettant de garantir l'intégrité d'un document et d'en identifier l'auteur.

Non répudiation : Vérification qu'aucune des parties ne peut remettre en cause les échanges.

Cryptographie : Discipline de la cryptologie visant à protéger des messages.

Cryptologie : La cryptologie correspond à la science du secret, elle englobe la cryptographie et la cryptanalyse.

Cryptanalyse : Discipline de la cryptologie qui consiste en l'étude de la cryptographie.

Physique quantique : Regroupe l'ensemble des théories physiques qui décrivent le comportement de l'infiniment petit.

Informatique quantique : Sous domaine de l'informatique qui traite des calculateurs quantiques.

Calculateur quantique ou ordinateur quantique :Ordinateur qui utilise les propriétés de la physique quantique.

Cryptographie quantique : Utilisation des propriétés quantiques pour créer des protocoles de chiffrement.

Cryptographie post-quantique : Branche de la cryptographie qui consiste à garantir la sécurité des messages face à des attaquants munis d'un calculateur quantique.

ECC : Elliptic Curve Cryptography.

QKD : Quantum Key Distribution.