ESIT - Université Sorbonne Nouvelle

La cryptographie post-quantique

Antoine Astruc
Sous la direction de Madame Isabelle Collombat

Mémoire de Master 2
Mention traduction et interprétation
Spécialité traduction éditoriale, économique et technique
Anglais - Français

Session de septembre 2024

Déclaration sur l'honneur

Je soussigné, Antoine Astruc, déclare avoir rédigé ce travail sans aides extérieures ni sources autres que celles qui sont citées. Toutes les utilisations de textes préexistants, publiés ou non, y compris en version électronique, sont signalées comme telles. Ce travail n'a été soumis à aucun autre jury d'examen sous une forme identique ou similaire, que ce soit en France ou à l'étranger, à l'université ou dans une autre institution, par moi-même ou par autrui.

Remerciements

Je remercie tout d'abord Mme Isabelle Collombat, qui a dirigé ce mémoire, pour ses conseils précieux, ses relectures et ses encouragements tout au long de sa rédaction.

Je remercie également Mme Hanna Martikainen de m'avoir accompagné dans les premières étapes de ma réflexion au sujet du mémoire.

Je tiens ensuite à remercier M. Olivier Blazy, mon spécialiste référent, avec qui j'ai beaucoup apprécié travailler et dont les précieux conseils et explications m'ont permis d'aborder avec sérénité un sujet à la technicité parfois écrasante.

Enfin, je remercie chaleureusement Cécile Gagnard pour ses relectures attentives et son soutien infaillible pendant cette année de travail.

Table des matières

Première partie

Exposé

Avertissement au lecteur

Les termes relatifs au sujet traité sont répertoriés dans les lexiques du présent mémoire. Les termes figurant dans le glossaire sont soulignés lors de leur première occurrence (exemple : terme) et ceux faisant l'objet d'une fiche terminologique sont encadrés et suivis du numéro de la fiche en exposant lors de leur première occurrence (exemple : terme[F01]).

Introduction

Le perfectionnement de la recherche et des techniques est à l'origine d'une nouvelle révolution au carrefour des mathématiques, de l'informatique et de la physique. Depuis que l'entreprise Google a annoncé avoir atteint la suprématie quantique en 2019[1], suivie de peu par IBM avec qui elle livre une bataille féroce, le principe déjà ancien de l'ordinateur quantique est devenu réalité, avec des implications matérielles en passe de bousculer tout l'édifice de l'informatique et de la communication. Le calcul quantique, caractérisé par son parallélisme, associé à des algorithmes quantiques dédiés, serait en mesure de casser certains des systèmes de chiffrement actuels en un temps record.

Cette cryptapocalypse[2] cristallise les craintes liées à l'avènement de l'ère quantique en informatique. Près de 95 % du trafic internet fait aujourd'hui l'objet de mesures de chiffrement. L'ordinateur quantique, épée de Damoclès au-dessus des systèmes actuels de chiffrement, est donc le moteur de nouvelles recherches en cryptologie visant à protéger les systèmes classiques contre les attaques quantiques. Face à une attaque à l'ampleur potentiellement dévastatrice et susceptible de se produire dans la décennie à venir, les organismes de recherche se sont regroupés autour de l'autorité mondiale en matière de normalisation des procédés cryptographiques, le *National Institute of Standards and Technology* (NIST), qui a lancé dès 2016 une initiative mondiale dans l'objectif de normaliser le premier algorithme de cryptographie post-quantique en 2024.

Cet exposé s'intéressera d'abord à la cryptographie classique, à son fonctionnement et à sa mise en œuvre actuelle. Nous nous intéresserons ensuite à la cryptanalyse quantique afin de déterminer la nature de cette menace, tout en prenant soin d'étudier sa réalisation physique qui conditionne aujourd'hui son déploiement à grande échelle. Enfin, nous nous pencherons sur l'état du développement de la cryptographie post-quantique et sur ce à quoi pourrait ressembler la transition quantique initiée par le NIST en 2016.

[1] La notion de *suprématie quantique* revêt une signification plus médiatique que proprement scientifique. L'article publié par Google dans *Nature* a lui-même fait l'objet de critiques quant au problème et à l'algorithme utilisés pour la démonstration.

[2] Le terme alarmiste de cryptapocalypse désigne le déploiement soudain et imprévu de technologies de cryptanalyse quantique et l'effondrement de l'édifice cryptographique mondial – un scénario aujourd'hui jugé très peu probable par les spécialistes.

1 La cryptographie classique

La cryptographie désigne l'ensemble des méthodes employées pour chiffrer des messages. Au-delà de la confidentialité des données chiffrées, elle s'intéresse de nos jours également à leur authenticité et à leur intégrité. L'avènement de l'informatique a transformé la cryptographie, l'exécution d'algorithmes de chiffrement suffisamment puissants ne pouvant reposer que sur un calcul informatique. La notion de cryptographie classique désigne l'ensemble des algorithmes de chiffrement exécutés sur des processeurs faits de transistors et travaillant sur des données binaires. Elle s'oppose à celle de cryptographie quantique, dont les algorithmes quantiques sont exécutés sur des ordinateurs quantiques dont nous détaillerons le fonctionnement un peu plus loin. La cryptographie quantique ne fait pas l'objet de ce mémoire : il s'agit d'une méthode de chiffrement encore inexploitée à grande échelle, dont le fonctionnement est détaillé en 3.1.1. Nous ne nous intéresserons qu'à la relation entre la cryptographie (chiffrement) classique et la cryptanalyse (déchiffrement) quantique.

1.1 L'informatique et la révolution cryptographique

Si l'emploi de méthodes de cryptographie remonte à l'antiquité, comme en témoigne le désormais célèbre chiffre de César ou chiffrement par décalage, la cryptologie en tant que science n'est réellement née qu'au XX^{e} siècle. C'est au cours de la Première et de la Seconde Guerres mondiales que les mathématiciens se sont réellement emparés de la cryptographie et, surtout, de la cryptanalyse.[1] Une première distinction théorique est nécessaire entre cryptologie, cryptographie et cryptanalyse.

1.1.1 Attaque et défense

La cryptologie désigne la science de la protection des messages.[2] Elle se divise ensuite en deux domaines : la cryptographie, dont l'objectif est de cacher le sens d'un message, et la cryptanalyse, dont l'objectif est de retrouver le sens caché de ce message. On peut ensuite multiplier les dichotomies, comme le *chiffrement* et le *déchiffrement* (dans l'application mathématique de la cryptographie) ou bien, l'analogie la plus simple, *l'attaque* et la

[1] La cryptanalyse de la machine *Enigma* par les cryptanalystes britanniques, dont Alan Turing, permit aux Alliés d'intercepter et de déchiffrer un grand nombre de communications allemandes.

[2] Le terme « message » peut désigner n'importe quel type de donnée numérique : les algorithmes de chiffrement prennent des chiffres en base binaire en entrée et donnent des chiffres en base binaire en sortie.

défense. Les deux domaines sont inextricablement liés dans l'histoire de la cryptographie : celle-ci peut s'entendre comme une succession de découvertes en défense comme en attaque, un rapport de force constant entre deux objectifs opposés. La solidité du système cryptographique actuel tient du déploiement massif de puissantes fonctions cryptographiques que les cryptanalystes peinent à mettre en échec. Ces deux disciplines ne sont en rien hermétiques : le cryptographe ne cesse de se mettre dans la peau du cryptanalyste afin d'éprouver la solidité de ses propres conceptions.

1.1.2 La cryptologie algorithmique

La cryptologie proprement mathématique est née sous l'impulsion de Claude Shannon en 1949[1], avant de se concrétiser dans les années 1970 grâce à l'utilisation des ordinateurs. Avec à la clé une transformation radicale : les algorithmes de cryptographie ne s'exécutent plus à la main, mais uniquement par un calcul informatique. La cryptographie a non seulement gagné en complexité, mais elle est également devenue utilisable par tout un chacun. La science encore jeune de la cryptologie s'est déplacée à l'intersection des mathématiques et de l'informatique. Un algorithme cryptographique ne peut plus être imaginé en dehors de son support, de sa réalisation physique.

Celle-ci, dans le cadre d'une cryptographie classique exécutée sur des machines classiques, repose sur la circulation d'un grand nombre d'électrons (un courant) au sein d'un ensemble de transistors (un processeur). L'algorithme désigne ici une succession d'opérations mathématiques très simples mais exécutées un grand nombre de fois pour modéliser des fonctions complexes. Le fonctionnement de l'algorithmique classique est intrinsèquement lié à l'architecture des calculateurs employés pour l'exécuter. Il est ainsi essentiel de délimiter l'informatique classique, avec ses algorithmes classiques, fournissant des solutions de cryptographie et de cryptanalyse classiques, de l'informatique quantique, avec ses propres algorithmes et ses propres solutions cryptologiques, sur laquelle nous reviendrons dans une seconde partie. Nous pouvons ainsi délimiter plus clairement l'objet de cet exposé, qui se concentre sur un ensemble de méthodes cryptographiques, la cryptographie classique ; sur une cryptanalyse qui les menace, la cryptanalyse quantique ; et sur la réponse classique envisagée : la cryptographie post-quantique.

[1] Shannon Claude. Communication theory of secrecy systems. *The Bell System Technical Journal*, vol. 28, n°4, 1949, pp. 656-715.

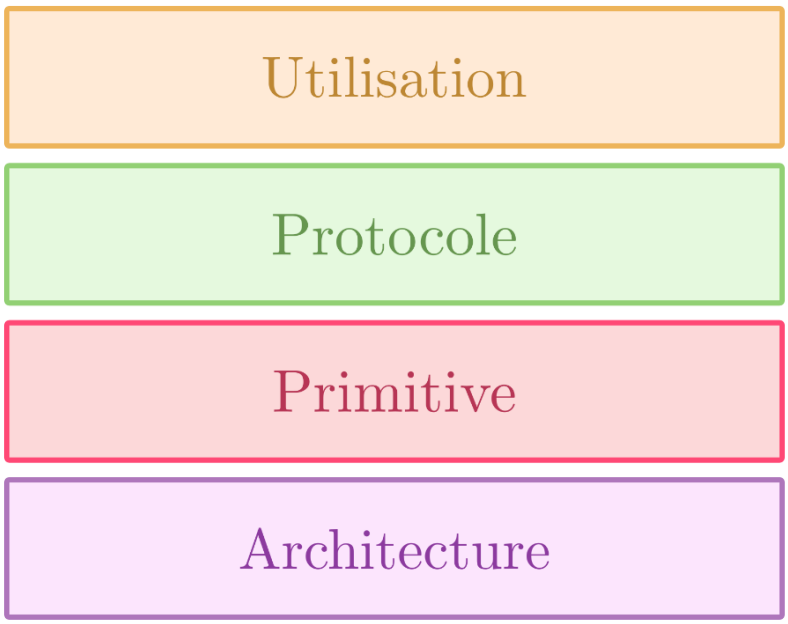

FIGURE 1.1 : Segmentation en couches des outils cryptographiques

Source : NUGIER Cyrius. *Adaptation d'Outils Cryptographiques pour un Contexte Post-Quantique*. Thèse de doctorat : Réseaux et télécommunications : Université de Toulouse : 2018.

1.1.3 La segmentation en couches de la cryptologie

Le fonctionnement des cryptosystèmes à l'ère informatique peut être segmenté sous forme de couches[1]. Nous nous intéresserons particulièrement à l'une d'entre elles, mais comprendre leur articulation est essentiel.

La couche Utilisation englobe l'ensemble des applications des outils cryptographiques. C'est la couche directement pilotée par l'utilisateur.

La couche Protocole se réfère aux transmissions de données entre utilisateurs. Elle définit la façon d'utiliser des outils cryptographiques définis à la couche Primitive.

La couche Primitive désigne les fonctions mathématiques utilisées pour le chiffrement : les primitives cryptographiques. Des algorithmes, dont certains seront détaillés plus loin dans cet exposé, permettent de calculer le résultat de ces fonctions. Toutes sont conçues pour fonctionner sur des architectures classiques.

La couche Architecture comprend les supports physiques des algorithmes, typiquement des PC ou des téléphones portables.

Imaginons un étudiant qui souhaite envoyer un mail depuis son adresse universitaire (Utilisation). Son navigateur sécurise la transmission à l'aide de TLS (Protocole), qui fonctionne avec l'algorithme SHA-2 (Primitive) dont le calcul est effectué sur son PC portable (Architecture).

Dans ces conditions, la puissance de calcul disponible pour faire fonctionner les algorithmes de chiffrement et de déchiffrement devient une variable indispensable en cryptologie. La sécurité d'un cryptosystème est toujours relative à la puissance de calcul de l'attaquant, qui s'exprime en cycles de calcul. Un cryptosystème est réputé sûr si sa cryptanalyse requiert un temps au-delà de l'échelle humaine ou des moyens démesurés, c'est-à-dire un investissement plus élevé que ce que la réussite de l'opération pourrait au mieux rapporter.[2]

Nous nous proposons, dans les sous-parties qui suivent, de détailler la mise en œuvre des solutions cryptographiques classiques. Nous nous concentrerons ainsi dans un premier

[1] Nugier Cyrius. op. cit. p. 12.

[2] Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005. p. 26.

```
-----BEGIN PGP MESSAGE-----
jA0ECQMCNhzp/6afLvb/0mMBMlJjq8KY4Rxya3gHjw+TUCwlRcymuywjxEFyj6l0
EjWwtpVtwGH/Op60zxSERjrKtXZIs92iirECujQK8Ht6wAdDkXOiJquCrP68uqqN
1xMenh84mEpLJe4LERzjpfv1EPI=
=hBS8
-----END PGP MESSAGE-----
```

FIGURE 1.2 : Exemple de message chiffré en utilisant le logiciel GnuPG avec l'algorithme AES-256.

Le message d'origine est *La déverbalisation est-elle un déchiffrement ?* et la phrase de passe employée *cettephraseestsecrete*.

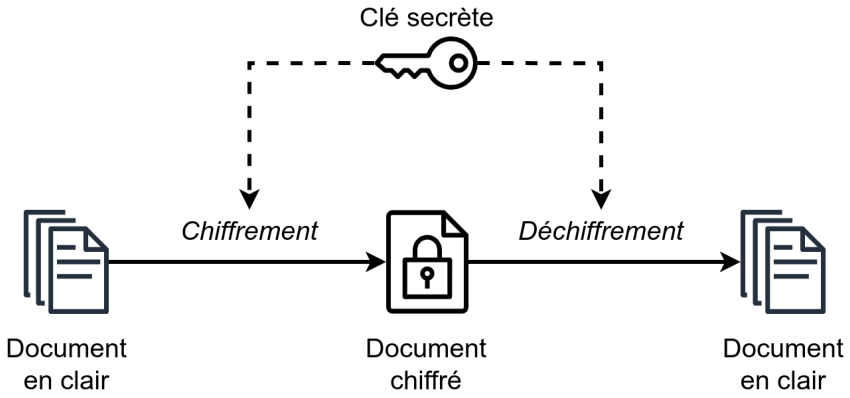

FIGURE 1.3 : Schéma du chiffrement symétrique.
Source : MarcT0K, CC BY-SA 4.0

temps sur la distinction entre la cryptographie symétrique et asymétrique, avant de nous intéresser aux constructions mathématiques derrière ces systèmes cryptographiques.

1.2 Cryptographie symétrique et asymétrique

1.2.1 Le secret, c'est la clé

Un algorithme de chiffrement désigne une technique de transformation d'un message. Il peut s'agir, dans le cas du Chiffre de César par exemple, d'un décalage des lettres de l'alphabet. Cet algorithme s'accompagne d'une clé : ici, il s'agit du nombre de lettres de décalage entre le message original et le message chiffré. Selon le principe fondamental de la cryptographie énoncé par A. Kerckchoffs[1], le secret d'un système ne doit reposer que sur la clé. Il serait contre-productif de fonder la sécurité d'un système sur la complexité de son algorithme, que tout adversaire est capable de comprendre. On considère même désormais qu'un système de chiffrement est plus sûr lorsqu'il est public : exposé aux attaques et largement étudié, il est plus simple d'évaluer sa sécurité à un moment donné. Un algorithme est donc dépourvu de point faible si le déchiffrement des messages n'est possible que si l'on est en possession de la clé. Sa distribution et sa protection sont donc les principaux gages de protection lorsque l'on utilise un cryptosystème dit *sûr*.

La cryptographie moderne repose sur deux types de systèmes : les cryptosystèmes symétriques et asymétriques. Il s'agit d'une dichotomie essentielle en ce qu'ils ne reposent pas sur les mêmes algorithmes et n'ont donc pas le même comportement ni la même résistance face à des tentatives de cryptanalyse quantique. Ils font tous deux l'objet de cet exposé.

1.2.2 La cryptographie symétrique

La cryptographie symétrique repose sur une clé partagée entre l'expéditeur et le destinataire d'un message.[2] Ce système est par exemple parfaitement adapté pour chiffrer un support de stockage utilisé par une seule personne, et s'assurer que personne ne puisse y accéder. Il s'agit du type de chiffrement auquel nous avons procédé pour obtenir la FIGURE 1.2. Le chiffrement symétrique montre toutefois ses limites dans le cadre d'une

[1] KERCKCHOFFS Auguste. La cryptographie militaire. *Journal des sciences militaires*, vol. IX, 1883, pp. 5–38, pp. 161–191.

[2] AMADIO Roberto. *Notes de cryptographie* [en ligne]. Université de Paris, 2022. p. 13. Disponible sur <https ://pastel.hal.science/pastel-00001442/document> (consulté le 13/03/2024)

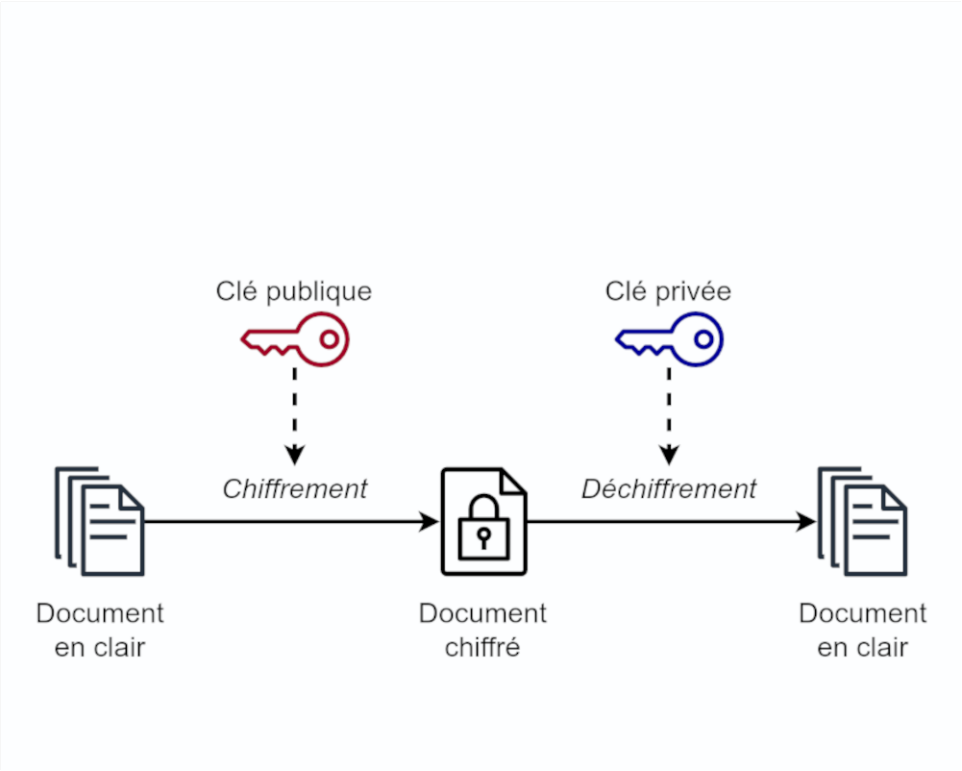

FIGURE 1.4 : Schéma du chiffrement asymétrique.

Source : MarcT0K, CC BY-SA 4.0

communication entre des personnes différentes. Si l'on utilisait une seule clé secrète pour communiquer avec plusieurs personnes, chacune serait capable de lire l'intégralité des messages en circulation, y compris ceux qui ne lui sont pas destinés. Ainsi, un système de communication nécessite au moins autant de clés secrètes qu'il y a de combinaisons d'interlocuteurs. La distribution des clés pose également problème : imaginons que l'on souhaite communiquer de manière sécurisée avec une personne avec qui l'on ne peut pas avoir de première interaction permettant d'échanger une clé. C'est tout le problème que cherche à résoudre la cryptographie asymétrique.

1.2.3 La cryptographie asymétrique

Le chiffrement asymétrique a vu le jour dans les années 70. Il a été conçu pour répondre aux problèmes inhérents au chiffrement symétrique que nous venons d'exposer. Chaque personne désirant communiquer possède une paire de clés. La première, la clé publique, est accessible à tous. Elle est utilisée par les autres personnes pour chiffrer des messages et les lui envoyer. La seconde, la clé privée, doit être gardée secrète. Elle permet de déchiffrer et donc d'accéder au sens original des messages chiffrés avec la clé publique.[1]

Imaginons qu'Angèle cherche à envoyer un message à Basile que seul ce dernier pourra lire. Le fonctionnement du cryptosystème est analogue à celui d'un cadenas à code déjà ouvert.

1. Basile met à la disposition d'Angèle un cadenas à code déjà ouvert (la clé publique) dont seul lui connaît le code.

2. Angèle met ce qu'elle veut envoyer à Basile dans une boîte (le message) qu'elle verrouille à l'aide du cadenas (la clé publique). Même elle ne peut plus rouvrir la boîte ensuite.

3. Basile reçoit la boîte (le message) envoyée par Angèle : il lui suffit d'entrer le code du cadenas (la clé privée) pour ouvrir la boîte (déchiffrer le message).

[1] Amadio Roberto. op. cit. p. 14.

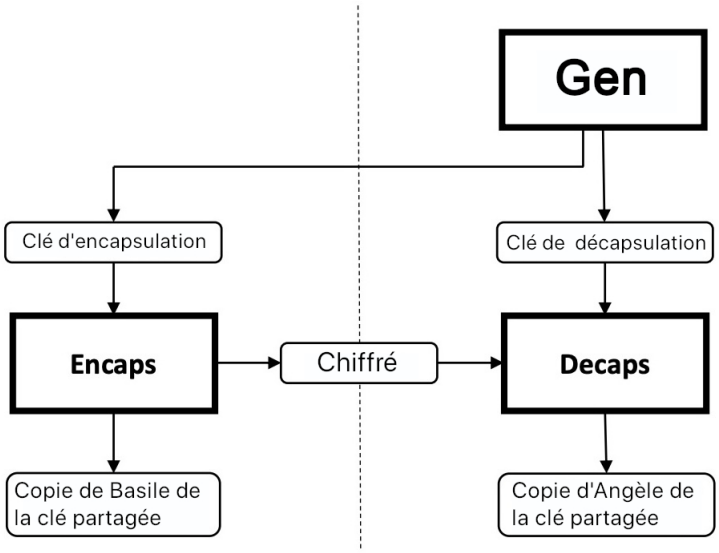

FIGURE 1.5 : Fonctionnement d'un mécanisme d'encapsulation de clé et de ses trois algorithmes *Gen*, *Encaps* et *Decaps*.

Ce système de chiffrement permet ainsi de résoudre les problèmes posés par le chiffrement symétrique.

1.2.4 Les mécanismes d'échange de clés

En pratique, la cryptographie asymétrique est beaucoup plus lente que la cryptographie symétrique en raison des fonctions mathématiques employées, que nous détaillerons dans la section 1.3. La cryptographie asymétrique permet cependant de contourner ce problème en n'intervenant qu'une fois par session de communication, afin de distribuer de manière sécurisée une clé de cryptographie symétrique. La communication peut ensuite avoir lieu de manière beaucoup plus importante entre les deux entités. Ce dispositif se nomme mécanisme d'échange de clés. Le protocole cryptographique TLS, le plus utilisé dans le cadre de la navigation internet, est fondé sur ce mécanisme. Les mécanismes d'encapsulation de clé[F02] diffèrent des mécanismes d'échange de clé car ce n'est pas directement la clé qui fait l'objet d'une transmission mais une donnée secrète qui est ensuite utilisée par les deux parties pour obtenir une clé symétrique, ou clé de session, à l'aide d'un algorithme appelé *Decaps*.[1] Cette solution, qui combine efficacement les avantages des deux mécanismes symétriques et asymétriques, est aujourd'hui la plus utilisée en cryptographie. À ce titre, c'est un mécanisme d'encapsulation de clé post-quantique que le NIST cherche à normaliser depuis 2016.[2]

1.3 Algorithmes et calculs en cryptographie classique

Nous nous proposons dans cette partie de franchir un pas de plus dans l'abstraction pour nous intéresser à la construction mathématique des fonctions cryptographiques. Nous nous intéresserons aux algorithmes de cryptographie symétrique et asymétrique.

1.3.1 Théorie de la complexité

En algorithmique, les algorithmes sont classés en fonction de leur complexité, c'est-à-dire de la quantité de ressources nécessaires pour les exécuter sur des données de taille N.[3] On distingue plusieurs classes de complexité, nous ne nous intéresserons ici qu'à certaines.

[1] Mortajine Lina. *Analyse d'algorithmes post-quantiques implantables en pratique*. Thèse de doctorat : Microélectronique : Université de Lyon : 2021.

[2] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2017. 25 p.

[3] Perifel Sylvain. *Complexité algorithmique*. Ellipses, 2014, p. 32.

Temps	Type de complexité	$n = 5$	$n = 50$	$n = 250$	$n = 10^4$	$n = 10^6$
n	Complexité linéaire	50 ns	500 ns	2,5 µs	100 µs	10 ms
n^2	Complexité polynomiale	250 ns	25 µs	625 µs	1 s	3 heures
$2^{n^{1/3}}$	Complexité sous-exponentielle	32 ns	130 ns	780 ns	30 ms	10^{14} ans
2^n	Complexité exponentielle	320 ns	130 jours	10^{59} ans	...	...

FIGURE 1.6 : Ordre de grandeur du temps nécessaire à l'exécution d'un algorithme sur des données de taille n et avec un temps d'accès mémoire de 10 ns. Il s'agit d'une approximation importante dont la seule fonction est de mettre en évidence la différence d'ordre de grandeur entre les différentes complexités.

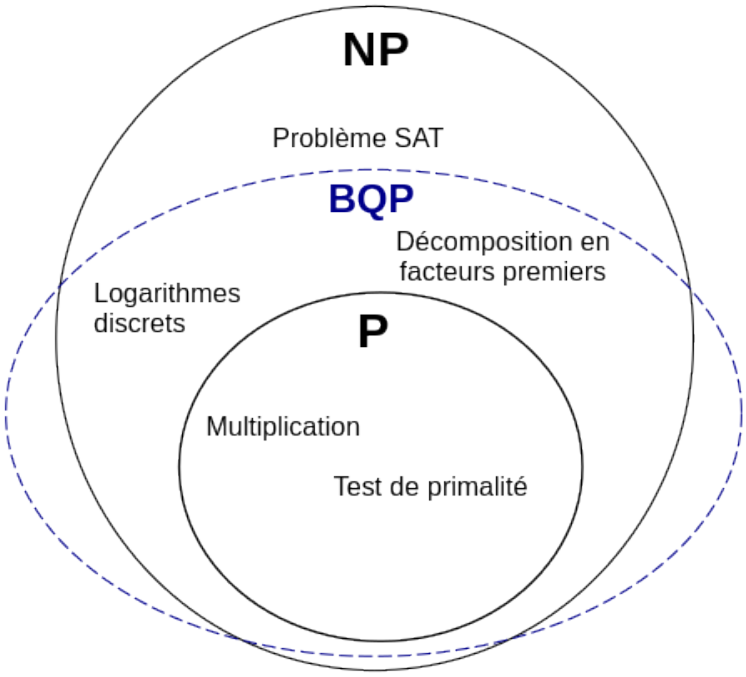

FIGURE 1.7 : Schéma d'inclusion des différentes classes de complexité avec les problèmes qu'elles contiennent.

La classe **P** comprend les problèmes décisionnels pour lesquels une machine peut trouver une solution déterministe en un temps polynomial par rapport à la taille des entrées. C'est à dire que le temps et les ressources consommées par l'exécution de l'algorithme augmentent proportionnellement à N^a, où a est un nombre réel.[1]

La classe **NP** contient les problèmes décisionnels pour lesquels il n'existe pas d'algorithme de résolution efficace (c'est-à-dire polynomial), les meilleurs algorithmes s'exécutant en temps exponentiel ou sous-exponentiel (c'est à dire proportionnellement à 2^N avec N la taille de l'entrée).[2] Toute solution à ce problème reste vérifiable en temps polynomial.

La classe **BQP** contient les problèmes réputés complexes qu'il est possible de résoudre en temps polynomial à l'aide d'un ordinateur quantique. Il s'agit d'une formation récente et dont les liens avec les classes de complexité classiques demeurent obscurs.

Nous nous réfèrerons à nouveau la théorie de la complexité et à ses classes dans cet exposé. En résumé, l'algorithmique range les différents problèmes décisionnels dans des classes de complexité (typiquement P, NP). Celles-ci dépendent des algorithmes découverts pour résoudre ces problèmes, dont la complexité est dite polynomiale, sous-exponentielle ou exponentielle selon le rapport de proportionnalité entre les ressources nécessaires à l'exécution et la taille des données en entrée. Le point commun aux deux classes est l'existence d'algorithmes permettant de vérifier des solutions dans un temps polynomial. Dans les points suivants, nous nous intéresserons aux problèmes qui sous-tendent les primitives cryptographiques en identifiant les classes auxquelles ils appartiennent.

1.3.2 Cryptographie symétrique et hachage

Dans la cryptographie symétrique, l'expéditeur et le destinataire partagent un secret : il peut s'agir de l'algorithme ou bien de la clé (de chiffrement comme de déchiffrement), solution la plus sûre. La clé utilisée doit pouvoir prendre suffisamment de valeurs pour qu'une attaque par force brute soit beaucoup trop longue pour être menée à bien. Pour

[1] Louapre David, *Insoluble mais vrai !*, Flammarion, 2017, p. 120.

[2] Les algorithmes de complexité sous-exponentielle se situent entre la complexité polynomiale et la complexité exponentielle. Mêmes s'ils s'exécutent beaucoup plus vite que des algorithmes de complexité exponentielle, ils ne peuvent être considérés polynomiaux. Le crible algébrique, présenté au point 1.3.3, en est un bon exemple.

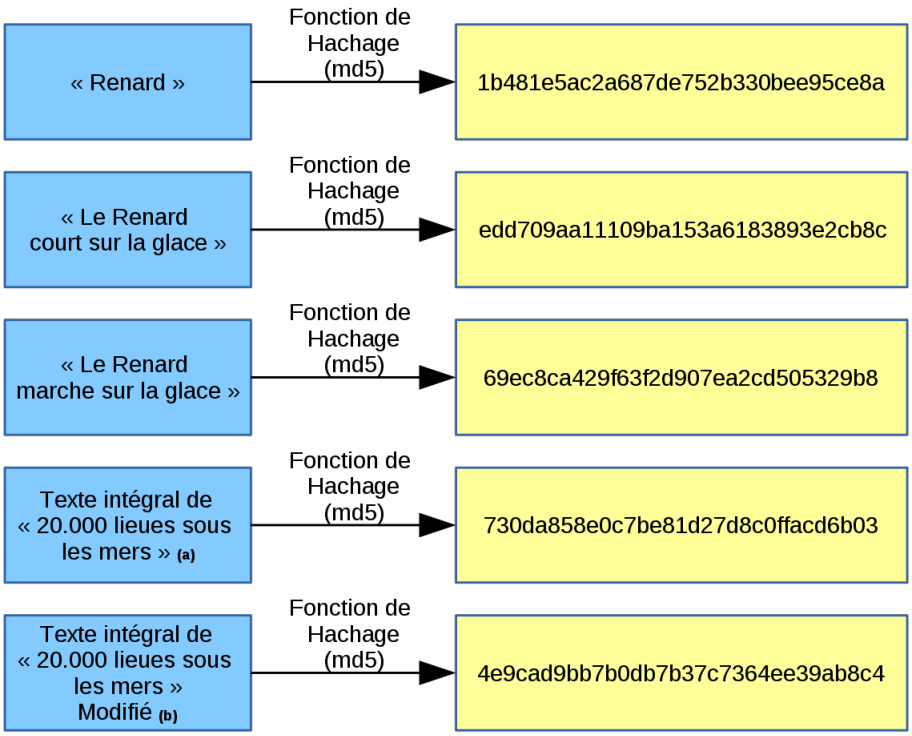

FIGURE 1.8 : Hachage réalisé avec la fontion md-5 proposée par le site *defuse.ca*.
Source : utilisateur *Unique Nitrogen* sur *Wikimedia*.

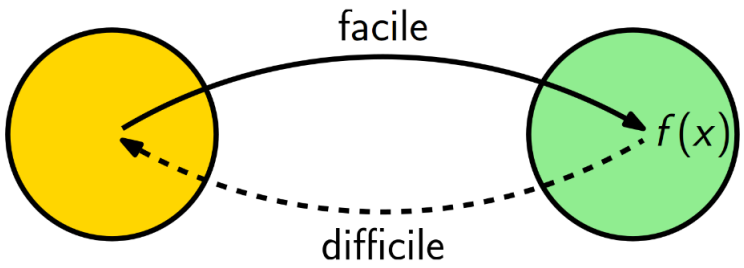

FIGURE 1.9 : Principe d'une fonction à sens unique.
Source : NITULESCU Anca. *Introduction à la cryptographie, Cours 4 : Cryptosystème ElGamal*. Paris : École Normale Supérieure.

cela, il est possible de jouer sur la longueur des clés. Une clé de 128 bits, comme celles préconisées pour l'algorithme AES normalisé en 2001 par le NIST, peut prendre environ $3{,}4 \times 10^{38}$ valeurs différentes.[1] Ce nombre démesuré permet aux algorithmes de chiffrement symétrique sur 128 bits d'être hors de portée de tous les meilleurs calculateurs classiques du monde dans le cas d'une attaque par force brute.

Les algorithmes peuvent traiter des blocs de données, découpant le message en un certain nombre de blocs longs d'un nombre constant de bits, ou bien agir au niveau du bit ou de l'octet. Les algorithmes de chiffrement symétrique par blocs agissent par substitution et par permutation. La substitution consiste à remplacer des données par d'autres, la permutation à changer les données de place. Ces opérations sont effectuées un nombre défini de fois, on parle de tours. Le chiffrement AES, standard mondial en matière de cryptographie, prend en entre un bloc de 128 bits soit 16 octets, et fonctionne avec des clés de 128, 192 ou 256 bits. Une clé de 128 bits nécessite d'effectuer 10 tours, une clé de 192, 12, et une clé de 256, 14. Du fait de cette avalanche de substitutions et de permutations opérées sur les données, le moindre changement en entrée donnera une sortie complètement différente. C'est là le cœur de la sécurité des algorithmes de chiffrement symétrique.

Les fonctions de hachage cryptographiques font également partie de la cryptographie symétrique. Ces fonctions déterministes permettent de calculer l'empreinte chiffrée d'un message, c'est-à-dire qu'elles associent à des données de taille arbitraire des données de taille fixe. Le déterminisme de ce procédé cryptographique implique que la même fonction de hachage utilisée sur les mêmes données donnera toujours la même empreinte. En revanche, la moindre petite différence dans les données d'entrée aboutira à un résultat complètement différent en vertu de l'effet dit d'avalanche.[2]

1.3.3 Cryptographie asymétrique : les fonctions à trappe

Les cryptosystèmes asymétriques fonctionnent de manière totalement différente. Ils impliquent la génération d'une paire de clés dont les deux clés sont intrinsèquement liées. Nous avons vu la relation unissant les clés publiques et privées : la seconde doit permettre de retrouver un message chiffré à partir de la première, sans pour autant que la clé privée

[1] National Institute of Standards and Technology. *FIPS PUB 197 : Advanced Encryption Standard (AES)*. 2001.

[2] Menezes Alfred, Van Oorschot Paul, Vanstone Scott. *Handbook of Applied Cryptography*. CRC Press : 1996, p. 324.

puisse être identifiée dans le processus. En mathématiques, cette situation est celle d'une fonction à sens unique f dont l'image $f(x)$ est facile à calculer en tout point de son domaine de définition mais qu'il est très difficile d'inverser, c'est-à-dire de retrouver x lorsque $f(x)$ est donné. La notion de fonctions à trappe est apparue dans les travaux des cryptologues Whitfield Diffie et Martin Hellman comme une solution au problème du chiffrement asymétrique.[1] Selon la théorie de la complexité définie en 1.3.1, il s'agit de résoudre des problèmes théoriquement NP mais dont la connaissance d'une trappe (la clé privée) permet une résolution en temps polynomial. Les algorithmes de cryptographie asymétrique reposent principalement sur deux primitives, dépendantes elles-mêmes de deux problèmes : le problème de la factorisation de grands entiers et le problème du logarithme discret.

La primitive RSA (des initiales des chercheurs qui l'ont découverte, Ronald Rivest, Adi Shamir et Léonard Adleman) relève de la théorie des nombres. Le problème porte sur la décomposition d'un nombre entier en facteurs premiers.[2] Pour générer une paire de clés RSA, on prend deux entiers premiers p et q et on calcule leur produit n. D'autres opérations ont lieu mais sont indépendantes du problème fondamental : retrouver p et q si l'on dispose seulement de n est pratiquement impossible pour des nombres suffisamment grands.[3]

L'algorithme est donc considéré sûr face aux attaques par force brute menées sur des ordinateurs classiques pour deux raisons :

1. Pour casser cet algorithme par force brute, l'attaquant doit parvenir à factoriser n en ses facteurs premiers p et q.

2. La difficulté de cette tâche croît de manière (sous-)exponentielle à mesure que la taille de la clé augmente.

La taille des clés recommandées actuellement pour l'algorithme RSA est de 2048 bits[4]. Si l'informatique devait rester classique, un doublement à 4096 bits, déjà mis en œuvre

[1] Whitfield Diffie, Hellman Martin. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. 22, n° 6, 1976, pp. 644–654.

[2] Rivest Ronald, Shamir Adi, Adleman Leonard. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol. 21, n° 2, 1978, pp. 120–126.

[3] La factorisation du nombre RSA-250, factorisé un an plus tard que RSA-240 et plus long de 10 chiffres (829 bits), a nécessité l'équivalent de 2700 ans de calcul sur un cœur CPU.

[4] RSA-2048, de la longueur utilisée de nos jours par le chiffrement RSA (617 chiffres), est probablement impossible à décomposer en informatique classique. La prime pour quiconque parviendra à le factoriser est de 200 000$.

par certains protocoles, permettrait d'assurer encore longtemps la sécurité de RSA, le doublement des temps de calcul étant marginal comparé au gain de sécurité (du fait des propriétés de la croissance exponentielle).

Le problème du logarithme discret porte sur l'inversion de la fonction d'exponentiation dans un groupe (c'est-à-dire un ensemble de nombres sur lequel on peut effectuer des opérations). Il existe des groupes pour lesquels on ne connaît pas d'algorithme efficace pour calculer le logarithme. Le calcul de l'exponentiation, sa réciproque, est lui réalisable très rapidement. On retrouve ici un problème NP, vérifiable en temps polynomial, et dont la trappe ou clé secrète permet de le résoudre en temps polynomial. Tout ceci fait du logarithme discret une autre fonction à trappe. Elle est utilisée en cryptographie dans le cadre des mécanismes d'échange de clés de Diffie-Hellman (DH) et El Gamal.

Les deux problèmes que nous venons d'exposer forment le véritable verrou de la cryptogaphie asymétrique. Leurs points communs font que lorsqu'un progrès est réalisé vers la résolution de l'un d'entre eux, il se répercute facilement sur le second. Une autre faiblesse les lie : leur vulnérabilité à la cryptanalyse quantique. Ils appartiennent tous les deux aux problèmes de classe NP contenus dans la classe BQP (Figure 1.7). Autrement dit, il existe des algorithmes permettant de résoudre ces problèmes en temps polynomial grâce aux avantages du calcul quantique.

2 La cryptanalyse quantique

Nous présenterons dans cette partie les phénomènes quantiques exploités en informatique à des fins de cryptanalyse. Nous nous intéresserons dans un premier temps aux spécificités du calcul quantique, avant de nous intéresser dans le détail aux algorithmes quantiques les plus célèbres puis de tenter d'évaluer la réalité de la menace quantique en matière de déchiffrement.

2.1 L'ordinateur quantique

2.1.1 Les phénomènes physiques à l'échelle quantique

La physique quantique est née au début du XX^{e} siècle pour décrire les phénomènes physiques à l'échelle atomique. Si l'on a ensuite mis en évidence des manifestations à notre

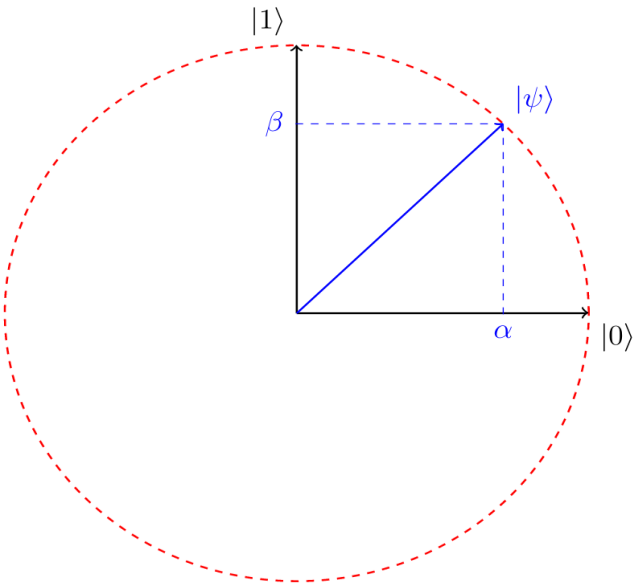

FIGURE 2.1 : Représentation graphique dans le plan du qubit $|\psi\rangle$ (en bleu). Le cercle rouge représente l'ensemble des états possibles lorsque α et β varient tout en vérifiant $|\alpha|^2 + |\beta|^2 = 1$. Un bit classique ne pourrait prendre que la valeur $|0\rangle$ ou la valeur $|1\rangle$.

Source : JAFFALI Hamza. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés*. Thèse de doctorat : Informatique : Université Bourgogne Franche-Comté : 2020.

échelle (macroscopique) de phénomènes quantiques[1], nous ne nous intéresserons ici qu'à l'échelle des particules (microscopique).

Le premier principe de la physique quantique appliquée à l'informatique est celui de superposition quantique. En physique classique, les objets ont un état défini, qu'il est possible de décrire en mesurant des grandeurs physiques (position, vitesse, énergie…). Les systèmes se trouvent dans un seul état à un endroit et à un moment donné. En physique quantique, un système (une particule) admet une superposition cohérente d'états.[2] Il peut se trouver dans tous les états possibles à la fois, avec une probabilité associée à chacun d'eux.

Le second principe est celui d'intrication quantique. Il s'agit d'un phénomène dans lequel deux particules distantes forment un système lié et possèdent des états quantiques dépendants l'un de l'autre. Un système de particules intriquées doit être appréhendé dans sa globalité. Enfin, le modèle quantique montre qu'à une certaine échelle, les valeurs physiques ne sont plus continues mais discrètes : elles sont quantifiées et varient par sauts, sans valeurs intermédiaires. Tous ces ingrédients ont permis d'établir une théorie de l'information quantique dont nous allons résumer les grands traits en nous concentrant sur son plus petit vecteur d'information : le qubit.

En informatique classique, le plus petit vecteur d'information est le bit. Un bit est une variable binaire qui prend comme valeur soit 0 soit 1. Il ne peut avoir que deux états différents, selon sa réalisation physique : ouvert ou fermé, actif ou inactif, percé ou plein, etc. Un bit quantique, ou qubit, en vertu du principe de superposition que nous venons d'exposer, peut être dans l'état 0, dans l'état 1, ou dans une superposition de ces deux états. Un qubit représente l'état d'une propriété spécifique d'un système quantique. Il existe en effet, à l'échelle des particules, des variables qui en plus d'être discrètes ne peuvent prendre que deux valeurs (le spin d'un électron ou la polarisation d'un photon par exemple).

[1] Balian Roger. La physique quantique à notre échelle. *Un siècle de quanta*, Les Ulis, EDP Sciences, 2003, pp. 59-89.

[2] Einstein Albert, Born Max, Born Hedwig. *Correspondance 1916-1955 [« The Born-Einstein letters »]*. Paris : Seuil, coll. « Science Ouverte », 1971. 255 p.

	Type de registre	
n	Classique	Quantique
2	4	4
8	64	256
16	256	65 536
32	1024	$4,2 \times 10^{9}$
64	4096	$1,8 \times 10^{19}$
128	16 384	$3,4 \times 10^{38}$
256	65 536	$1,16 \times 10^{77}$

FIGURE 2.2 : Nombre d'états possibles pour un système à n-bits et à n-qubits. Un système quantique peut manipuler des valeurs impossibles à stocker dans la mémoire vive d'un ordinateur classique.

2.1.2 L'avantage quantique

Les phénomènes quantiques que nous venons d'exposer et leur application sous forme de qubits sont à l'origine d'un avantage quantique, terme employé pour désigner la différence de rapidité pour des tâches bien précises entre un ordinateur classique et un ordinateur quantique. Mobilisons à nouveau les notions de polynômes et d'exponentielles pour déterminer l'ordre de grandeur de cet avantage.

Nous pouvons déduire de tous les principes exposés ci-dessus que l'ordinateur quantique se distingue de l'ordinateur classique par le nombre d'états qu'un vecteur de qubits peut prendre comparé à ceux que peut prendre un vecteur de bits classiques. En effet, un registre de 4 bits classiques peut prendre 16 valeurs différentes : 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111. Le nombre de valeurs possibles pour ce registre est égal à n^2 avec n le nombre de bits disponibles. Leur nombre augmente donc de manière polynomiale par rapport au nombre de bits.

En comparaison, un système quantique de n-qubits intriqués peut présenter et donc manipuler 2^n états simultanément. La progression du nombre d'états possibles est donc exponentielle par rapport à l'augmentation du nombre de qubits. On a, pour un système comportant 4 qubits, $2^4 = 16$ états possibles. Seulement, il suffit de passer à un système de 10 qubits pour obtenir 1024 états possibles, contre 100 dans le cas d'un registre de 10 bits classiques. L'augmentation exponentielle de la puissance de calcul des systèmes intriqués (voir FIGURE 2.2) est à l'origine du parallélisme démesuré permis par le calcul quantique. Un registre de 20 qubits permet d'atteindre le nombre d'états possibles d'un ordinateur de bureau classique, un registre de 40 qubits celui du meilleur supercalculateur classique du monde. Sycamore, le processeur quantique dévoilé par Google en 2019, était doté de 53 qubits. Un seul état superposé du processeur nécessite 250 millions de gigaoctets classiques (2^{18} bits) afin d'être stocké.[1]

[1] ARUTE Frank, ARYA Kunal, BABBUSH Ryan et al. Quantum supremacy using a programmable superconducting processor. *Nature*, n°574, pp. 505-510.

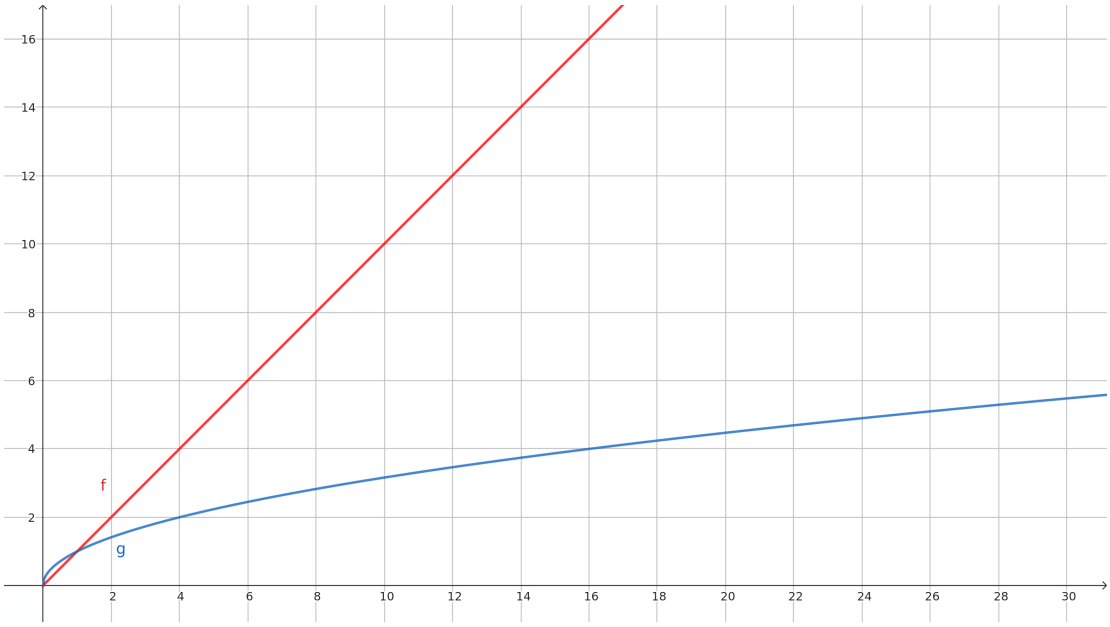

FIGURE 2.3 : Représentation graphique de la différence d'efficacité entre un algorithme de recherche naïf (en rouge) et l'algorithme de Grover (en bleu). Le nombre d'entrées dans la base de données figure en abcisse et le nombre d'opérations nécessaires pour retrouver une entrée précise est représenté en ordonnée.

La principale propriété responsable de l'avantage quantique est donc la taille des informations manipulables en parallèle par un processeur quantique. Celle-ci progresse de manière exponentielle à mesure que le nombre de qubits du processeur augmente. Nous devons cependant tirer une seconde conséquence du fonctionnement de l'ordinateur quantique : celui-ci ne peut faire fonctionner que des algorithmes quantiques prévus pour être exécutés sur des machines quantiques et utilisant à cette fin des circuits logiques quantiques. Nous proposons d'étudier dans la partie suivante deux algorithmes quantiques réputés pour réduire de manière drastique la complexité de problèmes longtemps considérés difficiles par l'informatique classique.

2.2 Les algorithmes de cryptanalyse quantique

L'algorithmique, nous l'avons vu, consiste à étudier les processus systématiques de résolution d'un problème. Centrale en informatique, la discipline s'est étendue à l'informatique quantique où elle a pu exploiter le formidable parallélisme des systèmes quantiques, allant jusqu'à remettre en question la sécurité des primitives cryptographiques. Comme nous nous sommes principalement intéressés aux primitives asymétriques (RSA, DH) et symétriques (AES), nous nous intéresserons principalement aux algorithmes qui s'y rapportent.

2.2.1 L'algorithme de Grover

L'algorithme de Grover, du nom de son créateur Lov Grover, a été dévoilé en 1996.[1] Cet algorithme s'intéresse au problème de la recherche d'un élément dans une base de données non ordonnée de taille N. Face à un annuaire contenant N entrées, ces dernières n'étant pas ordonnés, une personne à la recherche d'un numéro précis doit parcourir et évaluer au moins $\frac{N}{2}$ noms pour avoir atteindre une probabilité de 50% de trouver le bon, N noms dans le pire des cas. La complexité de résolution de ce problème à l'aide d'un algorithme classique est donc linéaire en fonction de la taille de N. Ici, le principe de superposition permet à l'ordinateur quantique d'évaluer plusieurs noms en parallèle. Certains calculs effectués augmentent encore la vitesse à laquelle la machine peut effectuer les calculs restants. En résulte une complexité de l'ordre de $\sqrt{N}$. Il s'agit d'une économie de ressources colossale au vu de la taille des bases de données actuelles. L'algorithme de Grover est l'algorithme quantique le plus efficace permettant de résoudre ce problème de

[1] Lov K. Grover, *A fast quantum mechanical algorithm for database search*. 1996.

recherche dans une base de données non ordonnée. Le parallélisme du calcul quantique ne pourra jamais faire mieux que fournir une amélioration quadratique de la complexité.[1]

2.2.2 L'algorithme de Shor

L'algorithme de Shor a été conçu en 1994 par Peter Shor.[2] Vingt ans après sa publication, il peut être considéré comme l'algorithme qui a rendu célèbres l'informatique et le calcul quantiques et permis l'émergence de la cryptographie post-quantique dont traite cet exposé. L'algorithme, qui porte sur la factorisation de nombres entiers en facteurs premiers, permet en effet de faire passer la de ce problème d'un temps sous-exponentiel à un temps polynomial. Son effet est analogue sur le problème du logarithme discret, qu'il permet également de résoudre en temps polynomial.

Ce passage à un temps d'exécution polynomial par rapport à la taille des données d'entrée menace la sécurité des primitives cryptographiques les plus répandues. Celles-ci sont en effet à portée des attaques menées par des ordinateurs quantiques, le doublement de la longueur des entiers utilisés pour la génération des clés ne permettant pas de rendre les algorithmes durablement plus sûrs. Si l'on parvenait à exécuter l'algorithme de Shor sur des grands nombres, de l'ordre de ceux employés par RSA ou DH (2048 à 4096 bits), l'intégralité des communications et des données chiffrées se retrouveraient accessibles au détenteur d'une telle puissance de calcul. C'est dans ce contexte qu'intervient l'effort de normalisation d'un algorithme de chiffrement post-quantique.

2.3 La réalité de la menace quantique

L'informatique quantique a toujours connu un décalage important entre l'avancée de la recherche théorique et la mise en œuvre réelle de ses découvertes. Presque 40 ans se sont écoulés entre la naissance de l'idée d'un ordinateur quantique dans l'esprit de Richard Feymann et la construction par Google d'un ordinateur sensiblement plus rapide sur un calcul précis que les meilleurs calculateurs classiques.

[1] Zalka Christoph. Grover's Quantum Searching Algorithm is Optimal. *Phys. rev. A*, Volume 60 numéro 4, 1999, p. 2476-2751.

[2] Shor Peter. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, n°26, 1997, p. 1484-1509.

2.3.1 Réalisation et stabilité des qubits

La première difficulté liée au fonctionnement de l'ordinateur quantique réside dans la réalisation et dans la stabilité des qubits sur lesquels il repose. Un qubit est une particule dont on observe l'une des propriétés intrinsèques et son évolution à mesure que des portes quantiques lui sont appliquées. On s'intéresse notamment au spin d'un électron (0 si son spin est *up*, 1 si celui-ci est *down*) ou la polarisation d'un photon (0 si horizontale, 1 si verticale). Il existe différentes classes de qubits, on peut par exemple citer les qubits supraconducteurs (les plus répandus), les qubits utilisant le spin d'un électron dans un matériau semi-conducteur, les ions piégés et les photons.

La stabilité des qubits pose problème. Du fait de l'impossibilité d'isoler un système physique de toute influence extérieure, il est difficile de maintenir des qubits stables dans le temps. Les qubits ont tendance à changer d'état d'eux-mêmes au bout d'un certain temps, au mépris des transformations que l'on cherche à leur imposer à l'aide des portes logiques. En résulte le problème qui mobilise le plus de recherches en informatique quantique actuellement : la correction d'erreurs.[1] L'une des pistes envisagées est la création de qubits logiques à partir d'un certain nombre de qubits physiques. Un qubit logique est ici entendu comme un qubit fonctionnant parfaitement et de manière stable, ce grâce aux très nombreux qubits physiques qui le composent (ce chiffre est en baisse constante, de 10^5 il y a quelques années à quelques centaines aujourd'hui).[2]

2.3.2 État de l'art de l'ordinateur quantique

Si de nombreux processeurs quantiques ont déjà été construits, aucun n'a permis d'exécuter les algorithmes quantiques que nous avons présentés plus haut sur des nombres de nature à menacer les primitives cryptographiques classiques. IBM, principal constructeur de processeurs quantiques, a présenté en décembre sa nouvelle feuille de route en matière de processeurs quantiques. L'entreprise développe des puces renfermant 127 qubits et espère passer la barre des 1000 qubits d'ici 2025. Le rythme d'augmentation du nombre de qubits a très récemment diminué, résultat des nouvelles recherches sur la correction

[1] Shor Peter. Scheme for reducing decoherence in quantum computer memory. *Physical Review*, n° 52, vol. 4. 1995.

[2] Sheldon Sarah. Quantum Computing With Noisy Qubits. *Frontiers of Engineering : Reports on Leading-Edge Engineering from the 2018 Symposium*. 2018.

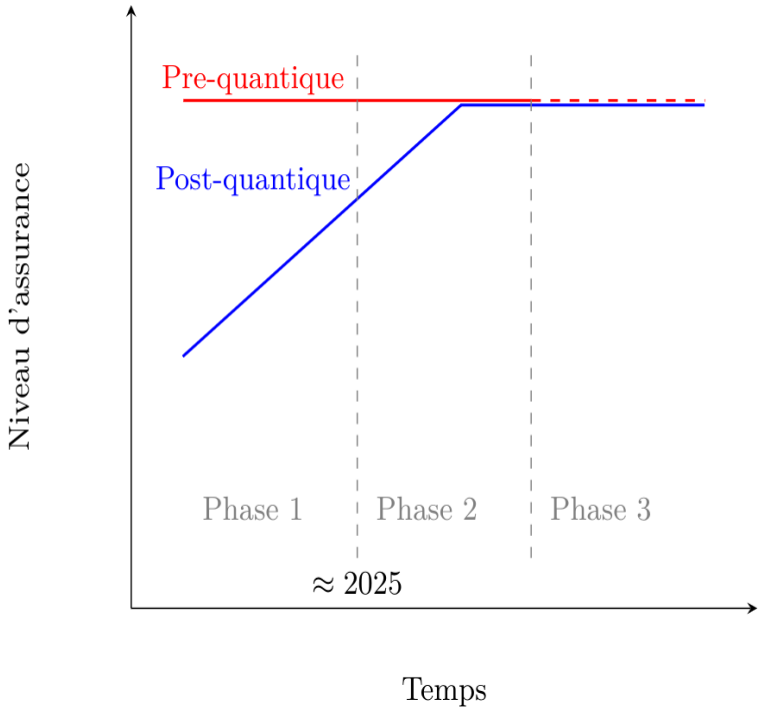

FIGURE 3.1 : La transition quantique « en biseau » prévue par l'ANSSI.

Source : Agence nationale de la sécurité des systèmes d'information. *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*. Paris, 2022.

d'erreurs qui permet d'améliorer la fiabilité et la stabilité des systèmes quantiques.[1] Il s'agit des deux voies actuellement exploitées par la recherche en informatique quantique : l'augmentation du nombre de qubits physiques et l'amélioration des codes correcteurs d'erreurs, les deux ayant le même objectif de faire fonctionner le plus grand nombre de qubits logiques intriqués possible.

Ainsi, en dépit des performances théoriques des algorithmes quantiques, le support physique de leur exécution présente encore de nombreux défauts. Si l'ordinateur quantique universel est un mythe, même les calculateurs quantiques algorithmiques mettent du temps à être développés. Nous ne sommes cependant jamais à l'abri d'une rupture technologique et d'une augmentation rapide et importante de la puissance de calcul quantique. C'est dans ce contexte précis qu'intervient la nécessité de normaliser au plus vite un algorithme de cryptographie post-quantique.

3 La cryptographie post-quantique

Nous venons d'explorer les notions fondamentales de cryptographie (classique) et de cryptanalyse quantique. Si l'histoire du chiffrement des données a toujours fait l'objet d'un duel entre technologies de défense et d'attaque, l'émergence de l'informatique quantique fournit un adversaire d'un nouveau genre aux algorithmes de chiffrement déjà normalisés. La normalisation est essentielle en cryptographie en vertu du principe de Kerckchoffs (1.2.1) : la sécurité d'un système ne doit pas reposer sur la complexité de ce dernier mais sur une clé d'une longueur suffisante. Pour garantir la sécurité d'un cryptosystème moderne, ce dernier doit être largement employé et étudié, d'où l'importance de le normaliser. Le NIST est l'organisme de normalisation national le plus important au monde et maintient déjà les normes cryptographiques symétriques et asymétriques actuelles. Nous nous intéresserons dans cette partie à la chronologie de la transition quantique en cryptologie, particulièrement à la phase de normalisation de la cryptographie post-quantique sous l'égide du NIST. Nous décrirons ensuite brièvement certains des algorithmes candidats à la normalisation en nous concentrant sur CRYSTALS–Kyber, le premier algorithme sélectionné par le NIST.

[1] Castelvecchi Davide. IBM releases first-ever 1,000-qubit quantum chip. In *Nature*, n°624, 2023, p. 238.

3.1 La transition quantique

La transition quantique désigne l'ensemble du passage des systèmes de sécurité à des cryptosystèmes quantique. Celle-ci passera par plusieurs phases qui devraient s'étendre sur plus d'une dizaine d'années.[1]

3.1.1 Chronologie

La chronologie de la transition quantique dépend de nombreux facteurs, c'est la raison pour laquelle presque chaque institut de normalisation ou de sécurité (NIST, ANSSI) et chaque laboratoire (INRIA, Lip) ont leur propre calendrier. L'inscription de cette transition dans un temps long reste un facteur commun à toutes les prévisions. Toutes donnent au moins dix ans à la menace quantique pour se concrétiser. Nous pouvons définir comme point de rupture le déchiffrement d'un message protégé par une clé RSA longue de 2048 bits. Le NIST a évalué à entre 3000 et 5000 le nombre de qubits logiques nécessaires pour casser une telle clé. Nous avons vu à la partie 2.3.3 que faire fonctionner un qubit logique nécessitait un nombre de qubits physiques bien plus important. En 2019, « le ratio entre qubits physiques et logiques [variait] entre 10^3 et 10^5 »[2]. La feuille de route présentée par IBM n'admet donc pas la construction d'un ordinateur quantique capable de casser le cryptosystème RSA avant une dizaine d'années.

La distribution quantique de clé est un système cryptographique que nous n'avons pas encore évoqué et qui constitue à ce jour le cryptosystème le plus efficace. Nous avons vu que la cryptographie symétrique était extrêmement performante et allait sans doute le rester, même face à des attaquants dotés de machines quantiques. Ce sont les mécanismes d'échange de clés, pierre angulaire de la cryptographie asymétrique, qui sont les plus menacés. La distribution quantique de clé repose sur la technologie quantique pour échanger de manière inviolable une clé de cryptographie symétrique. Ce système, qui s'appuie sur le théorème de non-clonage[3] pour garantir l'impossibilité de reproduire la particule employée pour l'échange, permet de plus sous certaines conditions de détecter

[1] Agence nationale de la sécurité des systèmes d'information. *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*. Paris, 2022.

[2] Villani Cédric. L'ordinateur quantique. *Les Notes scientifiques de l'Office*, n°15, 2019, p. 2.

[3] Le théorème de non-clonage quantique désigne l'impossibilité démontrée de copier sans erreur un qubit dans un état quantique inconnu en conservant l'état quantique initial (Avis du 20 décembre 2022 de la Commission d'Enrichissement de la Langue Française). Ainsi, la lecture d'un échange de qubits sur lesquels est codée un information entraîne leur destruction et donc une nécessaire détection de l'attaque menée sur une transmission.

les tentatives d'interception des communications. Puisque la distribution quantique de clé fonde sa sécurité sur les principes supposément inviolables de la physique quantique et non sur un problème calculatoire, elle ne craint aucune attaque menée par un ordinateur, qu'il soit considéré classique ou quantique.

Il s'agit donc d'une méthode de cryptographie quantique, qui présente toutefois de nombreuses difficultés de mise en place ne rendant son utilisation universelle probable qu'à long terme.

Voici à quoi ressemblerait la transition quantique idéale :

1. Les communications sont chiffrées à l'aide d'un chiffrement classique. La cryptanalyse quantique, bien qu'elle dispose de ses algorithmes (Shor, Grover), ne représente pas une menace sans support physique adapté.

2. Grâce aux efforts de normalisation de la cryptographie post-quantique, les communications sont désormais chiffrées avec des algorithmes résistants aux attaques quantiques. Ces dernières n'ont pas encore vu le jour.

3. Les recherches menées en informatique quantique ont permis de construire un ordinateur quantique renfermant plus de 5000 qubits logiques et capable de déchiffrer RSA-2048. Toutes les communications effectuées depuis ces dernières années ayant été chiffrées à l'aide d'un algorithme de cryptographie post-quantique, elles restent sécurisées.

4. La cryptographie quantique est adoptée à l'échelle de la planète. Les attaques calculatoires comme celles menées par les ordinateurs quantiques sont inopérantes. La cryptologie a effectué sa transition quantique.

Il s'agit d'un schéma idéal d'une transition qui s'effectuera sur plusieurs décennies. Sa trajectoire sera probablement plus accidentée. Des scénarios moins réjouissants doivent également être envisagés, tels l'apparition prématurée de la cryptanalyse quantique ou la mise au point d'attaques compromettant l'ensemble des primitives post-quantiques.

3.1.2 L'enjeu de la normalisation post-quantique

Nous pouvons tirer de la partie 3.1.1 que la normalisation post-quantique constitue la clé de voûte d'une nécessaire transition quantique de la cryptographie. Il s'agit d'un rempart efficace face aux attaques quantiques qui renforcera le niveau général de protection

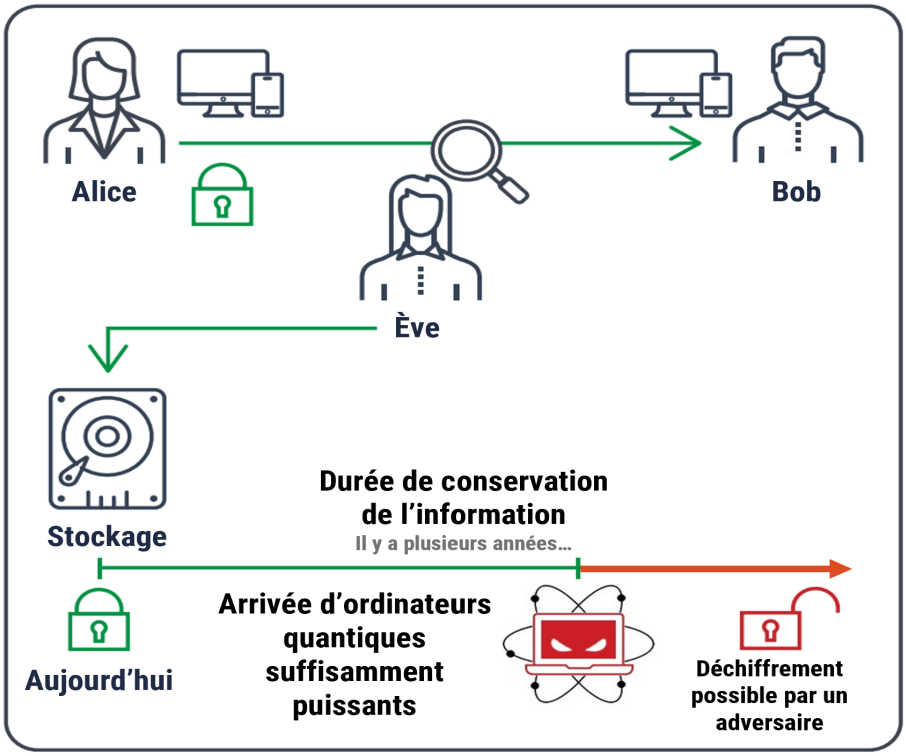

FIGURE 3.2 : Illustration d'une attaque du type « entreposer puis déchiffrer ».

Source : Centre canadien pour la cybersécurité

en vertu du principe de Kerckchoffs. Le chemin parcouru par la cryptographie classique montre à quel point la normalisation facilite l'adoption de solutions adaptées et sécurisées (*Advanced Encryption Standard, [NIST] ; Transport Layer Security [IETF]*). Les organismes de normalisation ont donc un rôle essentiel à jouer dans la protection de tous les utilisateurs des réseaux de communication de la planète.

Les enjeux principaux de cette tâche de normalisation seront comme souvent la dissémination des normes nouvellement établies ainsi que la dimension temporelle du processus. La normalisation dans des domaines en évolution rapide comme celui de l'informatique quantique obéit toujours à une contrainte temporelle importante. Dans le cas de la cryptanalyse quantique, celle-ci est renforcée par le risque d'une attaque du type « *store now, decrypt later* » (entreposer puis déchiffrer). La taille des infrastructures de stockage de données permet actuellement d'accumuler à peu de frais énormément de données interceptées confidentielles et qui le seront encore lors de l'avènement d'une cryptanalyse quantique. S'il ne sera pas possible de renforcer le chiffrement de données déjà interceptées, la mise en place dans les meilleurs délais d'un double chiffrement résistant aux attaques quantiques permettra de protéger énormément de données. Les experts en sécurité informatique considèrent les données en circulation sous un chiffrement classique comme déjà compromises du fait de leur probable stockage jusqu'à l'apparition d'un ordinateur quantique efficace.

Algorithmes sélectionnés en 2022		
Primitives employées	Échange de clés	Signature numérique
Réseaux euclidiens	CRYSTALS–Kyber	CRYSTALS-Dilithium FALCON
Fonctions de hachage		SPHINCS+

Algorithmes candidats pour la quatrième phase	
Primitives employées	Échange de clés
Codes correcteurs d'erreurs	BIKE Classic McEliece HQC
Courbes elliptiques supersingulières	SIKE (Cassé en août 2022)

Figure 3.3 : Synthèse de l'issue de la troisième phase de sélection. Les algorithmes sont classés selon leur fonction et le problème calculatoire sur lequel ils reposent.

3.1.3 Le déroulement de la normalisation post-quantique

Les premières recherches sur l'impact concret de l'informatique quantique sur les systèmes d'information remontent à 2001. Il a ensuite fallu attendre la publication du rapport NISTIR 8105 en avril 2016 dans lequel le NIST cite un chercheur prévoyant le déchiffrement de RSA par un ordinateur quantique pour 2030. Le NIST a ainsi lancé en décembre 2016 un appel à candidatures pour sélectionner les futurs algorithmes de cryptographie post-quantique. En juillet 2022, le NIST a annoncé la sélection d'un algorithme d'échange de clés et de trois algorithmes de signature numérique en vue d'une normalisation.

Avec la publication d'un premier projet de norme en août 2023, la normalisation des premiers algorithmes de cryptographie post-quantique aux États-Unis au niveau fédéral est désormais imminente. Le NIST, en tant que premier organisme national de normalisation au monde, joue un rôle évident dans l'adoption d'algorithmes et de normes par les autres pays. L'ANSSI devrait selon toute probabilité adopter ses propres normes en fonction de la décision du NIST peu de temps après ce dernier. L'ANSSI, consciente de la nécessité de normaliser au plus vite la cryptographie post-quantique afin d'accélérer son adoption, a annoncé en décembre 2023 son souhait de délivrer les premiers visas de sécurité français entre 2024 et 2025.[1]

3.2 Preuves de sécurité

3.2.1 Formaliser la sécurité

Avant de donner plus de détails sur les principales primitives cryptographiques post-quantiques, nous proposons de donner quelques notions de sécurité prouvable. Cette discipline vise à prouver, de manière formelle ou heuristique, la sécurité des primitives ou des fonctions face à divers niveaux d'attaques. Il n'est pas attendu des algorithmes cryptographiques qu'ils soient parfaitement sûrs face à un adversaire tout-puissant. La sécurité prouvable doit montrer que le coût nécessaire pour mener une attaque ayant une chance non négligeable de succès contre un algorithme cryptographique est exponentiel en fonction de la taille de la clé. Bien qu'objet de recherches théoriques, la sécurité prouvable s'intéresse à des attaques menées en pratique. La sécurité prouvable est généralement formalisée comme un jeu dans lequel s'affrontent un émetteur, un destinataire et un

[1] Agence nationale de la sécurité des systèmes d'information. *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)* [en ligne]. 2023.

adversaire (ou attaquant). L'objectif de l'émetteur est de transmettre son message secrètement, l'objectif de l'adversaire d'intercepter le contenu de ce message.

3.2.2 La notion d'indistinguabilité

L'indistinguabilité se formalise ainsi : un attaquant en possession de deux clairs m_0 et m_1 et de c, le chiffré de l'un des clairs, doit être incapable de deviner quel clair est à l'origine du chiffré. Il est ensuite possible de construire toutes sortes de scénarios pour mettre à l'épreuve l'indistinguabilité d'un algorithme. Dans le scénario de base, l'attaquant est considéré passif, c'est-à-dire qu'il n'a accès qu'à des informations publiques : il est libre de chiffrer les clairs de son choix avec l'algorithme et d'étudier le résultat pour mener son attaque. On appelle ce type d'attaques des attaques à clair choisi, ou CPA, de *chosen plaintext attack* en anglais. Un algorithme capable de garantir l'indistinguabilité face à de telles attaques est dit de sécurité IND-CPA[F01], pour indistinguabilité contre des attaques à clair choisi.

Les cryptologues sont allés plus loin en étudiant la possibilité où l'attaquant aurait accès à un oracle[F05] de déchiffrement, c'est-à-dire à la possibilité de déchiffrer tous les chiffrés de son choix. On appelle ce type d'attaques des attaques à chiffré choisi, ou CCA (*chosen cyphertext attacks*). Cette hypothèse mettait en péril tous les schémas précédents et a conduit à en construire de nouveaux. De nombreux schémas disposent désormais d'une sécurité IND-CCA, ou indistinguabilité contre des attaques à chiffré choisi.[1]

Pour simplifier, cette dernière constitue la preuve de sécurité la plus recherchée, de nos jours, pour les cryptosystèmes asymétriques. À ce titre, elle faisait partie des propriétés requises par le NIST dans son appel à candidatures pour la normalisation de mécanismes d'encapsulation de clé post-quantiques.[2]

3.3 Les algorithmes-candidats

Nous proposons dans cette dernière section de nous intéresser aux mécanismes d'encapsulation de clé sélectionnés par le NIST et qui feront l'objet soit d'une normalisation soit d'un réexamen au cours de la quatrième phase de sélection.

[1] Laguillaumie Fabien, Langlois Adeline, Stehlé Damien. Chiffrement avancé à partir du problème Learning With Errors. In *Informatique Mathématique : une photographie en 2014*. Presses universitaires de Perpignan, 2014.

[2] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2017. 25 p.

3.3.1 Les primitives basées sur les réseaux euclidiens

La cryptographie basée sur les réseaux euclidiens[F03], tout comme la cryptographie pré-quantique, repose sur des fonctions à trappe, c'est à dire des problèmes difficiles à résoudre (résolution virtuellement impossible en temps polynomial), et dont la résolution est facile lorsque l'on dispose d'une trappe (qui ne se retrouve qu'à l'aide de la clé privée). Si l'on reprend le schéma de la FIGURE 1.7, il s'agit des problèmes appartenant à NP (1), n'appartenant pas à BQP (2) et réductibles à P à condition de disposer de la clé privée (3). Ces problèmes sont évidemment difficiles à identifier, à modéliser et à mettre en œuvre dans des solutions cryptographiques.

Les réseaux euclidiens sont des structures mathématiques géométriques discrètes composées de points disposés à intervalles réguliers (on peut imaginer, par exemple, un maillage très régulier de tricot). Ces structures renferment plusieurs problèmes intéressants et calculatoirement difficiles comme celui du vecteur le plus court (*Shortest Vector Problem, SVP*). Le problème SVP consiste à trouver la distance la plus courte entre deux points. Triviale dans des réseaux de dimension 2 ou 3, la complexité du problème SVP augmente de manière exponentielle à mesure que la dimension n du réseau augmente, ce qui en fait un problème calculatoire difficile (classe NP). CRYSTALS–KYBER, l'algorithme sélectionné par le NIST, repose sur le problème de l'apprentissage avec erreurs[F04] (*Learning with errors* ou LWE) dans des réseaux ayant pour base une matrice structurée. Il existe une réduction qui prouve que le problème LWE et ses variantes structurées Polynomial-LWE, Ring-LWE et Module-LWE sont au moins aussi difficiles à résoudre que le problème SVP.[1] Le problème LWE se pose dans les termes suivants : soient $\mathbf{A}$ une matrice publique et $\mathbf{s}$ un vecteur secret. Si l'on connaît suffisamment de vecteurs $\mathbf{a} \in \mathbf{A}$ et de produits scalaires $\langle \mathbf{a}, \mathbf{s} \rangle$, retrouver $\mathbf{s}$ étant donné $(\mathbf{A}, \mathbf{As})$ à l'aide de pivots de Gauss est un problème qui se résout efficacement en temps polynomial. LWE est rendu difficile par l'ajout d'un terme d'erreur $\mathbf{e}$ échantillonné aléatoirement à partir d'une distribution précise puis intégré à l'équation. Trouver $\mathbf{s}$ étant donné $(\mathbf{A}, \mathbf{As} + \mathbf{e})$ peut-être aisé, difficile ou pratiquement impossible selon la distribution à partir de laquelle $\mathbf{e}$ est échantillonné. Aucun algorithme quantique connu ne permet de retrouver le vecteur secret $\mathbf{s}$ en temps polynomial, ce qui fait de LWE un problème très intéressant pour la cryptographie post-quantique. C'est sur ce dernier que repose CRYSTALS–KYBER, destiné à devenir la première norme cryptographique post-quantique normalisée par le NIST.

[1] REGEV Oded. *On lattices, learning with errors, random linear codes, and cryptography.* 2005.

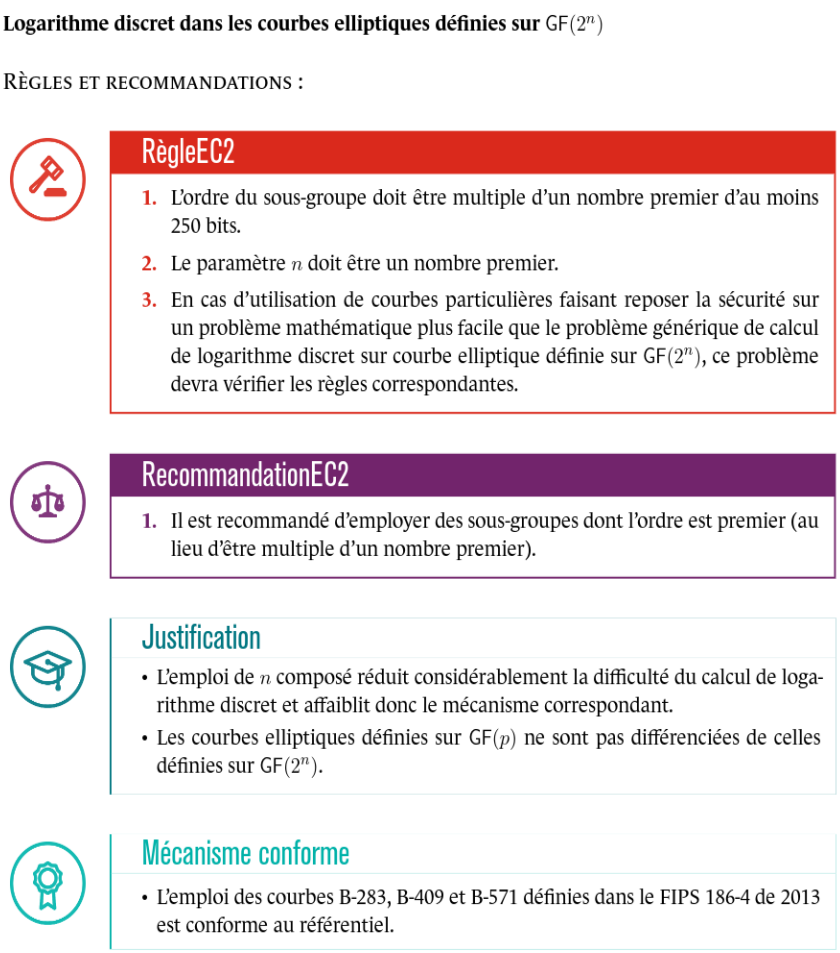

FIGURE 3.4 : Recommandations de l'ANSSI concernant la mise en œuvre d'un système de cryptographie asymétrique reposant sur le logarithme discret dans les courbes elliptiques. Le document fait référence à la publication FIPS 186-4 du NIST qui spécifie les algorithmes à utiliser.

Source : Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques*. Paris, 2021.

3.3.2 Les primitives basées sur les codes correcteurs d'erreurs

Il est possible de circonscrire une seconde famille de primitives cryptographiques qui reposent cette fois-ci sur les codes correcteurs d'erreur. Un code correcteur d'erreur désigne une technique de codage destinée à corriger les erreurs de transmission d'une information au moyen d'un canal peu fiable. La représentation la plus simple de ce principe réside dans le code des aviateurs, qui préfèrent employer la séquence Alpha Tango Charlie à place de la séquence A T C en raison des ajouts permettant de retrouver la séquence originale même en cas de dégradation de l'information. La redondance est un critère important des codes correcteurs d'erreur : reconnaître un schéma qui se répète permet de facilement retrouver la donnée d'origine. Nous nous intéresserons ici particulièrement au cryptosystème McEliece, qui fait partie des candidats qualifiés pour la quatrième phase de la sélection. Relativement ancien, ce système a été mis au point par Robert McEliece en 1978. Il exploite certaines propriétés d'un type particulier de codes algébriques, les codes de Goppa (dont nous ne détaillerons pas ici les spécificités). Le système consiste à masquer le message en lui ajoutant le plus d'erreurs possible, tout en laissant ouverte la possibilité d'une correction par une personne en possession de la bonne méthode de correction. Si la méthode d'encodage est correctement conçue, elle ne laisse aucun indice sur la méthode de décodage. On retrouve, une fois de plus, la clé publique et la clé privée caractéristiques des cryptosystèmes asymétriques.

Ce système n'a pas vraiment connu d'engouement à sa sortie du fait de la longueur de ses clés, qui sont de grandes matrices. La clé publique a une longueur de 2^{19} bits soit 64 Kio. S'il s'agissait d'un facteur particulièrement limitant à l'époque de la publication du cryptosystème, il l'est moins aujourd'hui. La sécurité des cryptosystèmes à l'heure de l'informatique quantique est liée à leur proximité avec les problèmes qui ne peuvent être résolus en temps polynomial, comme RSA ou Diffie-Hellman. Puisque très éloigné des problèmes calculatoires qui sous-tendent les algorithmes asymétriques usuels, Classic McEliece est à l'abri d'une éventuelle percée technologique dans la factorisation des entiers permise par l'ordinateur quantique. C'est cette propriété qui conduit à nouveau les chercheurs en cryptologie à s'intéresser à McEliece, au point d'en faire un des prochains candidats à la normalisation par le NIST. D'autres primitives reposant sur les codes correcteurs d'erreurs ont depuis été mises au point, telles BIKE et HQC, toujours candidates à la normalisation.

Conclusion

Loin d'épouser les postures alarmistes de certains acteurs du milieu, la cryptologie a tout de même trouvé un consensus au sujet de la cryptanalyse quantique : cette dernière constitue une menace importante pour tous les utilisateurs des réseaux de communication. C'est dans cette optique que les laboratoires du monde entier se sont lancés à la recherche d'un algorithme le plus sûr possible tout en étant léger et facile à déployer à l'échelle mondiale. Cette adoption universelle est un enjeu majeur de la transition vers la cryptographie post-quantique. Pareille à un vaccin, cette solution doit être utilisée par toute la chaîne de transmission des informations sans quoi ces dernières courront toujours le risque d'être interceptées et déchiffrées.

La normalisation prend ici le relai de la recherche. Une fois les algorithmes développés, éprouvés et attaqués de toutes parts pour essayer d'y déceler des failles de sécurité, ils doivent être assortis de dispositions adaptées quant à leur mise en œuvre concrète. Ces dispositions ne doivent pas trop différer d'une région ou d'un secteur à l'autre, sous peine de condamner la compatibilité des données échangées. Internet tire sa force d'une interopérabiité quasi immédiate, fruit du respect par tous les utilisateurs de la chaîne de normes et de protocoles savamment élaborés et déployés par des organismes au rôle devenu critique au fil des années. Dans le cas de la normalisation de la cryptographie post-quantique, le NIST est à la manœuvre et les organismes nationaux de sécurité des systèmes d'information devraient selon toute probabilité se ranger derrière les normes à paraître en 2024.

La normalisation des protocoles internet n'est pas seulement technique. Si les algorithmes et les protocoles ne sont écrits que dans des langages de programmation élaborés à partir de l'anglais, ce n'est pas le cas des normes qui encadrent leur mise en œuvre. La traduction constitue un enjeu majeur pour la dissémination des normes et des protocoles. Ceux-ci doivent être rédigés dans le plus de langues possible et dans un langage clair, simple, sans ambiguïtés. La terminologique qu'ils mobilisent doit être correctement construite et traduite. De plus, la prise en main de la cryptographie post-quantique par un laboratoire américain doit nécessairement interroger les terminologues français. Si la France est dotée depuis décembre 2022 d'un lexique normalisé pour l'informatique quantique, grâce aux travaux de la Commission d'enrichissement de la langue française, il apparaît nécessaire de poursuivre la veille terminologique dans les sous-domaines ouverts par ce champ de recherches tels la cryptographie post-quantique.

Deuxième partie

Texte-support et sa traduction

Avertissement au lecteur

Dans la partie qui suit, le texte source (en anglais) est présenté sur la page de gauche et sa traduction (en français) sur la page de droite. Les passages faisant l'objet d'une explication dans la troisième partie (stratégies de traduction) sont surlignés dans le texte-support et dans sa traduction. Les termes faisant l'objet d'une fiche terminologique sont encadrés dans le texte-support et dans sa traduction, ceux figurant dans le glossaire sont soulignés dans le texte-support et dans sa traduction.

Seules quelques unes des références bibliographiques mentionnées dans le texte-source sont reportées et *adaptées*, pour des raisons de concision et afin d'éviter un encombrement suscpetibles de gêner la lecture. Les choix relatifs à cette bibliographie sont détaillés au point 3.1.1 de la stratégie de traduction.

Références du texte-support

Alagic Gorjan, Apon Daniel, Cooper David et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/ Internal Report (NISTIR), National Institute of Standards and Technology, 2022. pp. 1-2, pp. 5-7, pp. 27-29.

Caractéristiques du texte-source : 3711 mots, 20 427 signes
Caractéristiques du texte-cible : 4474 mots, 24 849 signes

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

1. Introduction

Over the past several years, there has been steady progress toward building quantum computers. The security of many commonly used public-key cryptosystems would be at risk if large-scale quantum computers were ever realized. In particular, this would include key-establishment schemes and digital signatures that are based on factoring, discrete logarithms, and elliptic curve cryptography. In contrast, symmetric cryptographic primitives, such as block ciphers and hash functions, would not be as drastically impacted. As a result, there has been intensified research into finding public-key cryptosystems that would be secure against adversaries with both quantum and classical computers. This field is often referred to as *post-quantum cryptography* (PQC), or sometimes quantum-resistant cryptography. The goal is to develop schemes that can be deployed in existing communication networks and protocols without significant modifications.

In response, the National Institute of Standards and Technology (NIST) initiated a public, competition-like process to select quantum-resistant public-key cryptographic algorithms. The new public-key cryptography standards will specify algorithms for digital signatures, public-key encryption, and key establishment. The new standards will augment Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS)[1], Special Publication (SP) 800-56A Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [2], and SP 800-56B Revision 2, *Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography* [3]. It is intended that these algorithms will be capable of protecting sensitive U.S. Government information well into the foreseeable future, including after the advent of quantum computers. The process will be referred to as the NIST Post-Quantum Cryptography Standardization Process hereafter in this document.

Rapport sur l'état d'avancement de la troisième phase du processus de normalisation de la cryptographie post-quantique par le NIST

1. Introduction

Ces dernières années ont été marquées par des progrès réguliers vers l'avènement de l'ordinateur quantique. La construction d'un ordinateur quantique de grande taille est susceptible de compromettre la sécurité de nombreux cryptosystèmes à clé publique parmi les plus utilisés. Les mécanismes d'établissement de clé et de signature numérique reposant sur les problèmes de la factorisation de grands entiers et du logarithme discret sur un corps fini ou sur courbe elliptique sont notamment concernés. À l'inverse, l'impact sur les primitives cryptographiques symétriques telles que le chiffrement par blocs et les fonctions de hachage devrait rester limité. Des recherches approfondies ont été menées afin de mettre au point des cryptosystèmes conjecturés sûrs face à des adversaires dotés à la fois d'ordinateurs classiques et quantiques. Ce domaine est généralement désigné sous le nom de *cryptographie post-quantique* (CPQ) et parfois de cryptographie résistante aux attaques des ordinateurs quantiques. La CPQ vise à élaborer des systèmes pouvant être intégrés aux réseaux et aux protocoles de communication existants sans avoir à modifier ces derniers de manière significative.

En réponse, le National Institute of Standards and Technology (NIST) a lancé une campagne publique sous forme de compétition en vue de sélectionner des algorithmes de cryptographie à clé publique résistants aux attaques quantiques. Les nouvelles normes en matière de cryptographie asymétrique définiront des algorithmes de signature numérique, de chiffrement asymétrique et d'établissement de clé. Ces nouvelles normes viendront s'ajouter aux normes FIPS186-4[1], SP800-56A[2] et SP800-56B[3]. Ces algorithmes seront destinés à protéger les données confidentielles des institutions fédérales des États-Unis dans un avenir proche, notamment à l'aune de l'avènement de l'ordinateur quantique. Cette campagne de normalisation sera désignée ci-après sous le nom de processus de normalisation de la cryptographie post-quantique par le NIST.

[1]National Institute of Standards and Technology. *FIPS PUB 186-4 : Digital Signature Standard (DSS)*. 2013.

[2]National Institute of Standards and Technology. *SP800-56A Rev. 3 : Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. 2018.

[3]National Institute of Standards and Technology. *SP 800-56B Rev. 2 : Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. 2019.

NIST issued a public call for submissions to the PQC Standardization Process in December 2016 [4]. Prior to the November 2017 deadline a total of 82 candidate algorithms were submitted. Shortly thereafter, the 69 candidates that met both the submission requirements and the minimum acceptability criteria were accepted into the first round of the standardization process. Submission packages for the first-round candidates were posted online for public review and comment [5].

After a year-long review of the candidates, NIST selected 26 algorithms to move on to the second round of evaluation in January 2019 [6]. These algorithms were viewed as the most promising candidates for eventual standardization, and were selected based on both internal analysis and public feedback. During the second round, there was continued evaluation by NIST and the broader cryptographic community. After careful deliberation, NIST selected seven finalists and eight alternates to move on to the third round in July 2020 [7]. NIST's intent was to standardize a small number of the finalists at the end of the third round, as well as a small number of the alternate candidates after a fourth round.

The third round began in July 2020 and continued for approximately 18 months. During the third round, there was a more thorough analysis of the theoretical and empirical evidence used to justify the security of the candidates. There was also careful benchmarking of their performance using optimized implementations on a variety of software and hardware platforms. Similar to the first two rounds, NIST also held the (virtual) Third NIST PQC Standardization Conference in June 2021. Each of the finalists and alternates were invited to present an update on their candidate algorithm. In addition, several researchers presented work that was relevant to the PQC standardization process.

En décembre 2016, le NIST a appelé à soumettre des candidatures au processus de normalisation de la cryptographie post-quantique [4]. Quatre-vingt-deux algorithmes candidats ont été proposés avant la date butoir fixée en novembre 2017. Une fois les conditions de soumission et les critères minimums d'acceptabilité vérifiés, 69 d'entre eux ont été sélectionnés pour participer à la première étape du processus de normalisation. Les dossiers soumis au NIST pour cette première étape ont été publiés en ligne afin de faire l'objet d'un examen public et de recueillir des commentaires [5].

Au terme d'un an d'examen, le NIST a sélectionné en janvier 2019 les 26 algorithmes qualifiés pour la deuxième étape de l'évaluation [6]. Ces algorithmes sélectionnés sur la base d'analyses menées par les équipes du NIST et des retours de la communauté scientifique constituaient alors les candidats à la normalisation les plus prometteurs. L'examen détaillé par le NIST et par l'ensemble de la communauté de la cryptographie s'est poursuivi au cours de la deuxième étape. En juillet 2020, sept finalistes et huit algorithmes alternatifs ont été qualifiés pour la troisième étape après une délibération minutieuse. Le NIST avait pour objectif la normalisation d'une poignée de finalistes à la fin de la troisième étape ainsi que de quelques algorithmes alternatifs à l'issue d'une quatrième étape.

La troisième étape a débuté en juillet 2020 pour une durée estimée à 18 mois. Cette étape a donné lieu à une analyse approfondie des démonstrations théoriques et des données empiriques employées pour justifier de la sécurité des algorithmes candidats. Les performances des algorithmes ont fait l'objet d'une évaluation minutieuse à l'aide de mises en œuvre optimisées sur divers supports logiciels et matériels. Comme pour les deux premières étapes, une troisième conférence sur la normalisation post-quantique par le NIST a été organisée et s'est tenue en ligne en juin 2021. Les équipes derrière chaque algorithme finaliste ou alternatif ont eu l'occasion d'y présenter les dernières avancées réalisées sur leur algorithme candidat. Plusieurs chercheurs ont également pu y présenter des travaux concernant le processus de normalisation de la CPQ.

After three rounds of evaluation and analysis, NIST has selected the first algorithms it will standardize as a result of the PQC Standardization Process. The public-key encapsulation mechanism (KEM)[F02] that will be standardized is CRYSTALS–Kyber. The digital signatures that will be standardized are CRYSTALS–Dilithium, Falcon, and SPHINCS$^+$. While there are multiple signature algorithms selected, NIST recommends CRYSTALS–Dilithium as the primary algorithm to be implemented. In addition, four of the alternate KEM[F02] candidate algorithms will advance to a fourth round of evaluation : BIKE, Classic McEliece, HQC, and SIKE. These candidates will be considered for future standardization at the conclusion of the fourth round.

Table 1 shows a timeline of major events with respect to the NIST PQC Standardization Process to date.

2.2 Evaluation Criteria

NIST's Call for Proposals identified three broad aspects of the evaluation criteria that would be used to compare candidate algorithms throughout the NIST PQC Standardization Process : 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. These criteria are described below, along with a discussion of how they impacted the third-round candidate evaluations.

2.2.1 Security

As was the case for the past Advanced Encryption Standard (AES) and Secure Hash Algorithm 3 (SHA-3) competitions, security is the most important criterion that NIST uses when evaluating candidate post-quantum algorithms. NIST's public-key standards are currently utilized in a wide variety of applications, including internet protocols like TLS, SSH, IKE, IPsec, and DNSSEC, as well as for certificates, software code signing, and secure bootloaders. The new NIST public-key standards will provide post-quantum security for each of these applications.

Après trois étapes d'évaluation et d'analyse, le NIST a sélectionné les premiers algorithmes qui vont devenir des normes à l'issue du processus de normalisation de la CPQ. Le premier mécanisme d'encapsulation de clé[F02] normalisé sera CRYSTALS–Kyber. Les mécanismes de signature numérique normalisés seront CRYSTALS-Dilithium, Falcon et SPHINCS$^+$. Si plusieurs algorithmes de signature numérique ont été sélectionnés, le NIST recommande en priorité la mise en œuvre de l'algorithme CRYSTALS-Dilithium. Quatre des algorithmes candidats alternatifs d'encapsulation de clé prendront part à une quatrième étape de sélection : BIKE, Classic McEliece, HQC et SIKE. La future normalisation de ces candidats sera envisagée ou non à l'issue de cette quatrième étape.

Une chronologie du déroulement du processus de normalisation de la CPQ par le NIST jusqu'à ce jour figure dans le tableau 1.

2.2 Critères d'évaluation

L'appel à candidatures du NIST mettait en avant trois grands aspects parmi les critères sur lesquels les algorithmes seraient évalués et comparés au cours du processus de normalisation de la CPQ par le NIST : 1) leur sécurité, 2) leur coût et leurs performances, 3) les caractéristiques des algorithmes et de leur mise en œuvre. Ces critères sont décrits ci-dessous. Leur impact sur l'évaluation des algorithmes candidats au cours de la troisième étape est également étudié.

2.2.1 Sécurité

Comme lors des compétitions destinées à sélectionner l'Advanced Encryption Standard (AES) et le Secure Hash Algorithm 3 (SHA-3), le NIST a choisi la sécurité comme critère principal d'évaluation des algorithmes post-quantiques candidats. Les normes du NIST en matière de cryptographie à clé publique trouvent actuellement de très nombreuses applications : protocoles internet (TLS, SSH, IKE, Ipsec et DNSSEC), certificats, signature de code pour les logiciels et programmes d'amorçage sécurisés. Les nouvelles normes du NIST en matière de cryptographie asymétrique offriront un niveau de sécurité post-quantique à l'ensemble de ces applications.

For the purpose of quantifying the security of candidate algorithms, NIST gave three possible security definitions—two for encryption and one for signatures. NIST also designated five security strength categories for classifying the computational complexity of attacks that violate the security definitions (see [9]).

NIST also mentioned other desirable security properties, such as forward secrecy, resistance to side-channel and multi-key attacks, and resistance to misuse, all of which continue to be of interest. In some cases, NIST has encouraged submitters to make minor tweaks to provide or enhance these additional desirable security properties (e.g., by adding a public salt to ciphertexts to avoid multi-target attacks against KEMs[F02]).

For general-use encryption and key-establishment schemes, the Call for Proposals [9] asked for "semantically secure" schemes with respect to adaptive chosen ciphertext attack (equivalently, IND-CCA2 security). For ephemeral use cases, NIST also accepted algorithms that provided semantic security with respect to chosen plaintext attack (equivalently, IND-CPA security[F01]). IND-CCA2 security is not required in strictly ephemeral use cases and attempting to meet the more stringent requirements of IND-CCA2 security may incur significant performance penalties for some schemes. Digital signature schemes were required to provide existentially unforgeable signatures with respect to an adaptive chosen message attack (EUF-CMA security). Submitters were encouraged but not required to provide proofs of security in relevant models.

The five security strength categories defined in [9] were based on the computational resources required to perform certain brute-force attacks against the existing NIST standards for AES and SHA in a variety of different models of the cost of computation, both classical and quantum. In some cases, questions have arisen regarding whether various parameter sets meet their claimed security strength categories. The uncertainty arises principally from two distinct considerations.

Afin de quantifier le niveau de sécurité des algorithmes candidats, le NIST s'est doté de trois définitions possibles de la notion de sécurité : deux pour le chiffrement et une pour les signatures numériques. Le NIST a ensuite imaginé cinq niveaux de sécurité permettant de classer la complexité calculatoire des attaques nécessaires pour compromettre les notions de sécurité susmentionnées (voir [9]).

Le NIST a mentionné d'autres caractéristiques souhaitables en matière de sécurité, telles que la confidentialité persistante, la résistance aux attaques par canaux auxiliaires ou par clés apparentées et la résistance aux utilisations incorrectes. Toutes font encore l'objet de recherches. Dans certains cas, le NIST a encouragé les équipes candidates à modifier légèrement leurs algorithmes afin de présenter ces caractéristiques souhaitables supplémentaires ou de les améliorer, le cas échéant (par exemple, par l'ajout de données aléatoires publiques aux textes chiffrés pour prévenir les attaques multi-cibles contre des mécanismes d'encapsulation de clé[F02]).

Concernant le chiffrement d'usage général et les mécanismes d'encapsulation de clé[F02], l'appel à candidatures requérait des mécanismes « sémantiquement sûrs » face à une attaque adaptative à chiffré choisi (équivalent à une sécurité IND-CCA2). Le NIST a également accepté des algorithmes sémantiquement sûrs face à une attaque à texte clair choisi (équivalent à une sécurité IND-CPA[F01]), pour une utilisation strictement éphémère. La sécurité IND-CCA2 n'est pas requise pour une utilisation strictement éphémère. Pour certains mécanismes, satisfaire aux exigences plus strictes de la sécurité IND-CCA2 est susceptible d'entraîner une baisse considérable des performances. Les mécanismes de signature numérique devaient eux fournir des signatures avec une résistance aux contrefaçons existentielles face à une attaque adaptative à message choisi (niveau de sécurité EUF-CMA). Les équipes candidates ont été encouragées à fournir des preuves de sécurité pour les modèles concernés, sans toutefois y être tenues.

Les cinq niveaux de sécurité définis dans le document [9] ont été définis en fonction de la puissance de calcul nécessaire pour mener une attaque par force brute contre une des normes NIST actuelles, AES ou SHA, le coût des calculs et la technologie employée (classique ou quantique) variant selon les modèles. Certains cas ont soulevé des interrogations quant à la conformité de certains jeux de paramètres avec les niveaux de sécurité visés par ces derniers. Ces interrogations découlent de deux considérations distinctes.

First, the NIST security strength categories are defined in a way that leaves open the relative cost of various computational resources, including quantum gates, classical gates, quantum memory, classical memory, hardware, energy, and time. The idea is that in order to meet, for example, category 1, the best attack violating the security definition of a parameter set should cost more than a brute-force key search attack on a single instance of AES-128, according to any plausible assumption regarding the relative cost of the various computational resources involved in a real-world attack. Different opinions can therefore arise regarding what constitutes a plausible assumption regarding the relative cost of computational resources.

Second, even if one has agreed upon a model or a range of models for evaluating the relative cost of various computational resources, there may still be uncertainty how much of a given resource an attack actually requires. For example, many parameters of lattice reduction attacks (such as the BKZ block size, the number of required BKZ iterations, or the number of dimensions for free) are not proven optimal values but rather heuristic estimates based on simplified models, simulations, and mathematical conjectures. Additionally, while some submitters have rightly observed that many widely used cost models, such as the RAM model, underestimate the difficulty of certain memory intensive attacks, the comparative lack of published cryptanalysis using more realistic models may bring into question whether sufficient effort has been made to optimize the best-known attacks to perform well in these models.

Submitters were asked to provide a preliminary classification of all proposed parameter sets according to the definitions of the five security strength categories. While category 1, 2, and 3 parameters were (and continue to be) the most important targets for NIST's evaluation, NIST nevertheless strongly encouraged the submitters to provide at least one parameter set that meets category 5. Aside from NTRU, all of the third-round submission packages contained parameters that claimed to meet category 5. In June 2021, at NIST's request, the NTRU team announced parameters designed to meet category 5 given the state of the art in lattice cryptanalysis [10].

Premièrement, la définition des cinq niveaux de sécurité du NIST laisse ouverte la question du coût relatif des diverses ressources : nombre de portes quantiques ou classiques, quantité de mémoire quantique ou classique, quantité de matériel informatique, énergie consommée et temps nécessaire au calcul. Par exemple, pour qu'un jeu de paramètres atteigne le niveau 1, la meilleure attaque compromettant sa sécurité doit coûter plus cher qu'une attaque par force brute contre une instance d'AES-128, en tenant compte de toutes les hypothèses plausibles quant au coût relatif des ressources de calcul nécessaires pour réellement mener cette attaque. Les points de vue sur ce qui constitue ou non une hypothèse plausible quant au coût relatif des ressources nécessaires au calcul peuvent par conséquent diverger.

Ensuite, se mettre d'accord sur un modèle ou un ensemble de modèles pour évaluer le coût des diverses ressources nécessaires au calcul n'élimine pas toutes les incertitudes quant à la quantité d'une ressource donnée réellement requise pour mener une attaque. Ainsi, de nombreux paramètres des attaques par réductions de réseaux (comme la taille du bloc BKZ, le nombre d'itérations de l'algorithme BKZ nécessaires ou le nombre de dimensions gratuites) ne prennent pas des valeurs démontrées optimales, mais des estimations heuristiques reposant sur des modèles simplifiés, des simulations et des conjectures mathématiques. Certaines équipes candidates ont observé, à juste titre, que de nombreux modèles couramment utilisés pour calculer les coûts, le modèle RAM par exemple, sous-estiment la difficulté de certaines attaques nécessitant une mémoire importante. De plus, le faible nombre de cryptanalyses publiées s'appuyant sur des modèles plus réalistes pose la question suivante : des efforts suffisants ont-ils été déployés pour optimiser les meilleures attaques disponibles à ce jour dans ces modèles ?

Les équipes candidates ont été invitées à ranger de manière préliminaire tous leurs jeux de paramètres dans les cinq niveaux de sécurité définis au préalable. Si les paramètres satisfaisant les niveaux de sécurité 1, 2 et 3 ont été et seront toujours examinés en priorité, le NIST a tout de même fortement encouragé les candidats à soumettre au moins un jeu de paramètres remplissant les exigences du niveau 5. Hormis NTRU, tous les dossiers soumis pour la troisième étape d'évaluation contenaient des paramètres visant à satisfaire les exigences du niveau 5. En juin 2021 et sur demande du NIST, l'équipe NTRU a annoncé la publication de paramètres conformes au niveau 5 tenant compte des derniers progrès en cryptanalyse basée sur les réseaux euclidiens [10].

During the first, second, and third rounds of the NIST standardization process, a number of cryptanalytic results dramatically reduced the security assumed for some submitted schemes and undermined NIST's confidence in the maturity of others. These results were the basis for many of NIST's decisions thus far in the process, particularly for Rainbow and GeMSS [11–13]. Cryptanalysis has also brought some of the candidates' security category claims into question or shown them to be false. In response, NIST may move some parameter sets down to a lower category (or refrain from standardizing them) if warranted.

Progress was also made in clarifying some outstanding security questions during the third round. In lattice-based cryptography[F03], methods were developed to replace the asymptotic security estimates represented by the core SVP methodology with concrete security estimates expressed as a gate count that can be more directly compared with security estimates for the non-lattice candidates (see [14, 15], as well as discussion on the pqc-forum [16]). Several of the finalists have also been implemented with countermeasures to side-channel attacks (see Section 2.2.3). Additionally, further investigations have been performed to determine whether the BIKE submission's estimate of its decryption failure rate is accurate enough to justify a claim of IND-CCA2 security [17, 18].

NIST continues to see diversity of computational hardness assumptions as an important long-term security goal for its standards. NIST will standardize practically efficient schemes from different families of cryptosystems to reduce the risk that a single breakthrough in cryptanalysis will leave the world without a viable standard for either key-establishment or digital signatures. Nonetheless, NIST does not feel the need to establish these standards all at once but will rather prioritize those schemes that seem closest to being ready for standardization and wide adoption. NIST feels that this strategy balances the desire for diversity with the need for all standards to be thoroughly vetted before they are released.

Au cours de la première, de la deuxième et de la troisième étape du processus de normalisation par le NIST, un certain nombre d'avancées en matière de cryptanalyse ont entraîné une réduction importante de la sécurité présumée de certains mécanismes et ébranlé la confiance du NIST dans la maturité des autres. Ces avancées sont à l'origine de nombreuses décisions du NIST jusqu'à maintenant, notamment concernant Rainbow et GeMSS [11–13]. La cryptanalyse a également remis en question le niveau de sécurité visé par certains candidats, voire l'a contredit. Certains jeux de paramètres peuvent donc être rétrogradés au niveau de sécurité inférieur (ou ne pas être normalisés) par le NIST si la situation le justifie.

La troisième étape a permis de mieux éclaircir certaines questions de sécurité laissées en suspens. En matière de cryptographie basée sur les réseaux euclidiens[F03], des méthodes ont été imaginées pour remplacer les estimations de sécurité asymptotiques obtenues à l'aide de la méthodologie CoreSVP par des estimations de sécurité concrètes exprimées en nombre de portes directement comparables avec celles des candidats reposant sur d'autres problèmes (voir [14], [15], et le fil de discussion sur le forum consacré à la cpq [16]). Plusieurs algorithmes finalistes ont été mis en œuvre accompagnés de mesures de protection contre les attaques par canaux auxiliaires (voir section 2.2.3). Enfin, des recherches ont été menées afin de déterminer si l'estimation du taux d'échec de déchiffrement de BIKE était suffisamment précise pour justifier un niveau de sécurité IND-CCA2 [17, 18].

Le NIST conçoit toujours la diversité des hypothèses de complexité calculatoire comme une composante essentielle de la sécurité de ses normes à long terme. Le NIST prendra le soin de normaliser des mécanismes efficaces en pratique issus de différentes familles de cryptosystèmes afin de réduire le risque qu'une percée majeure de la cryptanalyse ne laisse le monde dépourvu de la moindre norme fiable relative à l'encapsulation de clés et à la signature numérique. Le NIST n'estime cependant pas nécessaire de publier toutes ces normes à la fois, se concentrant plutôt sur la normalisation prioritaire des mécanismes les plus aboutis et prêts à être adoptés par le plus grand nombre. D'après le NIST, cette stratégie offre un équilibre entre la recherche de diversité et la nécessité d'examiner minutieusement chaque norme avant de la publier.

4.1.1 CRYSTALS-Kyber

KYBER is a module learning with errors[F04] (MLWE)-based key encapsulation mechanism[F02] with its original design presented in [180]. As compared to similar schemes based on unstructured LWE[F04], this design offers significant efficiency advantages.

Design. Like other LWE[F04]-style KEM[F02] candidates in the third round, KYBER is constructed first as an IND-CPA-secure[F01] PKE scheme, then boosted to an IND-CCA-secure KEM[F02] by a Fujisaki-Okomoto (FO) type of transform [170].

The base PKE scheme is derived from the MLWE problem. The ring is a cyclotomic power-of-2 ring, $R = \mathbb{Z}[X]/(X^{256} + 1)$, and the module rank k is set to $k = 2$, 3 or 4 (corresponding to security categories 1, 3, 5). Other parameters include the integer modulus $q = 3329$, a distribution $\boldsymbol{\chi}$ on "short" polynomials of R_q, and a public matrix of polynomials $\mathbf{A} \in R_q^{k \times k}$ pseudorandomly generated from a uniformly random 256-bit string. Two secret vectors of polynomials $\mathbf{s}$,$\mathbf{e} \in R_q^k$ are sampled independently from $\boldsymbol{\chi}$ coefficient-wise. The vector $\mathbf{s}$ is regarded as the secret key, and the vector $\mathbf{e}$ is called the error term. This forms the MLWE public key $pk := (\mathbf{A}, \mathbf{b}) := (\mathbf{A}, \mathbf{As}+\mathbf{e})$.

Encryption and decryption instantiate the Lindner-Peikert paradigm [181]. To encrypt a message m (a 256-bit string), one samples two vectors of polynomials $\mathbf{r}$, $\mathbf{e}_1 \in R_q^k$ as well as a polynomial $e_2 \in R_q$, with all coefficients of each polynomial chosen independently from $\boldsymbol{\chi}$. Then, the ciphertext c is formed as

$$c := (c1, c2) := \left(\mathbf{rA} + \mathbf{e_1}, \mathbf{rb} + e_2 + \left\lceil \frac{q}{2} \right\rfloor \cdot m\right) \in R_q^k \times R_q,$$

4.1.1 CRYSTALS-Kyber

Le mécanisme d'encapsulation de clé[F02] KYBER repose sur le problème de l'apprentissage avec erreurs[F04] dans les modules de réseaux euclidiens (module learning with errors, MLWE). L'architecture d'origine du mécanisme est présentée dans l'article [180]. Par rapport à des mécanismes similaires reposant sur LWE[F04] dans des réseaux non structurés, cette architecture présente des avantages significatifs en termes d'efficacité.

Architecture. Comme les autres mécanismes d'encapsulation de clé[F02] qualifiés pour la troisième étape et reposant sur le problème LWE[F04], KYBER est d'abord construit comme un mécanisme de chiffrement asymétrique IND-CPA[F01] puis rendu IND-CCA par une transformation de type Fujisaki-Okamoto (FO) [170].

Le mécanisme de chiffrement asymétrique repose d'abord sur le problème MLWE. Soient $R = \mathbb{Z}[X]/(X^{256}+1)$ un anneau cyclotomique de puissances de 2 et k le rang du module. Celui-ci est fixé à $k = 2, 3$ ou 4 pour un niveau de sécurité de respectivement 1, 3 ou 5. Soient $q = 3329$ le module entier, $\boldsymbol{\chi}$ une loi de probabilité sur les polynômes « courts » de R_q et $\mathbf{A} \in R_q^{k\times k}$ une matrice publique de polynômes générés de manière pseudo-aléatoire à partir d'une chaîne de caractères uniformément aléatoire de 256 bits les autres paramètres. Un échantillonnage indépendant coefficient par coefficient suivant $\boldsymbol{\chi}$ permet d'obtenir les deux vecteurs secrets de polynômes $\mathbf{s}$,$\mathbf{e} \in R_q^k$. Le vecteur $\mathbf{s}$ constitue la clé secrète, le vecteur $\mathbf{e}$ le terme d'erreur. D'où la clé publique MLWE

$$pk := (\mathbf{A},\, \mathbf{b}) := (\mathbf{A},\, \mathbf{As}{+}\mathbf{e}).$$

Le chiffrement et le déchiffrement instancient le cryptosystème de Lindner-Peikert [181]. Le chiffrement d'un message m (une chaîne de caractères de 256 bits) nécessite d'échantillonner deux vecteurs de polynômes $\mathbf{r}$, $\mathbf{e}_1 \in R_q^k$ ainsi qu'un polynôme $e_2 \in R_q$, les coefficients de chaque polynôme étant choisis indépendamment suivant $\boldsymbol{\chi}$. Le chiffré c obtenu s'exprime

$$c := (c1, c2) := \left(\mathbf{rA} + \mathbf{e_1}, \mathbf{rb} + e_2 + \left\lceil \frac{q}{2} \right\rfloor \cdot m\right) \in R_q^k \times R_q,$$

where $\lceil \frac{q}{2} \rfloor \cdot m$ should be interpreted in the natural way – as the vector of coefficients of a single polynomial in R_q (with padding as needed). In the actual KYBER PKE scheme, some of the low-order bits of the ciphertexts are discarded; that is, the ciphertexts are "compressed" in a precise way.

To decrypt a ciphertext c using the secret key $\mathbf{s}$, after first "decompressing" the ciphertext, one computes the intermediate value $v = c_2 - \mathbf{c_1 s}$ then rounds each coefficient of the polynomial v modulo 2 to extract the transmitted bit-string m.

Security. KYBER inherits a strong theoretical security foundation from decades of lattice cryptography literature. Moreover, a series of results over the past decade support the notion that the Module version of LWE[F04] is suitable for high-performance cryptosystems without sacrificing security. In particular, a 2012 work by Langlois and Stehlé [182] provides a relatively tight reduction from worst-case Module-SIVP to average-case Module-LWE. Additional results have given evidence that, roughly speaking, transitioning from rank one (i.e., Ring-LWE) to constant rank (i.e., Module-LWE) is likely to increase performance and unlikely to sacrifice security [183–185].

Beyond discussion of lattice cryptographic theory, it was mentioned above that KYBER employs a particular variant of the FO transform to achieve CCA security. The security proofs hold tightly in the ROM [171, 172] and non-tightly in the QROM. Yet under various other natural assumptions, KYBER may also achieve a tight security reduction in the QROM [186].

In the third round, the KYBER team also provided an extensive analysis of the system's concrete security ([14, Sections 5.2 and 5.3]). While many of the details in this section remain somewhat speculative, the overall conclusions appear consistent with the state of the art in lattice cryptanalysis. In addition to a best guess concrete security estimate for all the parameter sets, that section contains a list of open questions in lattice cryptanalysis, and gives a range of estimates for the possible effect on concrete security corresponding to each open question.

où $\lceil \frac{q}{2} \rfloor \cdot m$ est interprété de façon classique comme le vecteur des coefficients d'un unique polynôme de R_q (avec le remplissage nécessaire). Le mécanisme de chiffrement asymétrique KYBER supprime certains des bits les moins significatifs du chiffré. Les chiffrés font donc l'objet d'un type précis de « compression ».

Après « décompression » du chiffré c, son déchiffrement à l'aide de la clé secrète $\mathbf{s}$ nécessite de calculer la valeur intermédiaire $v = c_2 - \mathbf{c_1 s}$ puis d'arrondir chaque coefficient du polynôme v modulo 2 pour obtenir la chaîne de caractères m.

Sécurité. KYBER repose sur des fondations théoriques solides héritées de plusieurs décennies de recherches en cryptographie basée sur les réseaux euclidiens[F03]. Ces dix dernières années, plusieurs avancées théoriques sont venues confirmer la pertinence du problème Module-LWE pour la construction de cryptosystèmes à la fois performants et sûrs. A. Langlois et D. Stehlé ont notamment démontré dans un article publié en 2012 [182] l'existence d'une réduction du cas le plus défavorable de Module-SIVP au cas moyen de Module-LWE. D'autres résultats ont permis de montrer que, de manière générale, le passage d'une base de rang 1 (problème Ring-LWE) à une base de rang n (problème Module-LWE) était susceptible d'offrir de meilleures performances sans entraîner de réduction de la sécurité [183–185].

Au-delà des questions inhérentes à la cryptographie basée sur les réseaux euclidiens[F03], il a été fait mention précédemment de l'utilisation par KYBER d'une variante particulière de la transformation FO afin de devenir indistinguable contre des attaques à chiffré choisi. Les preuves de sécurité obtenues sont fines dans le modèle de l'oracle aléatoire (ROM) [171, 172], et non fines dans le modèle de l'oracle aléatoire quantique (QROM). Sous diverses autres hypothèses naturelles, KYBER pourrait cependant parvenir à une réduction de sécurité fine dans le QROM.

Au cours de la troisième étape, l'équipe de KYBER a fourni une analyse détaillée de la sécurité concrète du système ([14, sections 5.2 et 5.3]). Si de nombreuses informations présentées dans ces sections conservent un caractère spéculatif, leurs conclusions semblent conformes à l'état de la recherche en cryptanalyse des réseaux euclidiens. En plus de la meilleure estimation à ce jour de la sécurité offerte par chaque jeu de paramètres, chaque section contient une liste de questions ouvertes en cryptanalyse des réseaux euclidiens et un ensemble d'estimations des effets potentiels de chacune d'entre elles sur la sécurité concrète du système.

According to the analysis provided in the KYBER specification, in the very worst case, if every open question is resolved in the worst case for KYBER, some of the parameter sets may fall below their targeted security level in the gate-count model, although even in this case, it is likely the submitted parameter sets will still meet their targeted security levels in any cost model which realistically models the cost of memory access.

Performance. Like the other structured lattice KEMs[F02], KYBER's public key and ciphertext sizes are on the order of a thousand bytes, which should be acceptable for most applications (see Table 6). In comparison, KYBER's bandwidth is smaller than NTRU but about 10% larger than Saber.

KYBER has fast key generation, encapsulation and decapsulation in software [33] (see Section 2.2.2). There have been several works on optimizing implementations of KYBER in both software and hardware, as well as in hybrid hardware/software settings [35, 40–45, 80]. For high-speed FPGA implementations, [46] shows that in terms of speed and resource realization, KYBER is a leading performer for all operations : key generation, encapsulation and decapsulation (among the finalist lattice KEMs[F02]).

Overall, the performance data reported from these referred works indicate that KYBER has sufficient performance in many different environments.

Significant events since Round 2. At the beginning of the third round, the KYBER team increased the binomial noise parameter η from 2 to 3 for the centered binomial distribution used to sample public-key components in its category 1 parameter set. This was partly due to a suggestion from the NIST PQC team. Mildly increasing the noise resulted in a stronger defense against lattice reduction attacks without raising the decryption failure rate above the requisite threshold for security.

Selon l'analyse fournie avec le dossier de candidature de KYBER, dans le pire des cas, où la réponse à chaque question s'avère être la plus défavorable possible pour KYBER, certains jeux de paramètres sont susceptibles de s'éloigner de leur niveau de sécurité théorique prévu par le modèle du nombre de portes. Cependant, même dans ce cas de figure, les jeux de paramètres proposés devraient atteindre leur niveau de sécurité théorique dans tous les modèles de simulation des coûts estimant de manière réaliste le coût de l'accès à la mémoire.

Performances. Comme pour les autres mécanismes d'encapsulation de clé[F02] basés sur les réseaux euclidiens structurés, la clé publique et le chiffré de KYBER ont une taille de l'ordre du millier d'octets, une valeur satisfaisante pour la plupart des applications (voir le tableau 6). KYBER dispose d'une bande passante 10 % plus importante que celle de Saber, bien que plus faible que celle de NTRU.

KYBER génère, encapsule et décapsule rapidement des clés au sein d'un logiciel [33] (voir section 2.2.2). De nombreux travaux ont été menés sur l'optimisation des mises en œuvre de KYBER à la fois sur les plans logiciel et matériel ainsi que dans des configurations hybrides [35, 40–45, 80]. Concernant les mises en œuvre à haute fréquence sur des FPGA, cet article [46] démontre la supériorité de KYBER sur les autres mécanismes finalistes basés sur les réseaux euclidiens en matière de rapidité et d'utilisation des ressources, et ce dans toutes les opérations observées : génération, encapsulation et décapsulation de clé.

Les données récoltées dans ces différents travaux sur les performances de KYBER lui attribuent des performances satisfaisantes dans de nombreux environnements différents.

Évènements notables depuis la deuxième étape. Au début de la troisième étape, l'équipe de KYBER a choisi de modifier son jeu de paramètres de catégorie 1 en relevant de 2 à 3 le paramètre de bruit binomial η de la loi binomiale centrée servant à échantillonner les composants de la clé publique. Cette décision résulte en partie d'une suggestion de l'équipe PQC du NIST. Cette légère augmentation du bruit a permis de renforcer la résistance aux attaques par réduction de réseaux sans pour autant accroître le taux d'échec de déchiffrement au-delà du seuil maximum de sécurité.

To compensate for the increase in decryption failure probability, the number of dropped bits for each coefficient of the second component of the ciphertext was changed from 4 to 3 for the category 1 parameters (KYBER512). In addition, during key generation the uniform sampling was made more efficient by using rejection sampling on 12-bit integers instead of 2-byte integers.

To provide a more precise core SVP estimate of KYBER512, the KYBER team accounted for the noise added from the rounding operation of the ciphertext. Assuming a weak version of LWR, the added noise yields 6 more bits of core SVP hardness for KYBER512.

During the third round, some improvements to the dual attack were proposed [165, 166], leading to lower estimated security in the RAM model than was claimed in the KYBER specification. These results suggest that all three KYBER parameter sets fall slightly below the security targets for their claimed security levels when the cost of memory access for the attacker is not explicitly taken into account.

Overall assessment. The security of KYBER has been thoroughly analyzed and is based on a strong framework of results in lattice-based cryptography[F03]. KYBER has excellent performance overall in software, hardware and many hybrid settings.

While the three structured lattice finalists are all strong candidates, NIST has selected KYBER for standardization. A significant factor in the decision to choose KYBER over NTRU was NTRU's performance (particularly key generation), which was not quite as efficient as that of KYBER. There is arguably more evidence to support the MLWE problem (which KYBER is based upon) than the MLWR or NTRU assumptions which Saber and NTRU respectively rely upon.

Pour compenser l'augmentation de la probabilité d'échec de déchiffrement, le nombre de bits supprimés pour chaque coefficient du deuxième composant du chiffré a été réduit de 4 à 3 pour tous les jeux de paramètres de catégorie 1 (Kyber512). L'échantillonnage uniforme nécessaire à la génération de la clé a également été rendu plus efficace par l'utilisation d'un échantillonnage par rejet sur des entiers longs de 12 bits au lieu de 16.

L'équipe de Kyber a inclus le bruit généré par l'arrondissage du chiffré à son calcul du score core SVP de Kyber afin d'estimer plus précisément ce dernier. Dans le cadre d'une version faible de Learning With Rounding (LWR), ce bruit supplémentaire augmente de 6 bits la difficulté core SVP de Kyber512.

L'attaque duale a reçu des améliorations au cours de la troisième étape [165, 166], entraînant une réduction de la sécurité estimée de Kyber dans le modèle du RAM comparé au cahier des charges de l'algorithme. Ces résultats indiquent que les trois jeux de paramètres de Kyber offrent une sécurité légèrement inférieure à celle requise par les niveaux de sécurité visés lorsque le coût de l'accès à la mémoire de l'attaquant n'est pas explicitement pris en compte.

Bilan général. La sécurité de Kyber a fait l'objet d'analyses poussées dans le cadre d'importantes recherches en cryptographie basée sur les réseaux euclidiens[F03]. Kyber a montré d'excellentes performances globales dans diverses configurations matérielles, logicielles et hybrides.

Si les trois finalistes basés sur les réseaux euclidiens structurés sont des candidats sérieux, le NIST a choisi Kyber comme future norme. Les performances de NTRU, moins efficace que Kyber (particulièrement lors de la génération de la clé), ont joué un rôle considérable dans la sélection de Kyber au détriment de NTRU. Le problème MLWE (sur lequel repose Kyber) s'appuie vraisemblablement sur davantage de preuves que les problèmes MLWR et NTRU qui sous-tendent respectivement Saber et NTRU.

4.2.2 Classic McEliece

Design. Classic McEliece is a code-based KEM[F02] that uses a binary Goppa code in the Niederreiter variant of the McEliece cryptosystem combined with standard techniques to achieve CCA security. Due to the use of Goppa codes, the KEM has perfect correctness.[12] It is a merger of the second-round submissions Classic McEliece and NTS-KEM. The original McEliece cryptosystem was published in [197] and was also based on a binary Goppa code.

Security. The Classic McEliece submission cites [198] and other results as giving a tight proof of the submitted KEM's[F02] IND-CCA2 security in the quantum random oracle[F05] model, based on the assumption that the 1978 McEliece scheme provides one-way under chosen-plaintext attacks (OW-CPA) security. Confidence in the security of the 1978 scheme is mostly established based on the scheme's long history of surviving cryptanalysis with only minor changes in the complexity of the best-known attack. Alternatively, the security of the scheme could be established under the assumptions that row-reduced parity check matrices for the binary Goppa codes used by Classic McEliece are indistinguishable from row-reduced parity check matrices for random linear codes of the same dimensions and that the syndrome decoding problem is hard for random linear codes with those dimensions. The state of the art in cryptanalysis does not contradict these assumptions, although binary Goppa codes with very different dimensions from those used by the Classic McEliece submission have been shown to be distinguishable from random codes [199].

A number of approaches to the cryptanalysis of Classic McEliece have been studied. The most effective known attacks, and those used to set the parameters of Classic McEliece, are information set decoding attacks, as described in Section 3.2.1.

[12] A perfectly correct KEM[F02] or PKE is one for which every ciphertext generated using the encapsulation/encryption function may be correctly decrypted using the decapsulation/decryption function. In contrast, some KEMs[F02] and PKEs have a very small decryption failure rate.

4.2.2 Classic McEliece

Architecture. Classic McEliece est un mécanisme d'encapsulation de clé[F02] basé sur les codes correcteurs d'erreur. Il s'agit de la variante Niederreiter du cryptosystème McEliece, utilisée avec des codes de Goppa binaires et combinée aux techniques employées habituellement pour résister aux attaques à chiffré choisi (CCA). L'utilisation des codes de Goppa rend ce mécanisme d'encapsulation de clé[F02] parfaitement correct.[12] Ce mécanisme est issu de la fusion des candidats Classic McEliece et NTS-KEM à l'issue de la deuxième étape. Le cryptosystème McEliece a été publié ici [197] à l'origine. Il reposait également sur les codes de Goppa binaires.

Sécurité. Le dossier de candidature de Classic McEliece s'appuie sur [198] ainsi que sur d'autres résultats pour justifier de la sécurité IND-CCA2 du mécanisme candidat dans le modèle de l'oracle[F05] aléatoire quantique, en partant de l'hypothèse selon laquelle le mécanisme McEliece de 1978 offre une sécurité à sens unique face à une attaque à clair choisi (OW-CPA). La confiance dans la sécurité du mécanisme de 1978 découle essentiellement de sa résistance aux nombreuses tentatives de cryptanalyse, la meilleure attaque connue n'affectant que légèrement sa complexité. La sécurité du mécanisme peut également reposer sur l'hypothèse selon laquelle les matrices de contrôle échelonnées réduites des codes de Goppa binaires utilisées par Classic McEliece sont indistinguables des matrices de contrôle échelonnées réduites des codes linéaires aléatoires de mêmes dimensions et selon laquelle le problème du décodage par syndrome est difficile pour des codes linéaires aléatoires de cette dimension. L'état de la recherche en cryptanalyse ne contredit pas ces hypothèses, bien qu'il ait été démontré que certains codes de Goppa binaires de dimensions très différentes de ceux employés par le mécanisme candidat Classic McEliece sont distinguables des codes aléatoires [199].

De nombreuses pistes ont été explorées pour la cryptanalyse de Classic McEliece. Les attaques les plus efficaces à ce jour reposent sur le décodage par ensemble d'informations. Décrites dans la section 3.2.1, elles sont utilisées pour définir les paramètres de Classic McEliece.

[12] Un mécanisme d'encapsulation de clé[F02] ou de chiffrement asymétrique est dit correct lorsque tous les chiffrés générés par les algorithmes d'encapsulation ou de chiffrement peuvent être déchiffrés à l'aide des algorithmes de décapsulation ou de déchiffrement. Certains mécanismes d'encapsulation de clé[F02] ou de chiffrement asymétrique ont un taux d'échec du déchiffrement très faible, mais non-nul.

Key recovery attacks have also been studied. These either attempt to find the private key by algebraic techniques or brute force search. While algebraic techniques have been used to break variants of McEliece based on other algebraic codes [200–204] or based on Goppa codes with additional structure imposed [205], these techniques appear to be significantly more costly than information set decoding for attacking Classic McEliece.

Performance. Classic McEliece has a very large public key size and fairly slow key generation. This is likely to make Classic McEliece undesirable in many common settings. However, in settings where a public key is reused many times and does not be need to be retransmitted for each new communication, it is possible that the performance profile of Classic McEliece could have some advantages. In particular, Classic McEliece has the smallest ciphertext sizes of any of the NIST PQC candidates.

Significant events since Round 2. While there has been no significant cryptanalysis on Classic McEliece, it did spark a large amount of discussion on the pqc-forum. Much of this discussion concerned issues that are generally applicable to code-based schemes or even KEMs[F02] in general. However, a few issues specific to the Classic McEliece submission were uncovered. In particular, based on the concrete analyses of [135], at least one of the parameter sets (targeting category 3) appears to fall slightly short of its target security level (probably meeting category 2 instead). The submission document also contains a potentially misleading implementation note that NIST recommends be removed. A misuse scenario was also brought up, where reusing the same error vector when encapsulating for multiple public keys can result in a significant security loss. This scenario should not happen assuming the random number generator is functioning properly, but it could be made even less likely through fairly simple countermeasures like incorporating the public key in the derivation of the error vector. A similar misuse scenario with similar countermeasures also applies to BIKE, HQC, and NTRU.

Des attaques visant à retrouver la clé privée, par des méthodes algébriques ou par force brute, sont également à l'étude. Si des méthodes algébriques ont été utilisées pour casser des variantes de McEliece reposant sur d'autres codes algébriques [200–204] ou sur des codes de Goppa avec une structure supplémentaire imposée [205], ces méthodes se sont montrées bien plus coûteuses que le décodage par ensemble d'informations pour attaquer Classic McEliece.

Performance. Les clés publiques de Classic McEliece sont très longues et plutôt lentes à générer. Cet aspect est susceptible de disqualifier Classic McEliece dans nombre d'usages courants. Toutefois, lorsqu'une clé publique est réutilisée de nombreuses fois et non retransmise à chaque communication, le profil de ClassicMcEliece présente certains avantages. De tous les candidats étudiés par le NIST, ClassicMcEliece renvoie notamment les chiffrés les plus courts.

Évènements notables depuis la deuxième étape. Si aucune attaque n'est parvenue à menacer ClassicMcEliece, le mécanisme a fait l'objet de nombreux débats sur le forum consacré à la cpq. Nombre d'entre eux portaient sur des questions relatives aux mécanismes basés sur les codes correcteurs d'erreur, voire aux mécanismes d'encapsulation de clé[F02] en général. Quelques questions relatives à Classic McEliece ont tout de même été soulevées. En particulier, selon les analyses menées dans [135], au moins un des jeux de paramètres manque de peu son objectif, offrant probablement une sécurité de niveau 2 au lieu de 3. Le dossier de candidature contient une note de la mise en œuvre potentiellement trompeuse que le NIST recommande de retirer. Un scénario d'utilisation incorrecte a également été mentionné : la réutilisation du même vecteur d'erreur lors de l'encapsulation de plusieurs clés publiques peut réduire considérablement la sécurité. Ce scénario ne devrait pas se produire en cas de fonctionnement normal du générateur de nombres aléatoires, mais des contre-mesures relativement simples, telles que l'incorporation de la clé publique à la dérivation du vecteur d'erreur, permettent de le rendre encore moins probable. Ce scénario et ces contre-mesures concernent également BIKE, HQC et NTRU.

Overall assessment. NIST is confident in the security of Classic McEliece and would be comfortable standardizing the submitted parameter sets (under a different claimed security strength in some cases). However, it is unclear whether Classic McEliece represents the best option for enough applications to justify standardizing it at this time. For general-purpose systems wishing to base their security on codes rather than lattices, BIKE or HQC may represent a more attractive option. For applications that need a very small ciphertext, SIKE may turn out to be more attractive. NIST will, therefore, consider Classic McEliece in the fourth round along with BIKE, HQC, and SIKE. NIST would like feedback on specific use cases for which Classic McEliece would be a good solution.

Bilan général. Le NIST a confiance dans la sécurité offerte par Classic McEliece et consent à normaliser les jeux paramètres qui lui ont été soumis (sous un niveau de sécurité différent si nécessaire). Il reste à déterminer si Classic McEliece représente la meilleure option pour suffisamment d'applications pour justifier sa normalisation immédiate. Pour les systèmes d'usage général qui souhaitent baser leur sécurité sur les codes correcteurs d'erreurs plutôt que sur les réseaux euclidiens, BIKE et HQC apparaissent être des choix plus pertinents. Pour les applications qui nécessitent un chiffré très court, SIKE semble plus adapté. Le NIST va donc examiner Classic McEliece au cours de la quatrième étape aux côtés de BIKE, HC et SIKE. Le NIST souhaite avoir un retour d'information sur les cas d'utilisation où Classic McEliece représenterait un solution pertinente.

References

[1] National Institute of Standards and Technology (2013) Digital signature standard (DSS) (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards (FIPS) Publication 186-4. https ://doi.org/10.6028/NIST.FIPS.186-4

[2] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R (2018) Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography (U.S. Department of Commerce, Washington, D.C.), Special Publication 800-56A Revision 3. https ://doi.org/10.6028/NIST.SP.800-56Ar3

[3] Barker EB, Chen L, Roginsky AL, Vassilev A, Davis R, Simon S (2019) Recommendation for pair-wise key-establishment using integer factorization cryptography (U.S. Department of Commerce, Washington, D.C.), Special Publication 800-56B Revision 2. https ://doi.org/10.6028/NIST.SP.800-56Br2

[4] National Institute of Standards and Technology (2016) Announcing request for nominations for public-key post-quantum cryptographic algorithms. Federal Register 81(244) :92787–92788.

[5] National Institute of Standards and Technology (2016) NIST post-quantum cryptography standardization.

[6] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tone D (2019) Status report on the first round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240.
https ://doi.org/10.6028/NIST.IR.8240

[7] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tone D (2020) Status report on the second round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8309.

[8] Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, Smith-Tone D (2016) Report on post-quantum cryptography (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105. https ://doi.org/10.6028/NIST.IR.8105

[9] National Institute of Standards and Technology (2016) Submission requirements and evaluation criteria for the post-quantum cryptography standardization process.

[10] Schank J (2021) Category 5 NTRU parameters. https ://groups.google.com/a/list.nist.gov/g/pqc-forum/c/t1JCgzSS-uk/m/VXXQaJgFCQAJ.

[11] Beullens W (2021) Improved cryptanalysis of UOV and Rainbow. Advances in Cryptology – EUROCRYPT 2021, eds Canteaut A, Standaert FX (Springer International Publishing, Cham), pp 348–373.

Bibliographie

[1] National Institute of Standards and Technology. *FIPS PUB 186-4* : Digital Signature Standard (DSS), 2013. https ://doi.org/10.6028/NIST.FIPS.186-4

[2] National Institute of Standards and Technology. *SP800-56A Rev. 3 : Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2018.
https ://doi.org/10.6028/NIST.SP.800-56Ar3

[3] National Institute of Standards and Technology. *SP800-56B Rev. 2 : Recommendation for pair-wise key-establishment using integer factorization cryptography*, 2019.
https ://doi.org/10.6028/NIST.SP.800-56Br2

[4] National Institute of Standards and Technology, *Announcing request for nominations for public-key post-quantum cryptographic algorithms. Federal Register 81(244) :92787–92788*, 2016.

[5] National Institute of Standards and Technology, *NIST post-quantum cryptography standardization*, 2016.

[6] G. Alagic, J. Alperin-Sheriff, D. Apon , D. Cooper, Q. Dang, YK. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, *Status report on the first round of the NIST post-quantum cryptography standardization process*, National Institute of Standards and Technology, 2019.
https ://doi.org/10.6028/NIST.IR.8240

[7] G. Alagic, J. Alperin-Sheriff, D. Apon , D. Cooper, Q. Dang, J. Kelsey, YK. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone *Status report on the second round of the NIST post-quantum cryptography standardization process*, National Institute of Standards and Technology, 2020.

[8] L. Chen, S. Jordan, YK. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, *Report on post-quantum cryptography*, National Institute of Standards and Technology, 2016.
https ://doi.org/10.6028/NIST.IR.8105

[9] National Institute of Standards and Technology, *Submission requirements and evaluation criteria for the post-quantum cryptography standardization process*, 2016.

[10] J. Schank, *Category 5 NTRU parameters*, 2021.
https ://groups.google.com/a/list.nist.gov/g/pqc-forum/c/t1JCgzSS-uk/m/VXXQaJgFCQAJ.

[11] W. Beullens, Improved cryptanalysis of UOV and Rainbow, *Advances in Cryptology*– EUROCRYPT 2021, pp 348–373, Springer, 2021.

Troisième partie

Stratégie de traduction

1 Un texte, une méthode

1.1 Choix du texte support

La cryptographie post-quantique est au centre des préoccupations de nombreux acteurs publics et privés. Plusieurs laboratoires français mènent des recherches dans le domaine : l'Institut national de recherche en sciences et technologies du numérique (INRIA), le Laboratoire d'informatique du Parallélisme (LIP), l'Institut de recherche en informatique et systèmes aléatoires (IRISA), l'institut de recherche XLIM, le Laboratoire d'informatique de l'École polytechnique (LIX) ou encore l'Institut de mathématiques de Bordeaux (IMB), chapeautés par le CNRS et soutenus par le plan quantique français dont 150 millions d'euros sur 1,8 milliard sont consacrés à la cryptographie post-quantique. Trois des quatre algorithmes sélectionnés en juillet 2022 pour être normalisés ont reçu des contributions de chercheurs issus de ces laboratoires français. C'est également le cas de deux des algorithmes sélectionnés pour la quatrième étape du processus.

Mon stage de trois mois en tant que traducteur au sein du Bureau international des poids et mesures m'a familiarisé avec le monde de la normalisation du fait des similitudes entre la dissémination des normes et celle des unités du Système international. Ce stage m'a également permis de découvrir l'existence du NIST et du processus de normalisation de la cryptographie post-quantique mené par ce dernier. La centralisation du processus initié par le NIST offre une vue d'ensemble sur le domaine de la cryptographie post-quantique. Ce projet qui réunit la majorité des initiatives importantes dans le domaine et catalyse les efforts de recherche me semblait parfaitement adapté à l'extraction d'un texte-support décrivant le domaine, ses enjeux et ses solutions techniques avec une certaine technicité tout en restant accessible.

J'ai d'abord envisagé de travailler sur le premier rapport du NIST sur la cryptographie post-quantique, NIST IR 8105, publié en 2016.[1] Ce dernier m'a finalement semblé daté, le processus de sélection n'ayant pas encore débuté à la publication du rapport. J'ai ensuite parcouru les rapports publiés par le NIST dans la suite du processus. Le troisième d'entre eux, publié à l'issue de la troisième étape en juillet 2022, m'a paru tout à fait adapté aux exigences du mémoire et d'un grand intérêt technique et terminologique.

[1] Chen Lily, Jordan Stephen, Liu Yi-Kai et al. *Report on Post-Quantum Cryptography.* NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. 2016.

1.2 Nature du texte-support

Le rapport NIST IR 8413 a été publié le 5 juillet 2022 par une équipe de chercheurs réunie par le NIST. Onze des quatorze auteurs du rapport avaient déjà participé à la rédaction du second rapport sur l'état d'avancement du processus de normalisation (NIST IR 8309).[1] Ce texte constitue l'aboutissement de six années de sélection des nouvelles normes cryptographiques états-uniennes et, de facto, internationales. Il s'agit d'un texte technique, destiné à des spécialistes. S'il contient de nombreuses explications sur le fonctionnement des algorithmes de cryptographie post-quantique élaborés dans le cadre de la sélection, il ne s'agit pas pour autant d'une norme. Rien dans ce rapport n'est immédiatement destiné à être appliqué, la rédaction des normes constituant l'étape suivante du processus de normalisation.

Le NIST justifie ici ses choix d'algorithmes d'encapsulation de clé et de signature numérique, en présentant les critères de sélection et les algorithmes lauréats. Il s'agit d'un résumé des travaux et des tests effectués par les équipes du NIST pendant les deux années qu'a duré la troisième étape de sélection. Le texte donne tout de même un aperçu de la manière dont seront construites les normes, en mobilisant les notions de niveau de sécurité et de jeux de paramètres. Une version révisée du rapport a été publiée le 26 septembre 2022 sous le nom de NIST IR 8413-upd1. Les légères modifications effectuées ne portant pas sur des segments faisant l'objet d'une traduction dans ce mémoire, les deux versions du rapport y sont considérées comme strictement équivalentes.

1.3 Découpage du texte

Avec 62 pages et 25 000 mots hors bibliographie et annexes, le texte d'origine excédait largement les prérequis du texte-support. J'ai donc choisi d'opérer plusieurs coupes afin de ramener sa longueur à 20 400 caractères. Cette longueur excède très légèrement les bornes du mémoire mais permet d'inclure l'intégralité d'une sous-partie riche en terminologie technique. J'ai veillé à garder la structure d'origine du rapport, en ne conservant qu'un ou deux exemples par grande partie. Je traite ainsi l'intégralité de l'introduction, qui pose les enjeux du processus de normalisation ; un critère d'évaluation choisi par le NIST, celui de la sécurité ; enfin, deux algorithmes d'encapsulation de clé, l'algorithme lauréat

[1] Alagic Gorjan, Alperin-Sheriff Jacob, Apon Daniel et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, 2020.

CRYSTALS–Kyber et un des algorithmes alternatifs, Classic McEliece. Le découpage permet selon moi de comprendre les enjeux de la sélection et la façon dont elle a eu lieu, en plus de présenter deux algorithmes qui seront très probablement les deux premiers mécanismes d'encapsulation de clé post-quantiques normalisés.

1.4 Travaux préliminaires à la traduction

J'ai choisi de rédiger l'intégralité de mon exposé avant même de me pencher sur la traduction. Les recherches effectuées afin de rédiger ce dernier m'ont permis de mieux comprendre les enjeux décrits dans le texte-support. Je pense que cette stratégie s'est montrée féconde dans le cas d'un texte aussi technique. Les sources accumulées pendant ces recherches m'ont également été d'un grand secours lors de la traduction du texte-support.

Les publications de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) m'ont notamment inspiré mon postulat traductif, que je présente plus en détail dans la section suivante. Comme je l'explique dans mon exposé, l'ANSSI joue en quelques sortes le rôle du NIST pour la France, du moins au plan légal. L'organisme indique quels algorithmes, normes et certificats déployer dans les entreprises et les administrations françaises. L'Agence publie à cet effet des avis[1] et des guides[2]. La production d'avis précède celle des guides, les avis permettant de dévoiler l'orientation de la politique de l'ANSSI vis-à-vis de l'état de l'art en matière de cryptographie. Les avis précèdent généralement la publication des normes par les instances internationales. Une fois ces normes publiées, l'ANSSI peut s'atteler à la rédaction d'un guide à destination des développeurs et des administrateurs qui recense les algorithmes, leurs cas d'usage et des conseils de mise en œuvre. Ces documents m'ont permis de m'immerger dans la terminologie cryptographique française.

[1] Agence nationale de la sécurité des systèmes d'information. *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*. Paris, 2022.

[2] Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques*. Paris, 2021.

Type de documents	Nombre de mots	Pourcentage
Thèses	373 183	70,5 %
Supports de cours	82 099	16 %
Rapports	63 999	12 %
Extraits de thèses	5633	1 %
Pages internet	2762	0,5 %
Total	527 271	100 %

FIGURE 4.1 : Description statistique du corpus français. On observe une surreprésentation des thèses et des supports de cours.

Comme souvent en informatique, et dans les sciences en général, on peut distinguer le champ de la recherche de celui de l'application. L'ANSSI couvre l'application mais ne mène pas de recherches proprement dites. La normalisation, qui fait l'objet de ce mémoire, se plaçant à l'exacte intersection de ces deux domaines, je me suis également plongé dans de nombreux articles de recherche et thèses. La production de recherche cryptographique en langue française subit les influences conjuguées de deux phénomènes : la forte présence de la France et de ses chercheurs dans ce domaine d'un côté, l'omniprésence de l'anglais dans la recherche en informatique de l'autre. Cette double influence explique selon moi la proportion importante de thèses parmi les sources utilisées pour ma traduction. Le parcours typique d'un universitaire français comporte généralement la rédaction d'une thèse au sein d'une université française et donc rédigée en français puis des contrats postdoctoraux dans des universités à l'étranger et donc la rédaction d'articles en anglais. La forte présence française en cryptographie m'a tout de même donné l'occasion d'échanger avec des spécialistes ayant le français comme langue maternelle sur des questions terminologiques pointues.

Les cours de cryptographie dispensés dans des universités françaises ont également constitué des sources documentaires précieuses. Je remercie M. Olivier Blazy de m'avoir indiqué les cours de M. Damien Stehlé à l'École Normale Supérieure de Lyon et de M. Pierre-Alain Fouque à l'université Rennes 1. Je me suis également beaucoup reposé sur les supports de cours de Mme Anca Nitulescu à l'École Normale Supérieure de Paris.

L'application commerciale est la grande absente de mes sources, et pour cause : dans le triptyque *recherche – normalisation – application*, nous n'en sommes qu'à l'étape charnière de la normalisation. Le protocole *Signal*, l'une des rares mises en œuvre commerciales actuelles de la cryptographie post-quantique, ne communique à ma connaissance qu'en anglais.

J'ai réalisé des statistiques sur le corpus documentaire en français qui m'a servi dans mes analyses qualitatives et quantitatives à l'aide du logiciel de gestion de corpus SketchEngine (voir FIGURE 4.1).

1.5 Public-cible et postulat traductif

J'ai choisi de définir mon postulat traductif en fonction d'un public cible fictif que j'ai imaginé. Pour la rédaction d'un éventuel guide sur la cryptographie post-quantique,

l'ANSSI devra se pencher sur la théorie qui sous-tend les normes rédigées par le NIST. L'ANSSI a en effet déjà annoncé se calquer sur les décisions du NIST pour la rédaction des visas de sécurité français.

En plus d'une traduction française des normes définitives, qui ne sont pas encore parues à la date de rédaction de ce mémoire, une traduction française des rapports du NIST sur les phases d'avancement du processus de la CPQ devrait apporter des lignes directrices terminologiques fondamentales aux rédacteurs de l'ANSSI. Ce sont ces derniers qui constitueront mon public-cible : les personnels chargés de transposer dans le droit et la sécurité des systèmes d'information français des normes rédigées aux États-Unis.

Les implications de ce postulat traductif sont nombreuses, je reviendrai sur certaines d'entre elles plus loin dans ma démonstration. Il me semble toutefois important de mentionner que la finalité du texte traduit est identique à celle du texte source : renseigner des spécialistes du domaine sur des questions pointues et dresser un état de l'art d'un domaine qui évolue d'une année sur l'autre. Je reviendrai sur la dimension frénétique de la cryptographie au point 2.2. Le postulat traductif m'a par exemple permis de répondre à la question du taux de foisonnement. La longueur du texte-cible est ici indéniablement supérieure à celle du texte source. La réduction du taux de foisonnement ne m'a pas guidé dans ma démarche de traduction en raison de la non-comparabilité des deux documents. Rédigés pour deux institutions différentes (le NIST d'un côté, l'ANSSI, de manière fictive, de l'autre), les textes ne sont pas voués à être affichés l'un face à l'autre ni comparés. Le texte-cible jouit, à mon sens, d'une grande indépendance vis-à-vis du texte source. Ceci également car sa durée de vie est éphémère : document de travail fondamental, état de l'art de la cryptographie post-quantique en 2022, il est destiné à être supplanté par des normes définitives qui fixeront encore mieux que lui des algorithmes et une terminologie pour la CPQ. Les exigences d'exactitude, d'exhaustivité et de conformité à la *langue des rapports* m'ont guidé dans la rédaction de ma traduction.

2 Traduire un domaine en gestation

La cryptographie post-quantique est jeune. C'est l'une des petites-filles de l'informatique, qui a engendré la cryptographie moderne, l'informatique quantique puis, il y a seulement deux décennies, la cryptographie post-quantique. Cette relative jeunesse du domaine a été déterminante dans ma stratégie de traduction. J'ai sélectionné plusieurs problèmes que j'estime relatifs au domaine de spécialité et à sa langue de spécialité. Je les détaillerai ici avec les solutions choisies pour les résoudre.

2.1 L'informatique est née anglaise

J'ai choisi de regrouper sous ce sous-titre, que j'ai tiré d'Alberto Sobrero cité par Maria Centrella[1], les différents problèmes traductologiques que j'estime liés à la place occupée par l'anglais dans la terminologie informatique. Je tenterai de contextualiser chacun des exemples, d'expliquer les recherches effectuées afin de les résoudre puis de présenter les choix de traduction pour lesquels j'ai opté. L'informatique, et particulièrement ses sous-domaines émergents comme la cryptographie post-quantique, occupent une place singulière face à l'anglais : la production universitaire se fait en anglais, la normalisation et l'application commerciale également.

Au-delà de la question des *anglicismes*, c'est la question de la traduction ou non de certains termes qui se pose. En français, la langue de spécialité, définie par Jean Delisle comme le « Sous-système linguistique qui comprend la terminologie et les moyens d'expression propres à un domaine de spécialité »[2], comprend en cryptographie des termes et des expressions en langue anglaise. En particulier, j'ai choisi de m'intéresser au terme *PQC*, sigle utilisé par le NIST et bien d'autres auteurs pour raccourcir l'expression *post-quantum cryptography*, qui me permettra d'aborder de façon plus générale la question des sigles en informatique.

Je suis d'abord allé chercher dans le même ouvrage des ressources sur la façon d'aborder ces termes anglais. Sur la question des anglicismes, et bien des anglicismes seulement, Jean Delisle pose que « La règle la plus sage à suivre, à notre avis, serait celle-ci : juger de la « tolérance linguistique » du client donneur d'ouvrage, de son réviseur ou de son

[1] Centrella Maria. *Le vocabulaire de l'informatique – De la norme à l'usage*. Paris : Hermann, 2013. 215 p.

[2] Delisle Jean. *La traduction raisonnée*. Ottawa : Presses de l'Université d'Ottawa, 2013 (1993). p. 666.

professeur afin d'éviter de prêter le flanc à la critique. »[1]. Puisque j'avais défini un donneur d'ordre fictif, j'ai adopté cette approche dans un premier temps. J'ai relu mes sources de l'ANSSI pour analyser le traitement des termes anglais dans ces derniers. Les deux termes auxquels je m'intéresse sont mentionnés dans la mise à jour de la position de l'ANSSI sur la transition vers la cryptographie post-quantique[2]. Dans ce texte, le sigle anglais *PQC* est utilisé en lieu et place de *cryptographie post-quantique*, et « Learning with errors » est entouré de guillemets mais non traduit. Je n'ai trouvé cette solution satisfaisante pour aucun des deux problèmes.

Intéressons-nous d'abord au cas du sigle. Une solution aurait pu être de ne pas utiliser de sigle du tout, et de conserver partout la forme longue *cryptographie post-quantique*. Je ne me suis pas satisfait de cette solution non plus. En effet, le sigle est un outil des plus précieux en communication spécialisée : « les sigles ont une vertu irrésistible aux spécialistes ; ils atteignent une concision remarquable sans perdre quoi que ce soit de la précision sémantique du syntagme source ».[3] J'ai donc envisagé une autre approche, celle de la traduction du sigle. Assez frileux à l'idée de traduire ce sigle en un sigle français très peu employé, je me suis inspiré de la méthode que j'ai appliquée au cours de mon stage à l'Organisation européenne pour la recherche nucléaire (CERN). Au cours de la traduction d'un texte sur la chromodynamique quantique, équivalent français du terme *quantum chromodynamics*, ou *QCD*, j'ai fait des recherches dans les mémoires de traduction du CERN où *QCD* était toujours traduit par CDQ. La traduction du sigle répond ici à une logique simple d'économie et de conservation du français dans la langue technique de la physique quantique. La traduction en français du sigle *PQC* par le sigle CPQ me paraît satisfaisante et tout à fait implantable. Dans son enquête sur l'implantation du vocabulaire normalisé de l'informatique, Maria Centrella mentionne comme critères d'ordre morphosémantiques susceptibles de faciliter l'implantation « la proximité du terme français avec le terme anglais » ainsi que « la brièveté du terme français »[4]. Sur ce deuxième critère, nous pouvons même considérer que la création du sigle CPQ peut faciliter l'implantation durable de la version développée « cryptographie

[1] Delisle Jean. op. cit. p. 60.

[2] Agence nationale de la sécurité des systèmes d'information. *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)* [en ligne]. 2023. Disponible sur : <https ://cyber.gouv.fr/sites/default/files/document/Avis-de-l-ANSSI-sur-la-migration-vers-la-cryptographie.pdf> (consulté le 31.10.2023).

[3] Kocourek Rostislav. *La langue française de la technique et de la science*. Wiesbaden : Brandstetter Verlag, 1982. p. 142.

[4] Centrella Maria. op. cit. p. 126.

post-quantique ».

Exemple de traduction de sigle :

After three rounds of evaluation and analysis, NIST has selected the first algorithms it will standardize as a result of the PQC Standardization Process
Après trois étapes d'évaluation et d'analyse, le NIST a sélectionné les premiers algorithmes qui vont devenir des normes à l'issue du processus de normalisation de la CPQ.

Je n'ai pas choisi cette option pour l'intégralité des sigles de mon texte. Le sigle de l'exemple précédent présentait à la fois un niveau de technicité peu élevé pour le domaine et une grande proximité avec l'anglais une fois traduit. Ces conditions n'étaient pas réunies pour d'autres sigles comme l'anglais *KEM*, forme abrégée de *Key-encspulation mechanism*, généralement traduit par « mécanisme d'encapsulation de clé » en français. Il n'existe pas de forme abrégée française de ce terme. Je n'ai pour autant pas fait le choix d'en imaginer un, puisque *MEC*, sans proximité avec l'anglais, n'aurait été compris par aucun spécialiste du domaine. Ce sigle m'a posé un véritable dilemme, que j'ai choisi de trancher à l'aide d'un autre document de l'ANSSI qui m'a semblé plus important, mieux installé dans la hiérarchie des normes que l'avis sur lequel je me suis reposé précédemment. Ce guide[1] définit clairement les mécanismes cryptographiques qu'administrations et entreprises sont contraintes de déployer en France pour assurer leur sécurité. Si les normes internationales qui y sont citées emploient le sigle KEM, le guide utilise systématiquement la forme développée en français. Conformément aux textes sur lesquels je me suis déjà appuyé et à mon postulat traductif, j'ai donc choisi d'opter pour la traduction littérale en développant la forme.

Exemple de traduction développée d'un sigle :

Due to the use of Goppa codes, the KEM has perfect correctness
L'utilisation des codes de Goppa rend ce mécanisme d'encapsulation de clé parfaitement correct.

[1] Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques*. Paris, 2021.

2.2 Un domaine immature

La jeunesse du domaine auquel appartient mon texte-support a également défini ma stratégie de traduction. Elle a nécessité d'avoir souvent recours à des méthodes de création linguistique et terminologique que je vais détailler ici. J'ai également défini une approche du terme « learning with errors », assez problématique dans le cas de ce texte. Ce terme désigne un problème mathématique réputé difficile dans les réseaux euclidiens de grande dimension. Comme je le détaille dans la fiche terminologique que j'ai dédiée au terme, l'équivalent « apprentissage avec erreurs », bien que rare, se retrouve sous la plume de grands spécialistes du domaine comme Damien Stehlé et Adeline Langlois. À ce titre, j'ai choisi de l'intégrer à mon texte-cible, tout en précisant en incise le terme anglais et son sigle attesté qui, quant à lui, est un incontournable du domaine et ne pouvait être traduit pour des raisons analogues à *KEM*. L'exemple ci-dessous traite d'une variante du terme, « apprentissage avec erreur dans les modules de réseaux euclidiens », mais le raisonnement est le même.

Exemple de traduction littérale d'un terme :

KYBER is a module learning with errors (MLWE)-based key encapsulation mechanism with its original design presented in [180].
Le mécanisme d'encapsulation de clé KYBER repose sur le problème de l'apprentissage avec erreurs dans les modules de réseaux euclidiens (module learning with errors, MLWE). L'architecture d'origine du mécanisme est présentée dans cet article [180].

J'ai beaucoup fait appel à la création linguistique et terminologique dans cette traduction. Il s'agissait d'une nécessité afin de rendre dans un français correct des concepts complexes émergents. Si la réponse au problème de traduction est venue d'une approche quantitative menée à l'aide du logiciel de traduction SketchEngine, des solutions qualitatives m'ont également été d'un grand secours. L'informatique et la cryptographie en particulier sont des domaines difficiles à traduire en raison de l'influence de l'anglais pendant la gestation de leur terminologie. Toutefois, la France a l'avantage d'être très représentée parmi les chercheurs à l'origine de cette terminologie. Ainsi, plutôt que de porter la charge de la création linguistique, j'ai eu la chance de pouvoir interagir avec des spécialistes du domaine qui m'ont largement assisté dans ma tâche.

J'aimerais me concentrer ici sur un terme, « dimensions for free ». Ce terme m'a posé de grandes difficultés car il recouvre une notion complexe et n'est accompagné d'aucune explication dans le texte anglais. J'ai douté de ma capacité à trouver un jour un équivalent pour ce terme en voyant qu'il n'était cité que dans un article[1] en dehors de mon texte-support. J'ai choisi de contacter son auteur afin d'avoir une explication du sens de ce terme. M. Ducas, à qui j'ai adressé un courrier électronique en mars, s'est avéré être francophone, et a pu m'expliquer en français le sens qu'il avait donné à ce terme en rédigeant son article.

Dans le détail: pour resoudre SVP, il existait depuis longetemps un algorithme de "crible" (sieving); pour resoudre SVP en dimension n on fesait tourner l'agorithme de crible en dimension n, le tout pour un cout de calcul environ $2^{(0.292n)}$. Cet article montre qu'avec un peu d'astuce, il suffit de faire tourner le crible en dimension $n - d$ pour tout de meme resoudre SVP en dimension n: les d dimensions restantes sont "gratuites", au sens ou le cout est $2^{(0.292(n-d))}$. $n - d$ dimensions payées, d dimensions offertes. En d'autre terme, le coeur de l'algorithme de crible ne change en rien, c'est juste une facon plus efficace de l'utiliser. Sinon je ne parlerai pas de dimension grauite, mais simplement d'une acceleration du crible. Léo Ducas, le 26/03/2024

Ces explications en main, j'ai pu faire le choix de la création linguistique pour la traduction du terme dimensions for free. Le résultat me semble recouvrir la réalité du concept tout en étant concis et idiomatique.

Exemple de création linguistique pour traduire un terme :

(such as the BKZ block size, the number of required BKZ iterations, or the number of dimensions for free)
(comme la taille du bloc BKZ, le nombre d'itérations de l'algorithme BKZ nécessaires ou le nombre de dimensions gratuites)

[1] Ducas Léo. Shortest vector from lattice sieving : A few dimensions for free. *Advances in Cryptology – EUROCRYPT 2018*. Berlin : Springer International Publishing, 2018. pp. 125–145.

3 Une norme pour les normes ?

J'ai choisi de regrouper sous cette section les problèmes de traduction que j'estime liés au type de texte et à sa fonction plus qu'au domaine dans lequel il s'inscrit. Je m'intéresserai dans un premier temps à l'écosystème dans lequel le texte-support s'inscrit, avant de me pencher sur les problèmes proprement traductologiques de la traduction de rapports et de normes.

3.1 S'insérer dans un écosystème

S'il ne se caractérise pas par une production très intense de textes, avec à peu près un rapport tous les deux ans puis, plus récemment, la rédaction de projets de normes, le rapport du NIST que j'ai choisi s'inscrit dans un écosystème de textes déjà fourni. En témoigne la longue bibliographie qui figure à la fin du document ainsi que les trente renvois bibliographiques qui figurent dans l'extrait que j'ai traduit. Ce nombre de mentions bibliographiques répond à une exigence spécifique au type de texte. Ce rapport, puisqu'il s'inscrit dans un processus de normalisation, possède une visée normative. La position d'autorité du NIST apparaît clairement à la lecture. Cette position d'autorité, tirée du fait d'être les créateurs et les arbitres de la compétition, doit cependant être légitimée par des sources fiables et des arguments démontrés.

Pour me positionner face à cette question de la bibliographie, j'ai à nouveau fait appel à mon postulat traductif et à mon public cible. L'ANSSI, organisme normatif également, publie des documents accompagnés d'une bibliographie en fin d'ouvrage. J'ai donc choisi de reporter les sources en fin de texte, dans une section nommée « Bibliographie » en lieu et place de la section « References » en anglais. J'ai également adapté la rédaction des sources biblographiques à la norme de rédaction de l'ANSSI.

Exemple d'adaptation de la rédaction bibliographique pour un article :

[11] Beullens W (2021) Improved cryptanalysis of UOV and Rainbow. Advances in Cryptology – EUROCRYPT 2021, eds Canteaut A, Standaert FX (Springer International Publishing, Cham), pp 348–373.
[11] W. Beullens, Improved cryptanalysis of UOV and Rainbow, *Advances in Cryptology – EUROCRYPT 2021*, pp 348–373, Springer, 2021.

Comme mon texte-support est un document normatif, préparatoire à une norme, les normes précédentes y sont mentionnées. J'ai choisi d'adapter ces normes, par ailleurs déjà fréquemment citées par l'ANSSI, pour m'assurer de la meilleure implantation possible dans l'écosystème d'arrivée.

Exemple d'adaptation de la rédaction bibliographique pour une norme :

[1] National Institute of Standards and Technology (2013) Digital signature standard (DSS) (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards (FIPS) Publication 186-4. https ://doi.org/10.6028/NIST.FIPS.186-4
[1] National Institute of Standards and Technology. *FIPS PUB 186-4 : Digital Signature Standard (DSS)*, 2013. https ://doi.org/10.6028/NIST.FIPS.186-4

Enfin, j'ai adopté une stratégie spécifique pour les trois premiers renvois bibliographiques. Ceux-ci font référence à des normes dont l'intitulé entier est cité dans le corps du texte. Afin de conserver cette mention explicite, qui a un sens bien précis ici, puisque ces normes sont destinées à être supplantées par les normes post-quantiques, j'ai choisi de ne garder que leur nom de code dans le corps du texte et de déplacer la forme développée en bas de page, ce afin d'éviter une accumulation de termes anglais dans le corps du texte cible.

3.2 La langue des rapports

Enfin, j'ai identifié des problèmes directement liés au type de texte-support que j'ai choisi, c'est-à-dire le rapport. Les rapports varient dans leurs destinataires. Souvent le fait de spécialistes du domaine, ils peuvent être destinés à des personnes elles aussi spécialistes comme extérieures au domaine. Cette question du destinataire se ressent évidemment dans les choix de rédaction et de traduction. Ce texte précis a été rédigé par des spécialistes à destination de spécialistes, dans le but d'informer une communauté mondiale de l'avancement du projet porté par le NIST.

Il arrive que ce choix de destinataire et les choix de rédaction qui en découlent entrent en contradiction avec un des autres objectifs de la communication scientifique, celui de la clarté. J'ai choisi comme exemple la phrase « Kyber is a module learning with errors (MLWE)-based key encapsulation mechanism with its original design presented in [180] ». Cette phrase m'a paru illogique dès la première lecture. Une seconde lecture m'a permis

de déterminer que la préposition « with » était en cause. Jean Delisle consacre plusieurs pages à la traduction de cette préposition, résumant le problème en ces termes : « Un des éléments de la clarté tient à la précision des rapports logiques. En traduisant littéralement *with* à sens vaguement causal ou marquant un faux rapport d'accompagnement, on crée une ambiguïté et on fait une entorse à la syntaxe française. »[1]

J'ai choisi de recourir à deux phrases indépendantes pour expliciter le rapport entre ces deux propositions. Ce choix me semble apporter la clarté nécessaire à ce passage, d'autant plus qu'il s'agit de la première ligne évoquant KYBER, un algorithme crucial dans le déroulement du processus de normalisation. La proposition « in », qui introduit sans plus d'explications une référence bibliographique, m'a également paru abrupte au plan de la clarté. J'ai opté pour l'étoffement, traduisant « in » par « dans l'article » afin d'introduire la référence bibliographique.

Exemple d'introduction d'une nouvelle phrase et d'étoffement, dans un objectif de clarté :

KYBER is a module learning with errors (MLWE)-based key encapsulation mechanism with its original design presented in [180].
Le mécanisme d'encapsulation de clé KYBER repose sur le problème de l'apprentissage avec erreurs dans les modules de réseaux euclidiens (module learning with errors, MLWE). L'architecture d'origine du mécanisme est présentée dans l'article [180].

On remarque également dans cet exemple que le français est beaucoup plus clair que l'anglais dans sa gestion des sigles. En anglais, l'incise de « MLWE » entre « module learning with errors » et « -based » nuit à la clarté de la phrase.

Enfin, j'ai sélectionné un autre passage du texte où l'étoffement a été nécessaire pour préserver la clarté. En anglais, l'incise « such as the BKZ block size, the number of required BKZ iterations, or the number of dimensions for free » suggère un bagage cognitif très important, voire trop important même pour des spécialistes. Comme je l'ai déjà indiqué, le terme « dimensions for free » désigne une notion extrêmement spécifique. J'ai choisi d'expliciter le sens du second « BKZ ». J'ai effectué des recherches et trouvé que « BKZ » renvoyait à un algorithme de réduction de réseaux. Les spécialistes du domaine le savent, j'ai toutefois jugé utile pour la clarté de la phrase que le nombre d'itérations

[1] DELISLE Jean. op. cit. p. 456.

faisait référence au nombre de fois où l'algorithme BKZ était exécuté, d'où « le nombre d'itérations de l'algorithme BKZ ».

Exemple d'étoffement à des fins de précision et de clarté :

(such as the BKZ block size, the number of required BKZ iterations, or the number of dimensions for free)
(comme la taille du bloc BKZ, le nombre d'itérations de l'algorithme BKZ nécessaires ou le nombre de dimensions gratuites)

J'ai souhaité montrer avec ces quelques exemples que la traduction d'un rapport rédigé par des spécialistes à destination d'autres spécialistes impose de trouver un équilibre entre la prise en compte de « ce qui va de soi » et la nécessité d'améliorer certaines phrases qui penchent vers l'ambiguïté. La recherche de cet équilibre a constitué, à mon sens, l'un des problèmes les plus intéressants de cette traduction.

Conclusion

Cet exercice de traduction assortie d'une réflexion, auquel ne m'étais jamais réellement prêté, s'est avéré très formateur sur plusieurs plans à la fois. Concernant la traduction dans ce qu'elle a de plus académique, il s'agit du texte dans lequel j'ai pu mettre en œuvre de la manière la plus poussée les enseignements de mes deux années à l'ESIT. L'étalement sur plusieurs mois de la traduction, la longue étape de recherche documentaire et de formation au sujet en amont, ainsi que la précieuse relecture de M. Olivier Blazy ont posé le cadre d'une *traduction en milieu idéal*. L'absence de contrainte de temps pour l'acquisition de connaissances m'a permis de pousser la compréhension et la *déverbalisation* au-delà de ce à quoi les cours et mes stages m'ont habitué. Seule ma traduction du compte-rendu de la Conférence Générale des Poids et Mesures, réalisée au cours de mon stage au BIPM, m'avait déjà permis d'expérimenter ce type de traductions au long cours. Mes deux ans en master m'ont enseigné combien la traduction pouvait être exigeante, en dehors même des conditions particulières au domaine technique concerné.

Ensuite, ce mémoire a été l'occasion d'envisager la traduction sous un angle beaucoup plus systématique, avec l'établissement d'un système terminologique qui vient dialoguer avec la traduction. Je regretterai peut-être, dans ce travail, de n'avoir pas fait suffisamment résonner cette dimension terminologique avec la traduction elle-même, d'avoir trop cloisonné ces deux espaces de réflexion. La rigueur de la rédaction terminologique constitue, avec la déverbalisation, l'enseignement de l'ESIT qui a le plus guidé ma stratégie de traduction pour ce mémoire et dans ma pratique professionnelle. À la façon d'un protocole en chimie ou en physique expérimentale, j'y vois un ensemble de règles et d'étapes à suivre pour s'assurer de produire un travail cohérent et cumulatif, en contribuant à une normalisation de la langue technique.

La stratégie que j'ai mise en œuvre dans le cadre de ce mémoire, imprégnée de mes années d'études en traduction, a déjà eu et continuera d'avoir une influence importante sur mon rapport à la traduction, y compris dans un cadre professionnel.

Quatrième partie

Analyse terminologique

Vedette anglaise	n°	Vedette française
IND-CPA security	01	sécurité IND-CPA
key encapsulation mechanism	02	mécanisme d'encapsulation de clés
lattice-based-cryptography	03	cryptographie basée sur les réseaux euclidiens
learning with errors	04	problème LWE
oracle	05	oracle

COMMENT LIRE UNE FICHE TERMINOLOGIQUE

Les fiches terminologiques ci-après sont constituées de tout ou partie des champs suivants :

VE	VEdette (terme faisant l'objet de la fiche et des synonymes)
EN	ENglish
FR	Français
DF	DéFinition de la vedette
DOM	DOMaine
CTX	ConTeXte
COL	COLlocations
ID	IDentification de l'auteur : Bureau Émetteur (organisme pour lequel la fiche a été rédigée) : ESIT Collection terminologique à laquelle appartient la fiche : MEM24 pour MÉMoire soutenu en 2024 Auteur de la fiche : AAS = Antoine AStruc
NT	NoTes : EXP = renseignements encyclopédiques qui ne font pas partie de la définition USG = indications relatives à l'USaGe, au niveau de la langue, au registre, à la région, etc. GRM = indications GRaMmaticales ETY = ETYmologie DER = mots DERivés HOM = HOMonyme ANT = ANTonyme SPE = termes SPÉcifiques GEN = termes GÉNériques REL = renvois associatifs à d'autres termes
RF	RéFérences (sources bibliographiques)

Choix des vedettes

Ces cinq vedettes extraites de mon texte-support relèvent toutes de la cryptographie, soit de la cryptographie post-quantique spécifiquement (vedettes 03 et 05) soit de la sécurité prouvable en général (vedettes 01, 02 et 05). Toutes désignent des concepts essentiels à la compréhension et à l'articulation logique du texte-support. En effet, il porte sur la démonstration de la sécurité de nouveaux mécanismes d'encapsulation de clé (02), dont le NIST attend une sécurité IND-CPA (01). L'extrait que j'ai choisi porte sur un algorithme de cryptographie basée sur les réseaux euclidiens (03), reposant au plan mathématique sur le problème LWE (04). Enfin, la preuve de la sécurité de ce système fait intervenir des simulations d'attaque et donc un oracle (05).

Si la plupart des traductions proposées sont transparentes ou quasi-transparentes, la réalisation de fiches terminologiques a été motivée par l'extrême jeunesse du domaine et l'absence de traductions attestées et reproduites par des organismes. Si bien qu'en dépit de l'existence de traductions, comme *apprentissage avec erreurs* pour *learning with errors*, la majorité des textes français emploient une vedette anglaise. La cryptographie post-quantique est appelée à grandir dans les années qui viennent, et l'absence de ressources en français concernant des termes aussi fondamentaux qu'*oracle* ou *LWE* pourrait, tôt ou tard, freiner l'élaboration de normes ou le ralentissement de protocoles à l'importance critique.

1 Fiches terminologiques

VE EN	IND-CPA security [1] indistinguishability under chosen plaintext attack [2] indistinguishability against chosen plaintext attack [3]
DF	Property of a cryptographic scheme against which a polynomial time adversary who has access to the ciphertext of any arbitrary plain text message has only a negligible advantage over random guessing.
DOM	mathematics, computation theory
CTX	IND-CPA security is equivalent to semantic security, where an adversary that sees the ciphertext has no advantage against an adversary that does not see the ciphertext. In this paper, we show that IND-CPA security does not imply n-circular security *for any n*.
COL	v. achieve *, break the *, fail *, prove the * * imply adj. game-based *, semantic *
ID	ESIT MEM24 AAS
EXP1	The property of indistinguishability under chosen plaintext attack is equivalent to that of semantic security. Both definitions are often used interchangeably.
EXP2	Most cryptographic schemes are indistinguishable under chosen plaintext attacks (IND-CPA) but also under chosen cyphertext attacks (IND-CCA) and adaptative chosen ciphertext attacks (IND-CCA2). Security under one of these definitions implies security under the previous ones, making IND-CCA2 security the strongest game-based security definition.
USG	[2] recommended NIST term
RF	Gorjan Alagic, Daniel Apon, David Cooper et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.* NISTIR-8413. Gaithersburg : NIST, 2022. 93 p. multigr. [SEC DF][USG] ; Wattenhofer Roger, *Computational Thinking, chapter 3 : cryptography* [Cours]. École polytechnique fédérale de Zurich. [SEC DF][CTX] ; Marcedone Antonio, Orlandi Claudio. Obfuscation ⇒ (IND-CPA Security ⇏ Circular Security) *Cryptology ePrint Archive*. 2013, 690. [CTX] ; Goldwasser Shafrira, Micali Silvio. Probabilistic encryption. *Journal of Computer and System Sciences*. 28 :270-299. 1984. [EXP1] ; Bellare Mihir et al. Relations Among Notions of Security for Public-Key Encryption Schemes. *Advances in Cryptology – CRYPTO '98*. 1999. [EXP2]

VE FR	sécurité IND-CPA [1] indistinguabilité contre les attaques à clairs choisis [2]
DF	Propriété d'un schéma de chiffrement face auquel un attaquant qui a accès à un oracle de chiffrement ne peut obtenir en temps polynomial le moindre bit d'information sur les textes chiffrés.
DOM	mathématiques, informatique théorique
CTX	Nous montrons que pour le chiffrement par bloc, la propriété de permutation super pseudo-aléatoire et l'indistinguabilité contre des attaques à clairs choisis sont équivalentes, sous l'hypothèse que le chiffrement et le déchiffrement aient le même niveau de sécurité contre les attaques non-adaptatives. L'objet de ce paragraphe est de décrire le mode chaîné (CBC Cipher Block Chaining) et de prouver sa sécurité IND-CPA.
COL	v. atteindre la * , garantir la * , prouver la * * implique n. niveau de * , notion de * , propriété de *
EXP1	La propriété d'indistinguabilité contre les attaques à clairs choisis implique celle de sécurité sémantique. La réciproque étant vraie, elles sont considérées équivalentes.
EXP2	L'ANSSI désignant les attaques à chiffrés choisis par le terme attaquants passifs, celle-ci emploie donc le terme sécurité contre les attaquants passifs comme synonyme de sécurité IND-CPA.
USG	[1] terme recommandé
RF	Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005. [SEC DF][CTX] ; Phan Hieu, Guillot Philippe. *Fondements théoriques de la cryptographie.* École Normale Supérieure (Paris). 2020. [CTX][EXP1] ; Agence nationale de la sécurité des systèmes d'information. *Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)* [en ligne]. 2023. Disponible sur : <https ://cyber.gouv.fr/sites/default/files/document/Avis-de-l-ANSSI-sur-la-migration-vers-la-cryptographie.pdf> (consulté le 31.10.2023). [EXP2]

VE FR	key encapsulation mechanism [1] KEM [2]
DF	Cryptographic primitive that relies on public key encryption to allow two parties to obtain a shared secret key for further symmetric encryption.
DOM	theoretical computer science, cryptography
CTX	Recently, in post-quantum cryptography migration, it has been shown that an IND-1-CCA-secure key encapsulation mechanism (KEM) is required for replacing an ephemeral Diffie-Hellman (DH) in widely-used protocols, e.g., TLS, Signal, and Noise.
COL	v. implement * * produce adj. backup * , code-based * , lattice-based * , post-quantum * , quantum-resistant * , secure * , standard * n. * implementation
ID	ESIT MEM24 AAS
EXP1	Once communication is established in both ways, a protocol for secure communication (e.g. TLS or IPsec) has been set up.
EXP2	A key encapsulation mechanism KEM consists of three algorithms : the key generation algorithm *Gen*, the key encapsulation algorithm *Encaps*, and the key decapsulation algorithm *Decaps*.
RF	Shoup Victor. A Proposal for an ISO Standard for Public Key Encryption. *Cryptology ePrint Archive*. 2001, 112. Disponible sur : <https ://ia.cr/2001/112> (consulté le 15/06/2024). [SEC DF] ; Coretti Sandro, Maurer Ueli, Tackmann Björn. A Constructive Perspective on Key Encapsulation. *Number Theory and Cryptography, Lecture Notes in Computer Science*, 2013, vol. 8260, pp. 226–239. [SEC DF][EXP1] ; Jiang Haodong, Ma Zhi, Zhang Zhenfeng. Post-Quantum Security of Key Encapsulation Mechanism against CCA Attacks with a Single Decapsulation Query. *Cryptology ePrint Archive*. 2023, 007. Disponible sur : <https ://ia.cr/2023/007> (consulté le 15/06/2024). [CTX][EXP2] ;

VE FR	mécanisme d'encapsulation de clés [1] mécanisme d'encapsulation de clé [2] mécanisme d'encapsulation de la clé [3]
DF	Protocole cryptographique permettant à deux parties d'établir une communication sécurisée en se transmettant une donnée à partir de laquelle elles peuvent dériver une clé de cryptographie symétrique.
DOM	mathématiques, informatique théorique
CTX	Les mots de passe (effectifs) pw_i sont utilisés pour définir une paire de clés $(sk, pk = g^{sk})$ pour un mécanisme d'encapsulation de clés ElGamal basé sur un mot de passe (KEM).
COL	v. utiliser un * * exécute adj. * déterministe, * hybride, * post-quantique, * sûr n. implantation d'un *
EXP1	L'encapsulation est le moyen de profiter de l'avantage des chiffrements symétriques (le chiffré est de même taille ou légèrement plus grand que le message) et de la capacité à partager un secret des chiffrements asymétriques, grâce à l'utilisation de fonctions de hachage.
EXP2	Le mécanisme d'encapsulation de clé (Key encapsulation mechanism - KEM) est composé de trois algorithmes : un algorithme de génération de clés qui retourne une paire de clés (privée et publique), un algorithme d'encapsulation (Encap) qui utilise la clé publique pour générer une clé symétrique et un chiffré, et un algorithme de décapsulation (Décap) qui utilise la clé privée pour obtenir la même clé symétrique à partir du chiffré reçu.
RF	Nugier Cyrius. *Adaptation d'Outils Cryptographiques pour un Contexte Post-Quantique*. Thèse de doctorat : Réseaux et télécommunications : Université de Toulouse : 2018. [1][SEC DF][EXP1] ; Mortajine Lina. *Analyse d'algorithmes post-quantiques implantables en pratique*. Thèse de doctorat : Microélectronique : Université de Lyon : 2021. [2][SEC DF][EXP2] ; Union internationale des télécommunications. *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes* [En ligne]. Recommandation UIT-T X.1811. 2021. [3] ; Chevalier Céline. *Étude de protocoles cryptographiques à base de mots de passe*. Thèse de doctorat : Informatique : Université Paris 7 Denis Diderot : 2009. [CTX].

VE EN	lattice-based cryptography [1] lattice cryptography [2]
DF	Set of cryptosystems relying on lattice problems and resistant to all known quantum algorithms.
DOM	mathematics, computation theory
CTX	The AVX instruction set has been used before to speed up the computation of lattice-based cryptography, and in particular the number-theoretic transform. In modern lattice cryptography almost all protocols are based on two average-case computational problems : the Short Integer Solution problem (SIS) and the Learning with Errors problem (LWE).
COL	v. break * , use * * meet, * rely, * require adj. post-quantum * , quantum-resistant * , quantum-safe * , n. * algorithm, * system, technique *
ID	ESIT MEM24 AAS
EXP1	Lattice cryptography encompasses many primitives based on serveral sets such as the *learning with errors* problem (LWE), the *learning with errors over rings* problem (rings-LWE) or the *short integer solution over rings problem* (rings-SIS).
RF	Alkim Erdem, Ducas Léo, Pöppelmann Thomas et al. Post-quantum key exchange - a new hope. *Cryptology ePrint Archive*. 2015, 1092. Disponible sur : <https ://ia.cr/2015/1092> (consulté le 16/06/2024). [1][SEC DF][CTX] ; Peikert Chris. Lattice Cryptography for the Internet. *Cryptology ePrint Archive*. 2014, 070. Disponible sur : <https ://ia.cr/2014/070> (consulté le 16/06/2024). [2][EXP1]

VE FR	cryptographie basée sur les réseaux euclidiens [1] cryptographie à base de réseaux [2] cryptographie fondée sur les réseaux [3]
DF	Ensemble des cryptosystèmes reposant sur la difficulté algorithmique de problèmes liés aux réseaux, réputés difficiles y compris pour des ordinateurs quantiques.
DOM	mathématiques, informatique théorique
CTX	Bien que la plupart des propriétés « avancées » d'ABE soient souvent basées sur les couplages de points de courbes elliptiques et donc appartiennent à la cryptographie classique, celles-ci sont petit à petit répliquées en cryptographie basée sur les réseaux euclidiens et donc résistants à l'ordinateur quantique.
COL	v. utiliser la * adj. * post-quantique n. algorithme de *
RF	Stehlé Damien. Algorithmique des réseaux euclidiens et applications. Master Pro ISFA, filière Codes, Cryptographie et Sécurité. 2008. [SEC DF][1] ; Boudgoust Katharina. *Difficulté théorique des variantes algébriques du problème learning with errors*. Thèse de doctorat : Informatique : Université de Rennes : 2021. [SEC DF][2] ; Nugier Cyrius. *Adaptation d'Outils Cryptographiques pour un Contexte Post-Quantique*. Thèse de doctorat : Réseaux et télécommunications : Université de Toulouse : 2018. [CTX] ; Laguillaumie Fabien, Langlois Adeline, Stehlé Damien. Chiffrement avancé à partir du problème Learning With Errors. In *Informatique Mathématique : une photographie en 2014*. Presses universitaires de Perpignan, 2014. [3]

VE EN	learning with errrors [1] LWE [2] learning with errors problem [3] LWE problem [4]
DF	Mathematical problem that consists of distinguishing linear equations with noise from uniformly sampled values.
DOM	mathematics, computation theory
CTX	For an integer $q = q(n)$ and an error distribution $\phi = \phi(n)$ over $\mathbb{T}$, the (worst-case, search) learning with errors problem $LWE_{n,q,\phi}$ in n dimensions is : given access to arbitrarily many independent samples from $A_{s,\phi}$, output s with non-negligible probability. It means that if there exists an efficient solver for LWE, then it can be used to construct a quantum solver for SIVP_γ in the worst case, i.e., in any Euclidean lattice.
COL	v. compute * , solve * adj. average-case * , decision * , hard * , search * , worst-case *
ID	ESIT MEM24 AAS
SPE	Module-LWE, Ring-LWE
EXP1	Due to its computational hardness for both quantum and classical computers, LWE allows for the construction of a large variety of cryptographic schemes.
RF	Balbás David. The Hardness of LWE and Ring-LWE : A Survey. *Cryptology ePrint Archive*. 2021, 1358. Disponible sur : <https ://ia.cr/2021/1358> (consulté le 15/06/2024). [1][2][SEC DF][EXP1] ; Boudgoust Katharina, Jeudy Corentin, Adeline Roux-Langlois et al. On the Hardness of Module Learning with Errors with Short Distributions. *Cryptology ePrint Archive*. 2022, 472. Disponible sur : <https ://ia.cr/2022/472> (consulté le 15/06/2024). [3][4][CTX] ; Goldwasser Shafi, Kalai Yael, Peikert Chris et al. Robustness of the Learning with Errors Assumption. *Innovations in Computer Science*, 2010, pp. 230-240. [CTX]

VE FR	problème LWE [1] LWE [2] problème de l'apprentissage avec erreurs [3] apprentissage avec erreurs [4]
DF	Problème mathématique consistant à retrouver un vecteur secret à partir d'un système d'équations linéaires bruité par un terme d'erreur tiré d'une distribution uniforme.
DOM	mathématiques, algorithmique
CTX	Commençons dans un premier temps par résoudre la version calculatoire de LWE, avec probabilité non-négligeable vis-à-vis de $s \leftarrow U(\mathbb{Z}_q^n)$. Au cœur de la plupart des schémas reposant sur les réseaux euclidiens, et en particulier au centre de cette thèse, se trouve un problème de calcul, celui de l'apprentissage avec erreurs, souvent abrégé LWE (acronyme de l'anglais Learning With Errors).
COL	v. construire * , formuler * , réduire * , résoudre * adj. * calculatoire, * décisionnel n. paramètres du * , primitives * , variantes du *
EXP1	Comme de nombreux problèmes portant sur les réseaux euclidiens, le problème LWE semble à ce jour résister aux attaques quantiques en temps polynomial.
SPE	problème de l'apprentissage avec erreurs dans les modules de réseaux euclidiens, problème de l'apprentissage avec erreurs dans un anneau
RF	Remaud Maxime. *Applications of Quantum Fourier Sampling and the Dihedral Hidden Subgroup Problem.* Thèse de doctorat : Informatique : Sorbonne Université : 2023. [1][2] ; Laguillaumie Fabien, Langlois Adeline, Stehlé Damien. Chiffrement avancé à partir du problème Learning With Errors. In *Informatique Mathématique : une photographie en 2014*. Presses universitaires de Perpignan, 2014. [3][SEC DF][CTX][EXP1] ; Boudgoust Katharina. *Difficulté théorique des variantes algébriques du problème learning with errors.* Thèse de doctorat : Informatique : Université de Rennes : 2021. [CTX]

VE EN	oracle [1] black box [2]
DF	Theoretical machine assumed to be able to efficiently solve any computational problem.
DOM	mathematics, computation theory
CTX	In the classical game, the attacker is given classical access to a decryption oracle used to answer chosen ciphertext queries and to an encryption oracle used to create challenge ciphertexts.
COL	v. implement the *, query the * * compute adj. random * n. decryption *, encryption *
ID	ESIT MEM24 AAS
USG	[1] recommended term
RF	Marquez-Corbella Irene, Sendrier Nicolas, Finiasz Matthieu. *2.2. Security-Reduction Proof , in 2 : McEliece Cryptosystem.* [Vidéo]. Inria, 2015. [SEC DF] ; Boneh Dan, Zhandry Mark, *Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World*. Stanford University. [SEC DF][CTX]

VE FR	oracle [1] boîte noire [2]
DF	Construction abstraite capable de résoudre tout problème calculatoire en une seule opération.
DOM	mathématiques, informatique théorique
CTX	On dit qu'un problème A se réduit polynomialement à un problème B si, il existe un algorithme polynomial qui peut résoudre le problème A en se servant d'un oracle qui résout le problème B.
COL	v. interroger l' *, simuler l'* * calcule, * génère, * renvoie, adj. * aléatoire, * décisionnel n. * de chiffrement, * de déchiffrement
USG	[1] terme recommandé
RF	Phan Hieu, Guillot Philippe. *Fondements théoriques de la cryptographie.* École Normale Supérieure (Paris). 2020. [SEC DF] ; Mariya Georgieva. *Analyse probabiliste de la réduction des réseaux euclidiens cryptographiques.* Thèse : Cryptographie et sécurité : Université de Caen : 2013. [SEC DF][CTX]

2 Glossaire

algorithme	algorithm
Séquence de règles opératoires exécutées sur des données et qui permettent l'obtention d'un résultat. RF : Office québécois de la langue française. *Une intelligence artificielle bien réelle : les termes de l'IA* [en ligne]. 2024. Disponible sur <https ://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/VocabulairesPDF/vocabulaire-intelligence-artificielle.pdf> (consulté le 20/06/2024).	
ANSSI, Agence nationale de la sécurité des systèmes d'information	ANSSI, Fench cybersecurity agency
Autorité française en matière de cybersécurité et de cyberdéfense, chargée de la protection des infrastructures numériques publiques et privées les plus critiques. RF (SEC) : Agence nationale de la sécurité des systèmes d'information. Découvrir l'ANSSI [en ligne]. Disponible sur <https ://cyber.gouv.fr/decouvrir-lanssi> (consulté le 16/06/2024).	
attaque par canaux auxiliaires	side-channel atttack
Attaque exploitant une fuite d'information physique durant l'exécution d'un calcul, comme par exemple l'analyse de la consommation de courant, le rayonnement électromagnétique ou le temps de calcul global. RF (SEC) : Dugardin Margaux. *Amélioration d'attaques par canaux auxiliaires sur la cryptographie asymétrique*. Thèse de doctorat : Électronique et Communications : TELECOM ParisTech : 2017.	
attaque par force brute, recherche exhaustive	bruteforce attack
Technique d'attaque qui consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin se connecter au service ciblé. RF (SEC) : Commission Nationale de l'Informatique et des Libertés. Force brute (attaque informatique) [En ligne]. Disponible sur <https ://www.cnil.fr/fr/definition/force-brute-attaque-informatique> (consulté le 16/06/2024).	
chiffré, cryptogramme	ciphertext
Données résultant d'un chiffrement et dont le contenu sémantique n'est pas disponible sans recours à des techniques cryptographiques. RF : International Organization for Standardization. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015.	

chiffrement asymétrique, chiffrement à clé publique, cryptographie à clé publique	public-key encryption, public-key cryptography
Méthode de chiffrement consistant à chiffrer des données à partir de la clé publique du destinatire, seul à pouvoir ensuite déchiffrer le message à l'aide de sa clé privée. RF (SEC) : Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005.	
chiffrement symétrique, cryptographie symétrique	symmetric-key encryption, symmetric cryptography
Méthode de chiffrement consistant à chiffrer des données à partir d'une clé secrète employée également pour le déchiffrement. RF (SEC) : Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005.	
clair, texte clair	plaintext
Données dont le contenu sémantique est disponible sans recourir à des techniques cryptographiques. RF : International Organization for Standardization. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015.	
code correcteur d'erreurs, code correcteur, CCE	error-correcting code, ECC
Série de bits de contrôle permettant de détecter si des données ont été altérées et si c'est le cas, de reconstituer les données d'origine par un mécanisme de correction. RF (SEC) : IREM de Clermont-Ferrand. *Codes détecteurs et correcteurs d'erreurs* [en ligne]. 2015. Disponible sur <http ://www.irem.univ-bpclermont.fr/IMG/pdf/2FicheScientifique-4.pdf> (consulté le 20/06/2024)	
cœur de processeur, cœur CPU	processor core, CPU core
Unité de calcul d'un processeur permettant d'exécuter une instruction à la fois au rythme de son cycle d'horloge. RF (SEC) : Talbot Jean-Marc. *Architecture des ordinateurs, Processeur : description - fonctionnement - microprogrammation* [en ligne]. Université de Provence. Disponible sur : <https ://pageperso.lis-lab.fr/jean-marc.talbot/Teaching/Archi/cours7_print.pdf> (consulté le 26/06/2024) EXP : Les calculateurs actuels comportent des milliers de coeurs CPU, qui permettent un parallélisme massif mais les résultats sont présentés sur un seul cœur pour une meilleure comparabilité.	

complexité algorithmique, complexité	computational complexity, complexity
Mesure de la difficulté d'un problème à l'aune de l'efficacité des algorithmes disponibles pour le résoudre. RF (SEC) : Perifel Sylvain. *Complexité algorithmique*. Ellipses, 2014, 432 p. SPE : complexité en temps, complexité en espace	
crible algébrique, crible par corps de nombre généralisé, GNFS	general number fields sieve, GNFS
Algorithme classique de factorisation de grands entiers (supérieurs à 10^{100}) le plus efficace disponible actuellement. RF (SEC) : Lavauzelle Julien. *Algorithmes pour l'arithmétique II : Cours 7* [en ligne]. Université Paris 8, 2020. Disponible sur : <https ://www.math.univ-paris13.fr/˜lavauzelle/teaching/2020-21/docs/AA-slides-7.pdf> (consulté le 25/06/2024)	
cryptanalyse	cryptanalysis
Ensemble des méthodes et procédés de décodage visant à rétablir en clair un cryptogramme, sans connaissance préalable de la clé de chiffrement. RF : Office québecois de la langue française ; *Vocabulaire de la sécurité informatique* [en ligne]. 2023. Disponible sur <https ://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/VocabulairesPDF /vocabulaire-securite-informatique.pdf> (consulté le 20/06/2024). EXP : La cryptanalyse permet d'éprouver les procédés de chiffrement issus des recherches en cryptographie.	
cryptographie	cryptography
Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu sémantique, d'empêcher leur utilisation non autorisée ou de permettre la détection de modifications. RF : International Organization for Standardization. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015.	
cryptographie post-quantique	post-quantum cryptography, quantum-resistant cryptography
Ensemble d'algorithmes cryptographiques classiques comprenant les établissements de clés et les signatures numériques et assurant une sécurité conjecturée contre la menace quantique en plus de leur sécurité classique. RF (SEC) : Agence nationale de la sécurité des systèmes d'information. *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique*. Paris, 2022.	

distribution quantique de clés, échange quantique de clés, DQC	quantum key distribution, QCD
Protocole de communication fondé sur les lois de la physique quantique, permettant de transmettre un secret sur un canal de communication avec des preuves de sécurité inconditionnelles. RF (SEC) : Lodewyck Jérôme. *Dispositif de distribution quantique de clé avec des états cohérents à longueur d'onde télécom*. Thèse de doctorat : Laser et Matière : Université Paris XI : 2006. EXP : La DQC nécessite une infrastructure spécifique et ne peut pas encore s'effectuer sur toutes les distances. EXP2 : Le protocole repose généralement sur des photons intriqués.	
distribution uniforme, loi uniforme	uniform distribution
Distribution d'une variable aléatoire dont la densité de probabilité est constante sur un intervalle. RF : Organisation météorologique mondiale, Organisation des Nations Unies pour l'éducation, la science et la culture. *Glossaire international d'hydrologie*. Genève : OMM, 2012. 469 p. multigr.	
fonction de hachage, fonction de hachage cryptographique, fonction de condensation	hash function, cryptographic hash function, hashing function
Fonction qui prend en entrée un message et calcule une empreinte de ce message, de taille fixe et dépendante de tous les bits du message. RF (SEC) : Leurent Gaëtan. *Construction et Analyse de Fonctions de Hachage*. Thèse de doctorat : Informatique : Université Paris Diderot : 2010.	
fonction à sens unique	one-way function
Fonction pour laquelle il est facile et de calculer une image y sachant x mais difficile de retrouver l'antécédent x sachant y. RF (SEC) : Pointcheval David. *Comment sécuriser nos échanges de données ? Confidentialité et anonymat* [en ligne]. Olympiades de Mathématiques : Sorbonne : Paris, 2009. Disponible sur : <https ://www.di.ens.fr/david.pointcheval/Documents/Slides/s2009_olympiades.pdf> (consulté le 26/06/2024)	

fonction à trappe	trapdoor function
Fonction dont l'inversion est aussi facile que le calcul d'image si l'on dispose d'une information secrète. RF (SEC) : Martin Bruno. *Cryptographie à clé publique* [en ligne]. Université de Nice – Sophia Antipolis, 2010. Disponible sur : <https ://webusers.i3s.unice.fr/ƀmartin/4-CS.pdf> (consulté le 26/06/2024)	
intrication quantique, enchevêtrement quantique, intrication	quantum entanglement, entanglement
Phénomène quantique instituant une corrélation et une dépendance entre les états de différents systèmes quantiques, et ce, indifféremment de la distance séparant ces systèmes dans l'espace. RF (SEC) : Jaffali Hamza. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés*. Thèse de doctorat : Informatique : Université Bourgogne Franche-Comté : 2020.	
logarithme discret, problème du logarithme discret	discrete logarithm
Problème algorithmique portant sur l'inversion de la fonction d'exponentiation, considéré difficile pour certains groupes. RF (SEC) : Joux Antoine, Lercier Reynald. Algorithmes pour résoudre le problème du logarithme discret dans les corps finis. In *Nouvelles Méthodes Mathématiques en Cryptographie, Fascicule Journées Annuelles*. Paris : Société mathématique de France, 2007, pp. 23-53.	
mémoire vive, RAM	random access memory, RAM
Mémoire dans laquelle des données peuvent être lues et écrites. RF : International Organization for Standardization. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015. EXP : En anglais, RAM est l'abréviation de « Random-Access Memory », expression dont la signification ne correspond pas à ce que cette abréviation désigne maintenant.	

modèle de l'oracle aléatoire, ROM	random oracle model, ROM
Hypothèse idéaliste selon laquelle le challenger et l'adversaire peuvent faire des requêtes à un oracle qui renvoie une valeur aléatoire, avec pour seule contrainte que si on lui pose deux fois la même requête, alors il doit faire deux fois la même réponse. RF (SEC) : Zimmer Sébastien. *Mécanismes cryptographiques pour la génération de clés et l'authentification.* Thèse de doctorat : Informatique : École Polytechnique : 2008. ; Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005. EXP : Le ROM représente le fonctionnement d'une fonction de hachage idéale.	
modulo, mod	modulo, mod
Opération binaire qui renvoie le reste de la division euclidienne d'un entier naturel par un autre. RF (SEC) : Graham Ronald et al. *Mathématiques concrètes : Fondations pour l'informatique* (trad. Alain Denise). Paris : Vuibert, 2003. 704 p.	
nombre premier, facteur premier	prime number, prime factor
Entier naturel strictement supérieur à 1, n'admettant que deux entiers naturels diviseurs distincts : 1 et lui-même. RF : Jacon Nicolas. *Hisoitre des nombres premiers – 1ère partie : Les nombres premiers de l'antiquité à Riemann* [en ligne]. Université de Franche-Comté. Disponible sur : <https ://njacon.perso.math.cnrs.fr/jacon_Histoiresciences1.pdf> (consulté le 25/06/2024)	
ordinateur quantique	quantum computer
Dispositif de calcul qui exploite les phénomènes d'interférence et d'intrication, ou encore la capacité qu'ont les systèmes quantiques à être dans plusieurs états simultanément. RF (SEC) : Sayrin Clément. *Préparation et stabilisation d'un champ non classique en cavité par rétroaction quantique.* Thèse de doctorat : Physique quantique : Université Paris VI : 2011.	
paramètre, paramètre de sécurité	parameter
Valeur permettant de définir le niveau de sécurité d'un algorithme, généralement la longueur de la clé ou des nombres utilisés pour la générer (dans le cas de RSA). RF (SEC) : Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005. ; Nitulescu Anca. *Introduction à la cryptographie, Cours 6 : Cryptosystèmes, sécurité et attaques* [en ligne]. Université Paris 13, 2016. Disponible sur <https ://www.di.ens.fr/ñitulesc/files/CRYPTO13/cours6.pdf> (consulté le 24/06/2024)	

polynôme	polynomial
Suite de la forme $(a_0, a_1, ..., a_n, 0, 0, 0, ...)$ à coefficients dans $\mathbb{K}$. RF : Bertault Christophe. *Mathématiques en MPSI : Polynômes* [en ligne]. Disponible sur : <http ://christophebertault.fr/documents/coursetexercices/Cours%20-%20Polynomes.pdf> (consulté le 26/06/2024) EXP : En mathématiques, on distingue l'ensemble des polynômes formels (dont la définition est donnée plus haut) de celui des fonctions polynomiales, limité aux fonctions sur $\mathbb{R}$ de la forme $x \to a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ avec $n \in \mathbb{N}$ et $a_0, ..., a_n \in \mathbb{R}$.	
preuve de sécurité	proof of security, security proof
Démonstration formelle de la sécurité d'une primitive cryptographique, par opposition aux méthodes heuristiques. RF (SEC) : Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005. ; Phan Hieu, Guillot Philippe. *Fondements théoriques de la cryptographie.* École Normale Supérieure (Paris). 2020. EXP : Cette démonstration peut obéir à deux approches, l'une par déduction logique, l'autre par réduction au sens de la théorie de la complexité.	
primitive cryptographique, primitive	cryptographic primitive, primitive
Mécanisme cryptographique élémentaire utilisé pour construire un mécanisme de plus haut niveau, généralement un ensemble d'opérations mathématiques. RF (SEC) : Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques.* Paris, 2021.	
problème difficile	hard problem
Problème dont le calcul de la solution nécessite un temps exponentiel en fonction de la taille des données. RF (SEC) :Barsky Daniel, Dartois Ghislain. *Cryptographie Paris 13* [en ligne]. 2010. Disponible sur <https ://www.math.univ-paris13.fr/ƀoyer/enseignement/PolyCrypto2010.pdf> (consulté le 25/06/2024)	
qubit, bit quantique	qubit, quantum bit
Unité de mesure élémentaire de l'information représentant l'état d'un système quantique et pouvant être dans une superposition de deux états de base en fonction de ses amplitudes de probabilité. RF (SEC) : Jaffali Hamza. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés.* Thèse de doctorat : Informatique : Université Bourgogne Franche-Comté : 2020.	

réseau euclidien, réseau	lattice, euclidean lattice
Sous-groupe additif discret de $\mathbb{R}^n$ dans lequel certains problèmes calculatoires deviennent difficiles à mesure que la dimension n augmente. RF (SEC) : Pellet-Mary Alice, *Crytpographie et réseaux euclidiens* [en ligne]. Bordeaux : Université de Bordeaux, 2021. Disponible sur <https ://apelletm.pages.math.cnrs.fr/page-perso/documents/presentations/seminaire_ Licence_Alice.pdf> (consulté le 24/06/2024).	
RSA, cryptosystème RSA	RSA, RSA system
Système de chiffrement reposant sur la difficulté de résoudre le problème de la factorisation d'entiers de grande taille. RF (SEC) : Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques*. Paris, 2021. EXP : Il s'agit du système de chiffrement le plus utilisé dans le monde pour les données commerciales.	
sécurité sémantique	semantic security
Caractéristique d'un cryptosystème garantissant qu'un attaquant ne puisse extraire aucune information en temps polynomial sur un message clair à partir de l'un des chiffrés, en dehors de celles qu'il aurait pu obtenir sans ce chiffré. REF (SEC) : Castagnos Guilhem. *Cours de Cryptologie*. Institut de Mathématiques de Bordeaux. 2024.	
signature numérique	digital signature
Données ajoutées à un message, permettant au destinataire du message de vérifier la source de ce message. REF : International Organization for Standardization. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015.	
spin	spin
Moment cinétique intrinsèque d'une particule en physique quantique. REF (SC) : Bousselin Alain. *Richard Feynman et la mécanique quantique : genèse, développement et pérennité du concept d'intégrale de chemins*. Thèse de doctorat : Épistémologie et histoire des sciences : Université de Pau et des pays de l'Adour : 2021.	

superposition quantique, superposition d'états, superposition	quantum superposition, superposition of states, superposition
Principe de la mécanique quantique en vertu duquel l'état d'un système quantique à deux états peut être donné par une combinaison linéaire de ces deux états. RF (SEC) : Jaffali Hamza. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés*. Thèse de doctorat : Informatique : Université Bourgogne Franche-Comté : 2020.	
temps polynômial	polynomial time
Ordre de grandeur du temps d'exécution d'un algorithme tel qu'il existe une constante k telle que le nombre d'opérations de base que l'algorithme effectue est majoré par $O(n^k)$, où n est la longueur de l'entrée de l'algorithme. RF (SEC) : Eisenbrand Friedrich. *Optimisation discrète, Lecture 10 : L'algorithme du simplexe est-il efficace ?* [en ligne]. École Polytechnique Fédérale de Lausanne, 2011. Disponible sur : <https ://www.epfl.ch/labs/disopt/wp-content/uploads/2018/09/Slides_0605_print.pdf> (consulté le 25/06/2024) REL : temps exponentiel, temps sous-exponentiel	

3 Lexiques

3.1 Lexique français–anglais

Français	Synonymes	Anglais
AES		AES
agilité cryptographique	crypto-agilité	cryptographic agility
algorithme de chiffrement	algorithme cryptographique	encryption algorithm
algorithme de chiffrement par bloc		block cipher algorithm
algorithme de réduction		reduction algorithm
algorithme lll		LLL Algorithm
algorithme post-quantique		post-quantum algorithm
ANSSI	Agence nationale de la sécurité des systèmes d'information	ANSSI
asymptotique		asymptotic
attaque par canaux auxiliaires		side-channel attack
attaque par force brute	recherche exhaustive	brute-force attack
bit de poids faible	bit le moins significatif	least significant bit
bit de poids fort	bit le plus significatif	most significant bit
canal sécurisé		secure channel
chiffré	cryptogramme	ciphertext
chiffrement		encryption
chiffrement asymétrique	chiffrement à clé publique	public-key encryption
chiffrement commutatif		commutative encryption
chiffrement symétrique		symmetric-key encryption
chiffrer		encrypt
clair	texte clair	plaintext
classe de complexité		complexity class
clé de chiffrement		encryption key
clé de déchiffrement		decryption key
clé de session		session key
clé privée		private key
clé publique		public key
clé secrète		secret key
code correcteur d'erreurs	code correcteur, CCE	error-correcting code
code de Goppa	code de géométrie algébrique	Goppa code
code linéaire		linear code
complexité en temps		time complexity
corps fini	corps de Galois	finite field

courbe elliptique		elliptic curve
cryptanalyse		cryptanalysis
cryptographie		cryptography
cryptographie post-quantique		post-quantum cryptography
cryptologie		cryptology
cryptosystème	système de chiffrement, système cryptographique	cryptosystem
cycle d'horloge		clock cycle
déchiffrement		decryption
déchiffrer		decrypt
déterministe		deterministic
distribution de probabilité		probability distribution
distribution uniforme		uniform distribution
durée de calcul		computing time
échange de clés		key exchange
élément aléatoire		random element
espace mémoire	espace de stockage	storage space
espace vectoriel		vector space
établissement de clé		key establishment
état quantique		quantum state
exponentiel		exponential
factoriser		factorize
fonction à sens unique	fonction de chiffrement unidirectionnelle	one-way function
fonction à trappe		trapdoor function
fonction de hachage	fonction de hachage cryptographique, fonction de condensation	hash function
fonction pseudo-aléatoire		pseudorandom fonction
groupe		group
indistinguabilité		indistinguability
infalsifiable		unforgeable
informatique quantique		quantum computing
intrication quantique	enchevêtrement quantique	quantum entanglement
itération		iteration
jeu de paramètres	paramètre	parameter set
logarithme discret	problème du logarithme discret	discrete logarithm
logiciel		software
matériel	matériel informatique	hardware

matrice		matrix
mécanisme d'encapsulation de clé	KEM	key encapsulation mechanism
modèle de l'oracle aléatoire	ROM	random oracle model
modèle de l'oracle aléatoire quantique	QROM	quantum random oracle model
modulo	mod	modulo
NIST		NIST
nombre premier		prime number
np-difficile		np-hard
oracle	boîte noire	oracle
ordinateur classique		classical computer
ordinateur quantique		quantum computer
paradoxe des anniversaires		birthday paradox
paramètre de sécurité	niveau de sécurité	security level
permutation aléatoire		random permutation
polynôme		polynomial
polynôme formel	anneau des polynômes formels	polynomial ring
porte logique	porte	logic gate
preuve de sécurité		security proof
primitive cryptographique	primitive	cryptographic primitive
primitive post-quantique		post-quantum cryptographic primitive
probabiliste		probabilistic
problème LWE	LWE, problème de l'apprentissage avec erreurs, apprentissage avec erreurs	learning with errors
problème difficile		hard problem
problème du vecteur le plus court	problème svp	shortest vector problem
qubit	bit quantique	qubit
réseau	réseau euclidien	lattice
RSA	cryptosystème Rivest–Shamir–Adleman	RSA
schéma de chiffrement		encryption scheme
schéma de signature numérique	schéma de signature	digital signature scheme
sécurité sémantique		semantic security
sous-espace		subspace
spin		spin
superposition		supersposition

temps polynomial		polynomial time
test de performance		benchmark
valeur moyenne		mean value
variable aléatoire		random variable
vecteur		vector

3.2 Lexique anglais–français

Anglais	Synonymes	Français
AES	Advanced Encryption Standard, Rijndael	AES
ANSSI	French Cybersecurity Agency	ANSSI
asymptotic		asymptotique
benchmark		test de performance
birthday paradox		paradoxe des anniversaires
block cipher algorithm	block cipher	algorithme de chiffrement par bloc
brute-force attack	brute-force search, brute force attack	attaque par force brute
ciphertext		chiffré
classical computer		ordinateur classique
clock cycle		cycle d'horloge
commutative encryption		chiffrement commutatif
complexity class		classe de complexité
computing time		durée de calcul
cryptanalysis		cryptanalyse
cryptographic agility	crypto-agility	agilité cryptographique
cryptographic primitive	primitive	primitive cryptographique
cryptography		cryptographie
cryptology		cryptologie
cryptosystem	cyptography system, cryptographic system	cryptosystème
decrypt	decipher	déchiffrer
decryption	decipherment, deciphering	déchiffrement
decryption key	deciphering key, decipherment key	clé de déchiffrement
deterministic	determinist	déterministe
digital signature scheme	signature scheme	schéma de signature numérique
discrete logarithm		logarithme discret
elliptic curve		courbe elliptique
encrypt	cipher, encipher	chiffrer
encryption	encipherment, enciphering	chiffrement
encryption algorithm	cryptographic algorithm, encipherment algorithm	algorithme de chiffrement
encryption key	enchipherment key	clé de chiffrement
encryption scheme	encipherment scheme	schéma de chiffrement

error-correcting code	ECC	code correcteur d'erreurs
exponential		exponentiel
factorize	factor	factoriser
finite field	Galois field	corps fini
Goppa code	Algebraic geometry code, AG code	code de Goppa
group		groupe
hard problem		problème difficile
hardware		matériel
hash function	cryptographic hash function, hashing function	fonction de hachage
indistinguability		indistinguabilité
iteration		itération
key encapsulation mechanism	KEM	mécanisme d'encapsulation de clé
key establishment		établissement de clé
key exchange	key distribution	échange de clés
lattice	euclidean lattice	réseau euclidien
learning with errors	LWE, learning with errors problem, LWE problem	problème d'apprentissage avec erreurs
least significant bit	LSB, low-order bit	bit de poids faible
linear code		code linéaire
LLL Algorithm	Lenstra–Lenstra–Lovász lattice basis reduction algorithm	algorithme lll
logic gate	gate	porte logique
matrix		matrice
mean value		valeur moyenne
modulo	mod	modulo
most significant bit	MSB, high-order bit	bit de poids fort
NIST	National Institute of Standards and Technology	NIST
np-hard		np-difficile
one-way function		fonction à sens unique
oracle	black box	oracle
parameter set	parameter	jeu de paramètres
plaintext		clair
polynomial		polynôme
polynomial ring	polynomial algebra	polynôme formel
polynomial time		temps polynomial

post-quantum algorithm		algorithme post-quantique
post-quantum cryptographic primitive	post-quantum primitive	primitive post-quantique
post-quantum cryptography	PQC	cryptographie post-quantique
prime number		nombre premier
private key		clé privée
probabilistic		probabiliste
probability distribution		distribution de probabilité
pseudorandom fonction		fonction pseudo-aléatoire
public key		clé publique
public-key encryption	PKE	chiffrement asymétrique
quantum computer		ordinateur quantique
quantum computing		informatique quantique
quantum entanglement		intrication quantique
quantum random oracle model	QROM	modèle de l'oracle aléatoire quantique
quantum state		état quantique
qubit	quantum bit	qubit
random element		élément aléatoire
random oracle model	ROM	modèle de l" oracle aléatoire
random permutation		permutation aléatoire
random variable		variable aléatoire
reduction algorithm		algorithme de réduction
RSA	Rivest–Shamir–Adleman cryptosystem	RSA
secret key		clé secrète
secure channel		canal sécurisé
security level		paramètre de sécurité
security proof		preuve de sécurité
semantic security		sécurité sémantique
session key		clé de session
shortest vector problem	svp problem	problème du vecteur le plus court
side-channel attack		attaque par canaux auxiliaires
software		logiciel
spin		spin
storage space		espace mémoire
subspace		sous-espace
superposition		superposition

symmetric-key encryption	symmetric cryptography, symmetric encryption	chiffrement symétrique
time complexity		complexité en temps
trapdoor function		fonction à trappe
unforgeable		infalsifiable
uniform distribution		distribution uniforme
vector		vecteur
vector space		espace vectoriel

Cinquième partie

Bibliographie

Avertissement au lecteur

Cette bibliographie critique et sélective ne prend en compte que les sources les plus importantes du domaine, et n'inclut donc pas toutes les sources qui ont été consultées pour rédiger ce mémoire. Certaines références bibliographiques mentionnées dans d'autres parties de ce mémoire ne sont ainsi pas présentes ici. Les commentaires de chaque référence sont encadrés. Les « incontournables », c'est-à-dire les ouvrages structurants pour le domaine, sont précédés d'une étoile (★).

Les sources mentionnées dans cette bibliographie critique présentant pour la plupart un niveau de spécialisation très élevé, la compréhension de leur contenu dans toute sa profondeur échappera à tous les non-spécialistes du domaine, en dépit parfois de solides connaissances en mathématiques, informatique et physique. Je ne porterai donc un jugement que sur les parties les plus vulgarisées, souvent introductives, des sources mentionnées.

1 Bibliographie en langue française

1.1 Ouvrages

★ Guillot Philippe, *La cryptologie, l'art des codes secrets*. Les Ulis : EDP Sciences, 2013. 196 p. ISBN 978-2759808113

> Ce livre constitue l'ouvrage d'initiation à la cryptologie incontournable. Son auteur est professeur de cryptologie à l'Université Paris 8 et donc auteur de documents plus spécialisés mais celui-ci s'adresse aux néophytes. Certains passages présentent tout de même quelques difficultés théoriques. L'ouvrage offre une très bonne vue d'ensemble de la cryptographie comme science, des schémas symétriques et asymétriques, de la cryptanalyse, de la sécurité prouvable et propose même une ouverture sur la cryptanalyse quantique au chapitre 7. Je recommande sa lecture à toute personne désireuse de se former sur les enjeux de la cryptologie dans le contexte actuel. Le cours donné par Philippe Guillot et Duong Hieu Phan à l'Université Paris 8 contient quant à lui la formalisation mathématique des notions présentées dans cet ouvrage.

★ Collectif anonyme. *Guide d'Autodéfense Numérique (6e édition)*. Éditions tahin party, 2023. 570 p. ISBN 978-2912631053

> Rédigé par un collectif militant engagé pour la défense de la vie privée, ce guide mis à jour pour la dernière fois en 2023 décrit le fonctionnement des principaux protocoles de communication numérique, les attaques auxquelles ils sont vulnérables et comment s'en prémunir. Les auteurs se définissent comme passionnés mais non-spécialistes, la terminologie n'en reste pas moins très riche et l'adaptation à un public néophyte excellente. La seconde partie de l'ouvrage est conçue comme un véritable manuel et donne des outils très concret pour se protéger. Le collectif a choisi une approche expérientielle que j'ai également essayé d'adopter pour mon mémoire, en n'utilisant que des logiciels libres (LaTeX, *Scribus*, *Inkscape*, *Debian GNU/Linux*, etc.) et en optant pour une publication sous *Copyleft* qui autorise la diffusion, la reproduction et la modification de l'ouvrage.

1.2 Articles

★ Laguillaumie Fabien, Langlois Adeline, Stehlé Damien. Chiffrement avancé à partir du problème Learning With Errors. In *Informatique Mathématique : une photographie en 2014*. Presses universitaires de Perpignan, 2014.

Cet article est l'un des rares articles de cryptographie basée sur les réseaux euclidiens rédigé en français et publié dans un ouvrage français. Il présente une grande richesse terminologique dans le sous-domaines des problèmes sur les réseaux euclidiens, qu'il définit et contextualise vis-à-vis de la cryptanalyse quantique. Je le considère à ce titre comme un incontournable de la cryptographie basée sur les réseaux euclidiens.

1.3 Diplômes

★ Phan Hieu. *Sécurité et efficacité des schémas cryptographiques.* Thèse de doctorat : Informatique : École Polytechnique : 2005.

Cette thèse de doctorat ayant été rédigée en 2005, la cryptographie post-quantique n'y est pas évoquée. Elle aborde toutefois avec une certaine limpidité des notions essentielles en sécurité prouvée pour le chiffrement symétrique comme asymétrique au chapitre 1. Ces notions, détaillées dans les chapitres 2 et 3, s'appliquent tout aussi bien à la cryptographie classique que post-quantique et font de cette thèse un point de départ fondamental pour une réflexion sur la cryptographie moderne.

Nugier Cyrius. *Adaptation d'Outils Cryptographiques pour un Contexte Post-Quantique.* Thèse de doctorat : Réseaux et télécommunications : Université de Toulouse : 2018.

Moins théorique que les sources précédentes, ce travail de thèse s'intéresse à la mise en œuvre concrète des cryptosystèmes post-quantiques et aux moyens de réduire les ressources nécessaires aux calculs. Le chapitre 1 présente des notions importantes aux plans théorique comme pratique, tandis que le chapitre 4, qui traite des architectures matérielles émergente, permet de prendre une hauteur appréciable sur un sujet qui va bien au-delà des mathématiques. La liste bilingue des abréviations sera d'une utilité certaine au traducteur comme au terminologue. Cette thèse est également l'une des rares thèses de CPQ à présenter les notions de bases du calcul quantique.

Jaffali Hamza. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés.* Thèse de doctorat : Informatique : Université Bourgogne Franche-Comté : 2020.

Cette thèse de doctorat traite de la théorie de l'information quantique. Son auteur y décrit la formalisation mathématiques des phénomènes quantiques et établit le lien entre ces derniers et le parallélisme massif que peut permettre le calcul quantique. La partie II analyse en profondeur les algorithmes de Grover et de Shor, qui sont les pierres angulaires de la cryptanalyse quantique. Il s'agit d'un travail riche en terminologie qui m'a apporté de précieux éléments de compréhension de l'informatique quantique.

Mortajine Lina. *Analyse d'algorithmes post-quantiques implantables en pratique.* Thèse de doctorat : Microéléctronique : Université de Lyon : 2021.

Ce travail de thèse aborde la cryptographie post-quantique de manière assez large, en traitant les codes correcteurs d'erreurs (partie I) et les réseaux euclidiens (partie II). La microélectronique sur laquelle sont déployés les systèmes est également étudiée, ce qui n'est pas si fréquent dans les thèses en cryptographie. S'agissant d'une production récente, l'influence du processus de normalisation du NIST est palpable. Trois des algorithmes candidats sont étudiés : CRYSTALS-Dilithium, ROLLO et NTRU.

Deneuville Jean-Christophe/ *Contributions à la Cryptographie Post-quantique*. Thèse de doctorat : Informatique : Université de Limoges : 2016.

> Cette thèse rédigée en 2016 aborde la cryptographie selon la dichotomie classique entre les techniques basées sur les réseaux euclidiens et celles basées sur les codes correcteurs d'erreurs. Il s'agit de la thèse la plus ancienne sur laquelle je me suis appuyé pour la rédaction de ce mémoire. Le domaine de la CPQ a subi de nombreuses mutations depuis 2016, rendant son contenu peut-être moins pertinent pour le terminologue que les ouvrages précédents. Le travail sur les paramètres permettant d'agir sur les coûts calculatoires des algorithmes de CPQ m'ont tout de même été très utiles.

1.4 Cours

★ Phan Hieu, Guillot Philippe. *Fondements théoriques de la cryptographie*. École Normale Supérieure (Paris). 2020.

> Ce cours donné devant les étudiants de Master 2 de l'Université Paris 8 présente la construction et la preuve de sécurité des schémas cryptorgaphiques d'un point de vue mathématique. Sa rédaction est soigneuse et sa lecture fluide, faisant du polycopié un excellent support de travail pour la terminologie ou la traduction. Le document comporte également une introduction à la cryptographie très instructive. Au-delà des formalisations mathématiques, il s'agit selon moi d'un document de référence en matière de sécurité prouvable.

Castagnos Guilhem. *Cours de Cryptologie*. Institut de Mathématiques de Bordeaux. 2024.

> Rédigé en 2024, ce cours de l'Institut de Mathématiques de Bordeaux fournit une terminologie actualisée et couvre l'ensemble de la cryptographie, à l'exception de la cryptographie post-quantique. Je m'en suis servi pour affiner mon traitement des signatures numériques dans ma traduction, sur les conseils de M. Blazy.

1.5 Rapports

Agence nationale de la sécurité des systèmes d'information. *Guide de sélection d'algorithmes cryptographiques*. Paris, 2021.

> Ce document publié de manière régulière par l'ANSSI lorsque de nouvelles normes cryptographiques sont publiées représente l'une des meilleures sources officielles en matière de cryptographie en France. Il offre un tour d'horizon des différents systèmes existants, proposant même pour certains une explication du problème qui sous-tend la primitive. Je le considère à ce titre comme une lecture importante, en dépit de l'aspect abrupt du document. Il s'agit également de l'un des rares supports à traiter du déploiement concret d'un cryptosystème.

Union internationale des télécommunications. *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes*. Recommandation UIT-T X.1811. 2021.

> Cette recommandation de l'UIT concerne les appareils 5G, encadrés par la norme IMT-2020 émise par ce même organisme. Son champ d'application est donc plus réduit que celui de cet exposé. J'ai également choisi de traiter certains termes d'une manière différente par rapport à cette norme, me calquant en priorité sur les articles de recherche rédigés au sein d'universités françaises. J'ai choisi d'inclure la recommandation à cette bibliographie car il s'agit de l'un des rares rapports en français émis par des autorités internationales en matière de sécurité informatique.

1.6 Glossaires, lexiques, vocabulaires

★ International Organization for Standardization, International Electrotechnical Commission. *Technologies de l'information — Vocabulaire*. Norme ISO/IEC 2382 :2015(fr). 2015.

> Disponible en anglais et en français, ce voacbulaire rédigé par un groupe de travail rassemblant l'ISO et l'IEC constitue le glossaire de référence s'agissant des technologies de l'information.

2 Bibliographie en langue anglaise

2.1 Articles

Regev Oded. *On lattices, learning with errors, random linear codes, and cryptography.* 2005.

Avec plus de 5000 citations, cet article d'Oded Regev est l'un des plus cités de l'histoire de la cryptographie post-quantique. D'une extrême technicité, il traite du lien mathématique entre les problèmes basés sur les réseaux euclidiens, sur les courbes elliptiques et sur les codes correcteur d'erreurs. Son résumé est toutefois accessible, et l'ensemble de l'article propose une terminologie très intéressante pour les travaux de traduction.

2.2 Ouvrages

★ Bernstein Daniel et al. *Post-Quantum Cryptography.* Berlin : Springer. 2006.

Cet ouvrage regroupe les diverses interventions du premier atelier sur la cryptographie post-quantique qui s'est tenu en 2006 à l'université catholique de Louvain. Il couvre l'étendue de la cryptographie post-quantique, domaine encore émergent en 2006. En dépit de sa date de publication désormais assez ancienne, je considère cet ouvrage comme un point de départ important concernant la cryptographie post-quantique.

★ Bub Jeffrey. *Bananaworld : Quantum Mechanics for Primates.* Oxford : Oxford University Press, 2016. 288 p. ISBN 978-0198718536

J'ai utilisé cet article comme introduction personnelle aux notions de non-localité et d'intrication en physique quantique. L'auteur fait en effet le pari de vulgariser ces phénomènes microscopiques absolument contre-intuitifs avec une métaphore de bananes magiques. Derrière les bananes se cache la formalisation mathémtique de la physique quantique (qui est par définition impossible à observer). Le livre ne contient cependant pas d'équations complexes et s'adresse à tous les lecteurs dotés d'une appétence pour les sciences. Je le considère à ce titre comme une lecture incontournable lorsque l'on s'intéresse aux propriétés du calcul quantique.

2.3 Cours

★ Boneh Dan, Shoup Victor. *A Graduate Course in Applied Cryptography* [en ligne]. 6^{e} édition. 2023. Disponible sur <https ://toc.cryptobook.us/book.pdf>.

Ce cours de cryptographie de 1130 pages couvre l'intégralité de la théorie crypotgraphique actuelle. Mis à jour régulièrement par ses auteurs, il regroupe l'état de l'art des techniques et de leurs applications. Ce cours de référence le restera sûrement suite à ses prochaines mises à jour. Quelle que soit la notion de cryptographie moderne que vous cherchiez, celle-ci est couverte par les auteurs. Cette exhaustivité combinée à la mise à disposition gratuite du livre en fait un ouvrage de référence.

2.4 Rapports

★ Chen Lily et al. *Report on Post-Quantum Cryptography.* NISTIR-8105. Gaithersburg : NIST, 2016. 15 p. multigr.

Ce rapport constitue la pierre angulaire des futures normes cryptographiques post-quantiques. Publié par des chercheurs du NIST en 2016, il marque le début de l'initiative de normalisation d'algorithmes par l'organisme. Les auteurs reviennent sur la nature de la menace quantique, présentent les solutions envisagées pour y répondre et donnent des directives qui jettent les bases du processus de normalisation. Il s'agit d'un texte incontrournable car à l'origine d'un élan mondial. Il s'agit du texte qui m'a donné envie de centrer mon mémoire sur la cryptographie post-quantique.

2.5 Normes

★ National Institute of Standards and Technology. *Module-Lattice-based Key-Encapsulation Mechanism Standard*. Projet de norme FIPS 203. 2023.

Ce projet de norme publié par le NIST en août 2023 concerne un mécanisme d'encapsulation de clé post-quantique dont la sécurité repose sur un problème sur les réseaux euclidiens dérivé de l'algorithme CRYSTALS-Kyber. Ouvert aux commentaires depuis sa publication et appelé à être bientôt supplanté par la norme définitive, ce document représente l'aboutissement de 7 ans de travail de normalisation d'un schéma de chiffrement asymétrique post-quantique. À ce titre, la terminologie qu'il contient est ce qui s'approche le plus, à ce jour, d'une terminologie normalisée pour la cryptographie post-quantique. Il s'agit donc d'un texte incontournable en langue anglaise.

★ National Institute of Standards and Technology. *Module-Lattice-based Digital Signature Standard*. Projet de norme FIPS 204. 2023.

Ce projet de norme, publié en même temps que FIPS 203 et FIPS 205, concerne quant à lui un algorithme de signature numérique post-quantique. Il revêt à ce titre une importance comparable à FIPS 203 et FIPS 205.

★ National Institute of Standards and Technology. *Stateless Hash-based Digital Signature Standard*. Projet de norme FIPS 205. 2023.

Ce projet de norme, publié en même temps que FIPS 203 et FIPS 204, concerne également un algorithme de signature numérique post-quantique. Il revêt à ce titre une importance comparable à FIPS 203 et FIPS 204.

Index