... ZAOULI N°10, Vol. 7, Août 2025, pp. 692-718 ISSN : 2788-9343

**Soumission** : **03/06/2025** **Acceptation : 01/07/2025** **Publication** : **25/08/2025**

# Développement de systèmes cryptographiques post-quantiques propres à la Côte d'Ivoire : opportunité pour une indépendance dans la protection des données

**Célestin Désiré MELEDJE**
Université NANGUI ABROGOUA (UNA),
Abidjan, Côte d'Ivoire,
Email : desiremeledje@gmail.com

**Michelle TOPE Epse GUEU**
Université Félix Houphoët-Boigny (UFHB),
Abidjan, Côte d'Ivoire
Email : michelletope@yahoo.fr

**Amah Louise Chantal ANDJOU**
Institut des Sciences et Techniques
de la Communication (ISTC)
Abidjan, Côte d'Ivoire
Email : chandjou2015@gmail.com

***Résumé***
*L'évolution du trafic des données via Internet en Afrique et notamment en Côte d'Ivoire croit de manière exponentielle. Les organisations publiques ou privées utilisent généralement la cryptographie classique pour assurer la sécurité des données surtout celles qui doivent rester secrètes. Malgré ce fait, on constate toujours une forte augmentation des atteintes à la confidentialité des données par les hackers et/ou par les propriétaires des logiciels installés sur les systèmes informatiques. Et, cela est perceptible grâce aux médias.*
*Le présent document vise à proposer le développement de systèmes cryptographiques post-quantiques propres à la Côte d'Ivoire. La cryptographie*

*post-quantique permet de garantir la sécurité des données face à un attaquant disposant d'un ordinateur quantique.*
*Le développement de ce système post-quantique devra se faire par des équipes avec trois parties prenantes qui sont l'autorité politique, le secteur privé et les spécialistes du domaine de la cryptographie post-quantique. Ce système post-quantique devra d'une part, tenir compte des dernières recherches et avancées dans le domaine de la cryptographie post-quantique, notamment des meilleurs algorithmes post-quantiques sélectionnés par les États-Unis, après une étude documentaire et des entretiens individuels. D'autre part, il devra aussi tenir compte des spécificités de la Côte d'Ivoire.*

***Mots clés :*** *Cryptographie post-quantique, données, média, sécurité.*

## Development of post-quantum cryptographic systems specific to Côte d'Ivoire: an opportunity for independence in data protection

***Abstract***
*Internet data traffic in Africa, and particularly in Côte d'Ivoire, is growing exponentially. Public and private organizations generally use traditional cryptography to ensure data security, especially for data that must remain confidential. Despite this, there has been a sharp increase in breaches of data confidentiality by hackers and/or the owners of software installed on computer systems. This is evident in the media.*
*This document aims to propose the development of post-quantum cryptographic systems specific to Côte d'Ivoire. Post-quantum cryptography ensures data security against attackers with quantum computers.*
*The development of this post-quantum system will require teams comprising three stakeholders: political authorities, the private sector, and specialists in the field of post-quantum cryptography. This post-quantum system must, on the one hand, take into account the latest research and advances in the field of post-quantum cryptography, in particular the best post-quantum algorithms selected by the United States after a documentary study and individual interviews. On the other hand, it must also take into account the specific characteristics of Côte d'Ivoire.*

*Keywords: Post-quantum cryptography, data, media, security.*

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

## Introduction

Internet est devenu aujourd'hui un outil quasi indispensable aussi bien pour les particuliers, les organisations privées que les administrations publiques et cela, dans tous les pays du monde. Ce fait a été mis en évidence par la crise sanitaire mondiale de la Covid-19. En effet, pendant cette période de crise, les activités administratives, économiques et sociales ont pu continuer grâce à Internet. On peut citer en particulier certains services offerts par le biais d'Internet comme la visioconférence, les réseaux sociaux, le télétravail, etc.

Depuis l'année 2010, on constate une augmentation exponentielle de l'utilisation d'Internet en Afrique subsaharienne. Cette évolution est encore plus forte en Côte d'Ivoire [1]. Ce fait est montré par les données de la banque Mondiale illustrées à la figure 1. Cette évolution de l'utilisation d'Internet en Côte d'Ivoire concerne aussi bien les particuliers, les entreprises privées que les administrations publiques. Cette grande utilisation d'Internet entraîne un volume important de données, sensibles ou non, à protéger.

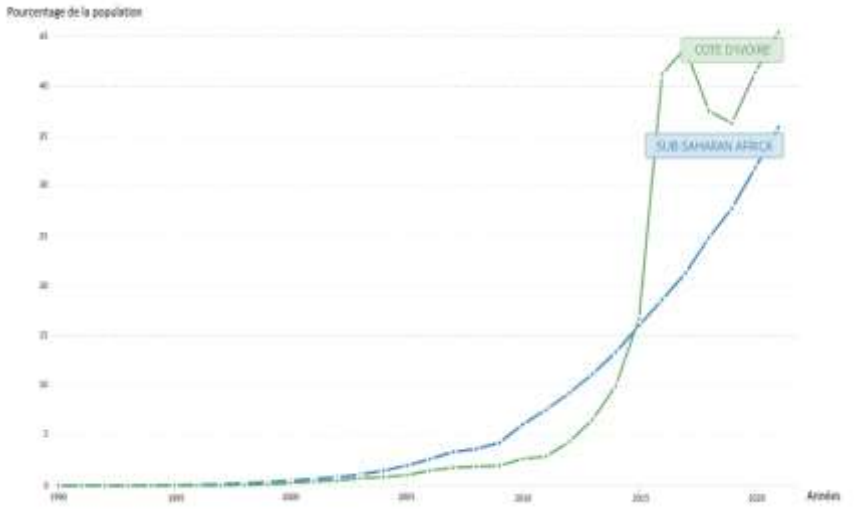


**Figure 1 : Evolution de la population de l'Afrique subsaharienne utilisant Internet [1].**

Pour la protection de toutes ces données, les organisations publiques ou privées en Côte d'Ivoire ou à l'étranger utilisent la cryptographie. La cryptographie est la science qui consiste à rendre des données illisibles pour ceux qui ne sont pas autorisés à y accéder en utilisant les mathématiques. La cryptographie consiste à transformer des données lisibles appelées textes en clair en des données illisibles appelées texte chiffré ou encore texte crypté à l'aide d'algorithme de cryptographie. L'algorithme de cryptographie utilise une clé pour crypter le texte en clair et décrypter le texte chiffré. Lorsque la même clé permet de chiffrer et déchiffrer, on parle de cryptographie symétrique. Quand on utilise deux clés différentes, l'une pour crypter et l'autre pour décrypter, on parle alors de cryptographie asymétrique ou cryptographie à clé publique. Les technologies de

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

cryptographie classique sont utilisées par les administrations publiques, les organisations privées et même les particuliers pour authentifier la source, protéger la confidentialité et assurer l'intégrité des informations stockées sur les disques durs des ordinateurs ainsi que les données transitant sur le réseau Internet [2].

Cependant, on constate de nos jours une forte augmentation des atteintes à la confidentialité des données. Les médias nationaux et internationaux font régulièrement états de toutes ces violations de la sécurité des données informatiques des organisations privées ou publiques. Cette violation de la sécurité affecte tous les pays et entrainent très souvent des perturbations majeures au niveau des états. Aux Etats-Unis, le plus grand opérateur d'oléoducs pour produits raffinés, le groupe Colonial Pipeline, a été frappé par un *ransomware* (logiciel malveillant qui prend en otage des données personnelles d'un ordinateur en les cryptant jusqu'à ce que la victime paie une rançon) en 2021. Cet incident de sécurité, a entrainé l'arrêt du fonctionnement d'un oléoduc de 8800 kilomètres transportant du diesel et de l'essence depuis Houston jusqu'à New York, approvisionnant 45% de la côte Est des Etats Unis [3]. En France, l'assureur Axa fait l'objet d'une attaque du même type. L'assureur français a déclaré en mai 2021, que l'une de ses unités commerciales asiatiques a été victime d'une "attaque ciblée par *ransomware*". L'assureur a indiqué que sa filiale Axa Partners a été victime d'une intrusion dans son système qui a touché ses activités en Thaïlande, en Malaisie, à Hong Kong et aux Philippines [3].

De plus, l'avènement des ordinateurs quantiques a remis en question la sécurité des algorithmes cryptographiques

classiques. En effet, la cryptographie symétrique et la cryptographie asymétrique ont été rendues obsolète par les capacités des ordinateurs quantiques [2]. Par exemple, le RSA [4] principal algorithme de cryptographie asymétrique base sa robustesse sur la difficulté à factoriser un grand nombre premier. En effet, il faut un temps exponentiel pour factoriser un grand nombre premier [5]. Cependant, les algorithmes de Shor [6] et de Groover [7] implémentés dans un ordinateur quantique permet de factoriser un grand nombre premier en un temps polynomial [8]. Autrement dit, la puissance de calcul des ordinateurs quantiques permet de réaliser en quelques heures des calculs qui demandent aujourd'hui des semaines ou des mois de travail aux meilleurs superordinateurs [9]. Les ordinateurs quantiques fragilisent donc les systèmes de cryptographie classique utilisés dans le monde. Aujourd'hui, des états comme les Etats-Unis et la Chine disposent d'ordinateurs quantiques.

Face à ce péril, les chercheurs en cryptographie ont travaillé à proposer de nouvelles méthodes de cryptographies qui soient capables de résister à la puissance des ordinateurs quantiques. Ce type d'algorithmes cryptographiques a été appelé cryptographie post-quantique. La cryptographie post-quantique permet donc de garantir la sécurité des données face à un attaquant disposant d'un ordinateur quantique.

L'étude vise à proposer le développement de systèmes cryptographiques post-quantiques propres à la Côte d'Ivoire. De manière plus spécifique, elle décrire les actions à mener et le travail à faire pour la Côte d'Ivoire afin que celle-ci dispose de ses propres algorithmes cryptographiques post-quantiques.

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

La présente étude est organisée autour de trois axes. D'abord, le premier axe est relatif à l'implication des médias dans le processus de développement de la cryptographie post-quantique en Côte d'Ivoire, ensuite le second traite des algorithmes candidats sélectionnés par le NIST et enfin le troisième est une méthodologie de mise en œuvre d'algorithme post-quantique en Côte d'Ivoire ainsi que les résultats attendus.

## 1. L'implication des médias dans le processus de développement de la cryptographie post-quantique en Côte d'Ivoire

L'étude documentaire et les entretiens réalisés révèle des conséquences paradoxales dans la contribution des médias au développement de la cryptographie post-quantique en Côte d'Ivoire. Les conséquences sont d'abord positives pour le monde des médias. En effet, la cryptographie permettra de sécuriser le contenu des médias numériques à travers la lutte contre le piratage. Les informations publiées par les journalistes seront donc stabilisées et consolidées. Par ailleurs, étant donné que les réseaux sociaux numériques constituent une source pour les professionnels de l'information, la cryptographie servira à baliser les données accessibles par la presse. De ce fait, les données personnelles et confidentielles pourront être inaccessibles. Cette technique replonge le journaliste au cœur des codes d'éthiques et de déontologie. Ne pas avoir systématiquement accès aux données confidentielles et personnelles aidera le journaliste au respect de sa charte de travail. Car, les règles qui balisent l'exercice du métier l'obligent à ne pas publier des informations issues de la vie privée des personnes et de

celles non encore évoquées en audience publique. « Respecter la vie privée des personnes. Le droit de la personne à protéger sa réputation et son intégrité doit être respectée. Eviter de publier des informations qui violent l'intimité de la vie privée » (Article 15, code de déontologie du journaliste en Côte d'Ivoire, 2012) [10].

Certes, de nombreux médias se nourrissent et se développent dans des buzz à partir de la diffusion de données confidentielles piratées sur des sites de plusieurs institutions. WikiLeaks a été l'exemple le plus patent. Son porte-parole et rédacteur en chef Julian Assange, de son vrai nom, Julian Paul Hawkins, journaliste-informaticien, a diffusé de nombreuses informations confidentiels de diplomates qu'il a réussi à pirater. La cryptographie vient donc aider à assainir le monde des médias surtout que le respect de bonnes pratiques est une exigence consacrée dans le code de déontologie du journaliste. Les médias doivent alors, à ce niveau également, intervenir dans l'éducation des populations et des institutions sur le bien-fondé de la cryptographie. Cela est d'autant plus important car le nombre d'utilisateurs d'Internet en Côte d'Ivoire ne cesse de croître. La majeure partie des Internautes ne sont pas des journalistes professionnels instruits à observer le code de bonnes conduites dans la pratique du métier de collecte, de traitement et de diffusion de l'information. Le paradigme proposé avec la cryptographie vient rendre efficace la loi sur la cybercriminalité en réduisant le champ de nuire des citoyens mal intentionnés.

Cependant, cette approche ne limite-t-elle pas la liberté d'expression des populations ? Pour certains chercheurs en communication et pour certains juristes, cette approche réduirait la liberté de recevoir et de communiquer des

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

informations sans ingérence des pouvoirs publics. Ces chercheurs se posent comme les défenseurs de la Déclaration universelle des Droits de l'Homme et du Citoyen de 1789. Cette disposition constitue d'ailleurs le fondement de la pratique du journalisme. Vu sous cet angle ; la cryptographie représente une entrave à la liberté d'expression et de la presse [11]. En effet, « l'analyse de la législation sur la cryptographie met en exergue un conflit de libertés qui s'arbitre autour d'un conflit de sécurité (…) les législations sur la cryptographie se situent à la limite des impératifs commerciaux et des libertés individuelles ? » [12].

En revanche, d'autres opinions appellent à une restriction de plus en plus importante en raison de la forte utilisation d'Internet. Ils sont des milliers pour qui Internet est devenu une arme de destruction. De nombreuses images et informations sont souvent publiées pour ternir la réputation et déshonorer la vie de certaines personnes. D'où l'importance de rendre inaccessibles les informations à caractère privé et confidentiel

## 2. Algorithmes candidats sélectionnés par le NIST

Face à l'avancer des technologies informatiques classiques et à l'arrivée des ordinateurs quantiques, les chercheurs en cryptographies ont travaillé à la mise en œuvre d'algorithmes de cryptographie post-quantique. Un système de cryptographie post-quantique est un algorithme qui fonctionne sur des ordinateurs classiques mais capables de résister à la puissance des ordinateurs quantiques et donc par conséquent de résister aussi aux ordinateurs classiques les plus puissants. Autrement dit, l'utilisation d'ordinateur quantique pour casser un crypto-système post-quantique ne

sera pas aisé comme c'est le cas actuellement pour la cryptographie classique. En effet, Peter Shor a démontré qu'un algorithme classique, déterministe ou probabiliste peut être résolue en $O(N)$ étapes par un système informatique classique. Cependant, les ordinateurs quantiques quant à eux peuvent résoudre ce même algorithme $O(\sqrt{N})$ étapes grâce à leurs propriétés ondulatoires [6].

Pour combler les limites actuelles de la cryptographie classique face aux ordinateurs quantique la NIST (*National Institute of Standards and Technology*) des Etats-Unis a entrepris de sélectionner un ou plusieurs algorithmes cryptographiques post-quantiques dans le cadre d'un concours public international débuté en 2017. Le NIST a émis les principaux critères que devaient respecter ces nouveaux algorithmes. Ces algorithmes devraient tout d'abord permettre de faire une transition des crypto-systèmes classiques vers des algorithmes de cryptographie post-quantique. Ces nouveaux algorithmes post-quantiques devront être des algorithmes à clés publiques, intégrer une ou plusieurs signatures numériques et avoir des schémas d'établissement de clés basés sur le problème du logarithme discret sur des champs finis et des courbes elliptiques, y compris plusieurs variantes des schémas d'établissement de clés Diffie-Hellman et Menezes-Qu-Vanstone (MQV) [13]. De plus, ces nouveaux algorithmes devront avoir des schémas d'établissement de clés utilisant la factorisation des nombres entiers. Avoir des schémas de validations et de transport de clé pour garantir que deux entités partagent le même matériel de chiffrement et fournir des propriétés de sécurités associées à chaque schéma [14]. Enfin, ces nouveaux algorithmes cryptographiques post-quantiques

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

devront spécifier des algorithmes qui pourront être utilisés pour générer des signatures numériques. Les signatures numériques sont utilisées pour détecter des modifications non autorisées de données et authentifier l'identité d'un signataire. En outre, le destinataire des données signées peut utiliser une signature numérique comme preuve pour démontrer à un tiers que la signature a bien été générée par le signataire revendiqué. C'est ce qu'on appelle la non-répudiation, car le signataire ne peut pas facilement répudier la signature ultérieurement [15].

L'appel à propositions du NIST a identifié trois grands aspects des critères d'évaluation qui seraient utilisés pour comparer les algorithmes candidats tout au long du processus de normalisation NIST : 1) la sécurité, 2) le coût et les performances, et 3) les caractéristiques de l'algorithme et de sa mise en œuvre. La sécurité est le critère le plus important utilisé par le NIST lors de l'évaluation des algorithmes post-quantiques candidats. Les normes de clé publique du NIST sont actuellement utilisées dans une grande variété d'applications, notamment les protocoles Internet tels que TLS, SSH, IKE, IPsec et DNSSEC, ainsi que pour les certificats, la signature de code logiciel et les chargeurs de démarrage sécurisés. Les nouvelles normes de clé publique du NIST assureront une sécurité post-quantique pour chacune de ces applications. Dans le but de quantifier la sécurité des algorithmes candidats, le NIST a donné trois définitions de sécurité possibles : deux pour le chiffrement et une pour les signatures. Le NIST a également désigné cinq catégories de sécurité pour classer la complexité informatique des attaques qui violent les définitions de sécurité [16].

L'appel à propositions initial [16] identifiait le coût comme le deuxième critère le plus important lors de l'évaluation des algorithmes candidats. Le coût comprend l'efficacité informatique de la génération des clés et des opérations avec les clés publiques et privées, les coûts de transmission des clés publiques et des signatures ou des textes chiffrés, ainsi que les coûts de mise en œuvre en termes de RAM (mémoire vive).

Au cours du troisième cycle du processus de normalisation NIST PQC (*Post-Quantum Cryptography*), davantage d'informations sur l'efficacité informatique des finalistes sont devenues disponibles. Des implémentations plus rapides et en temps constant ont été fournies pour de nombreux algorithmes, tout comme des implémentations axées sur la limitation de l'utilisation de la mémoire [16]. De plus amples informations sur de nombreux candidats suppléants sont également devenues disponibles. Cette section se concentre sur les considérations de coût et de performances qui ont été prises en compte dans les sélections du NIST. Lors de la comparaison des performances globales des algorithmes, le coût de calcul et le coût de transfert de données ont été pris en compte. Pour une utilisation générale, l'évaluation des performances globales a pris en compte le coût de transfert de la clé publique en plus de la signature ou du texte chiffré lors de chaque transaction. Pour les KEM (*Key Encapsulation Mechanisms*), le coût de génération des clés a également été pris en compte, car de nombreuses applications utilisent une nouvelle paire de clés KEM pour chaque transaction afin d'assurer la confidentialité des informations transmises. Pour les algorithmes de signature, le coût de génération des clés a été considéré comme moins important.

**Soumission** : **03/06/2025** **Acceptation : 01/07/2025** **Publication** : **25/08/2025**

En considérant d'autres critères d'évaluation au-delà de la sécurité, du coût et des performances, l'appel à propositions original [16] énumérait également diverses caractéristiques souhaitables d'algorithme et de mise en œuvre. Les caractéristiques spécifiques mentionnées étaient la flexibilité, la simplicité et l'adoption (l'absence de facteurs pouvant entraver l'adoption). Notez que cette liste n'est pas censée être exhaustive. Le NIST espérait qu'une attention particulière serait accordée aux finalistes, car il s'agissait des algorithmes les plus susceptibles d'être prêts à être standardisés à l'issue du troisième tour.

Répondant au concours du NIST, des chercheurs en cryptographie post-quantique de plus de 25 pays ont proposé des algorithmes. Le NIST en a retenu 69 algorithmes candidats. Ces dernières faisaient appel à des techniques tirées de plusieurs familles mathématiques différentes, dont les réseaux euclidiens, les codes de correction d'erreurs, les systèmes d'équations quadratiques multivariées, les fonctions de hachage et les courbes elliptiques. A la fin du premier tour, en 2020 le NIST a sélectionné 26 algorithmes pour passer au deuxième tour pour une analyse plus approfondie. Parmi les 26 algorithmes candidats retenu pour le deuxième tour on avait 17 algorithmes de chiffrement à clé publique et d'établissement de clé et 9 algorithmes de signature numérique (Tableau 1) [17].

Tableau 1 : Candidats du 2e tour

| **Cryptographie à clé publique / KEM** | | **Signature numérique** |
|---|---|---|
| Classic McEliece | CRYSTALS-KYBER | CRYSTALS-DILITHIUM |
| NTRU | SABER | FALCON |
| BIKE | FrodoKEM | Rainbow |
| HQC | NTRU Prime | GeMSS |
| SIKE | LAC | Picnic |
| LEDAcrypt | NewHope | SPHINCS+ |
| NTS-KEM | ROLLO | LUOV |
| Round5 | RQC | MQDSS |
| Three Bears | | qTESLA |

L'ensemble des finalistes (3e tour) comprenait les algorithmes que le NIST considérait comme les plus prometteurs pour s'adapter à la majorité des cas d'utilisation et les plus susceptibles d'être prêts à être standardisés peu après la fin du troisième tour. La cryptanalyse interne et externe, les critères de performance, les études et les expériences impliquant les candidats du deuxième tour ont conduit le NIST à sélectionner 7 finalistes pour le troisième tour et 8 candidats suppléants en 2022. Le NIST a donc retenu 15 algorithmes au troisième tour qui sont regroupés en deux grands groupes : des algorithmes qui utilisent une cryptographie à clé publique avec un mécanisme d'encapsulation de clé KEM (*Key Encapsulation Mechanisme*) et des algorithmes de signature numériques (tableaux 2 et 3) [18].

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

Tableau 2 : Finaliste du 3e tour

| **Cryptographie à clé publique / KEM** | **Signature numérique** |
|---|---|
| Classic McEliece | CRYSTALS–Dilithium |
| CRYSTALS–KYBER | FALCON |
| NTRU | Rainbow |
| Saber | |

Les candidats suppléants ont été considérés comme des candidats potentiels pour une normalisation future, très probablement après un autre cycle d'évaluation. Certains des candidats alternatifs ont des caractéristiques de performance moins bonnes que les finalistes, mais pourraient néanmoins être sélectionnés pour la normalisation sur la base de la grande confiance du NIST dans leur sécurité (tableau 3).

Tableau 3 : Candidats suppléant du 3e tour

| **Cryptographie à clé publique / KEM** | **Signature numérique** |
|---|---|
| BIKE | GeMSS |
| FrodoKEM | Picnic |
| HQC | SPHINCS+ |
| NTRU Prime | |
| SIKE | |

Début juillet 2022, après un examen attentif au cours du troisième cycle du processus de normalisation, le NIST dévoilait un groupe de quatre algorithmes qui seront normalisés aux futurs standards de cryptographie post-quantique, c'est-à-dire résistant aux ordinateurs

quantiques de demain. Le NIST recommande deux algorithmes principaux à mettre en œuvre pour la plupart des cas d'utilisation : CRYSTALS-KYBER (établissement de clé) et CRYSTALS-Dilithium (signatures numériques). De plus, les schémas de signature FALCON et SPHINCS+ seront également standardisés (Tableau 4) [18].

Tableau 4 : Algorithmes retenus pour la standardisation

| **Cryptographie à clé publique / KEM** | **Signature numérique** |
|---|---|
| CRYSTALS–KYBER | CRYSTALS–Dilithium |
| | FALCON |
| | SPHINCS$^+$ |

CRYSTALS-KYBER (établissement de clés) et CRYSTALS-Dilithium (signatures numériques) ont tous deux été sélectionnés pour leur sécurité renforcée et leurs excellentes performances, et le NIST s'attend à ce qu'ils fonctionnent bien dans la plupart des applications. FALCON sera également standardisé par le NIST car il peut y avoir des cas d'utilisation pour lesquels les signatures CRYSTALS-Dilithium sont trop grandes. SPHINCS+ sera également standardisé pour éviter de compter uniquement sur la sécurité des réseaux euclidiens pour les signatures. Le NIST a demandé des commentaires du public sur une version de SPHINCS+ avec un nombre maximum de signatures inférieur.

Le NIST créera de nouveaux projets de normes pour les algorithmes à normaliser et se coordonnera avec les équipes de soumission pour garantir que les normes sont conformes aux spécifications. Dans le cadre du processus de rédaction, le NIST sollicitera des commentaires sur les ensembles de

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

paramètres spécifiques à inclure, en particulier pour la catégorie de sécurité. Une fois terminées, les normes seront publiées pour commentaires publics. Après la clôture de la période de commentaires, le NIST révisera les projets de normes, le cas échéant, en fonction des commentaires reçus. Un processus final d'examen, d'approbation et de promulgation suivra ensuite.

Les autres algorithmes KEM candidats sélectionnés (BIKE, Classic McEliece, HQC, SIKE) continueront tous à être évalués au quatrième tour (tableau 5) [18]. BIKE et HQC sont tous deux basés sur des codes structurés et conviendraient comme KEM à usage général qui n'est pas basé sur des réseaux euclidiens. Le NIST peut sélectionner au plus un de ces deux candidats pour la normalisation à l'issue du quatrième tour. SIKE reste un candidat attrayant pour la normalisation en raison de la petite taille de sa clé et de son texte chiffré. Le NIST espère que des études plus approfondies se poursuivront sur SIKE au cours du quatrième cycle. Classic McEliece était finaliste, mais n'est pas normalisé par le NIST pour le moment. Bien qu'il soit largement considéré comme sécurisé, le NIST ne prévoit pas encore qu'il soit largement utilisé en raison de la grande taille de sa clé publique. Il n'est donc pas encore urgent de normaliser Classic McEliece.

Tableau 5 : Candidats du 4e tour pour étude et évaluation approfondie

| Cryptographie à clé publique / KEM | Signature numérique |
|---|---|
| BIKE | |
| Classic McEliece | |
| HQC | |
| SIKE | |

En résumé, le NIST a sélectionné quatre des candidats du troisième tour pour la normalisation et quatre pour passer au quatrième tour pour une évaluation et une étude plus approfondies. Les tableaux 4 et 5 montrent une liste de ces algorithmes.

## 3. Méthodologie de mise en œuvre et résultats

### 3.1. Méthodologie de mise en œuvre d'algorithme post-quantique en Côte d'Ivoire

La réalité de la fragilité des algorithmes de cryptographique classique face à l'arrivée des ordinateurs quantiques, impose à la Côte d'Ivoire de prendre des mesures afin de sécuriser l'ensemble de ces données, sensibles ou non. Une étude documentaire a permis de recenser les algorithmes proposés et retenus par la NIST. Ceux-ci feront l'objet d'analyse approfondie. Des entretiens avec une dizaine de chercheurs en informatique, mathématiques et communication ont également été réalisés. L'objectif a été de sélectionner les algorithmes pertinents à implémenter dans le cas ivoirien d'une part, et d'autre part, de comprendre l'implication des médias dans le processus de développement de cryptographies post-quantiques. Nous recommandons donc que la Côte d'Ivoire se saisisse des

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

travaux effectués par le NIST auxquels ont participés des laboratoires spécialisés en cryptographie post-quantique provenant de plus de 25 pays. Cela permettra d'une part à la Côte d'Ivoire de bénéficier des études qui ont été effectuées au NIST. D'autre part, cela permettra à la Côte d'Ivoire de pouvoir mettre en place des algorithmes de cryptographie post-quantique qui lui soit propre afin de sécuriser ces données. En effet, un algorithme connu peut être étudié afin d'identifier ces failles éventuelles. La personnalisation des algorithmes de cryptographie post-cryptographie connu est un critère qui permet d'accroître leurs fiabilités et leurs sécurités. Les implémentations des algorithmes post-quantiques devront aussi tenir compte des spécificités des connections Internet en Côte d'Ivoire. On devra tenir compte par exemple du débit et de la latence des connections Internet aussi bien pour les particuliers, les administrations publiques que les entreprises privées.

Afin de permettre une appropriation aisée par la population ivoirienne de la mise en œuvre des algorithmes de cryptographie post-quantique, il serait indispensable que les médias puissent participer à l'ensemble du processus. En effet, la culture peut être un facteur empêchant l'acceptation d'une technologie par une population. Cela a été démontré par Horkheimer et Adorno [19]. Max Horkheimer et Theodor Adorno créent l'Ecole de Francfort (1923-1950). Cette école fonde ses études sur la critique de l'industrie culturelle qu'ils considèrent comme le stade ultime de la domination. Pour eux, les médias sont le vecteur de la culture (de masse).

La notion de « culture populaire », disaient-ils, est idéologique. L'industrie culturelle nous approvisionne en

une culture « en toc », réifiée, sans spontanéité. Ici, le récepteur des médias est comparé à un « jouet passif ». En effet, les médias se posent ainsi comme un vecteur de transmission d'information et de savoir. Dans cette posture, les médias qui contribuent à la vulgarisation des données confidentielles des institutions nationales et internationales peuvent ainsi aider à la vulgarisation de bonnes pratiques. Par médias, il faut comprendre médias de masse, qui se définit dans le contexte actuel comme un moyen technique de diffusion massive de l'information. Ainsi, la presse imprimée, l'affichage, la télévision, la radio, le cinéma et de plus en plus Internet, sont des médias de masse.

Afin d'arriver à la mise en œuvre des algorithmes de cryptographie post-quantique en Côte d'Ivoire, nous proposons les principales étapes suivantes :

- Etape 1 : analyse des algorithmes
- Etape 2 : personnalisation des algorithmes
- Etape 3 : implémentation et évaluation

Pour la réalisation de toutes ces étapes, nous proposons la mise en place d'une équipe comprenant deux principaux groupes. D'une part, un groupe sera constitué des spécialistes en cryptographie post-quantique, en informatique, en mathématique et en communication. D'autre part, le second groupe sera constitué des représentants patronat ivoirien (CGECI : Confédération Générale des Entreprises de Côte d'Ivoire) et des administrations publiques. On peut citer par exemple l'organisme de normalisation en Côte d'Ivoire (CODINORM) et l'organisme chargé de la cyber-sécurité en Côte d'Ivoire le CI-CERT (CÔTE D'IVOIRE – COMPUTER EMERGENCY RESPONSE TEAM). Ces deux groupes devront travailler ensemble de façon harmonieuse afin

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

d'arriver à mettre à la disposition de la Côte d'ivoire des systèmes cryptographiques post-quantiques fiables pour la protection des données.

**Etape 1 : analyse des Algorithmes**

Cette étape va consister à analyser les algorithmes retenus par la NIST comme pouvant passer à l'étape de la normalisation. L'objectif de cette étape est de s'approprier les algorithmes retenus par le NIST.

Le NIST a proposé un seul algorithme à clé publique et trois algorithmes de signature numériques pour la cryptographie post-quantique. Nous trouvons le nombre d'algorithme proposé pour servir de base à la signature numérique suffisant. Cependant, nous trouvons insuffisant qu'un seul algorithme soit proposé pour servir de base pour la cryptographie à clé publique post-quantique. En effet, nous pensons qu'un choix doit être possible pour la mise en place d'un algorithme à clé publique post-quantique. Nous recommandons à cette étape que les spécialistes ivoiriens ayant étudié des algorithmes post-quantiques non retenu par la NIST ou tout autre algorithme post-quantique prometteur fasse des propositions afin de pouvoir proposer au moins un second algorithme post-quantique à clé publique.

**Etape 2 : personnalisation des algorithmes**

L'étape de la personnalisation des algorithmes retenus consiste à singulariser les algorithmes retenus en les rendant plus fiables. Cette personnalisation devra consister en une modification mathématique des algorithmes de cryptographie post-quantique retenus. Cette étape est très

importante. En effet, les algorithmes de cryptographie post-quantique sont disponibles et peuvent être connus par tous ceux qui le désirent. La personnalisation va donc permettre de rendre nos algorithmes différents des autres en les rendant plus efficaces et plus sécurisés. Ce qui rendra plus difficile une étude de cryptanalyse de nos algorithmes de cryptographie post-quantique. La cryptanalyse est la science qui permet d'étudier les failles des systèmes de cryptographie (classique ou non) afin de pouvoir accéder à une information cryptée sans avoir la clé. On veillera cependant, à cette étape, à éviter de dénaturer nos algorithmes de cryptographie post-quantique.

**Etape 3 : implémentation et évaluation**

Cette étape devra comprendre deux sous étapes. La première est l'implémentation et la seconde est l'évaluation.

L'implémentation va consister à traduire nos algorithmes post-quantiques en applications logicielles qui puissent être utilisées aussi bien par les entreprises privées, les administrations publiques que les particuliers. Nous recommandons que cette sous étape soit divisée en deux phases. La première phase va consister à rendre publique les algorithmes post-quantique issus de l'étape 2. Pour ce faire, il devra être demandé aux spécialistes en communication participants au projet de proposer un plan de communication afin de faire connaître nos algorithmes post-quantiques. La deuxième phase devra consister à organiser un concours ouvert à tous permettant aux participants de proposer des mises en œuvre logiciels des algorithmes post-quantiques. Un cahier des charges devra être défini et mise à disposition des participants au concours. Par exemple, il faudra tenir compte du fait que les implémentations

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

logicielles devront pouvoir correctement fonctionner aussi bien sur un smartphone que sur un ordinateur. De plus, les implémentations devront être transparentes pour l'utilisateur lors de la protection des données sensibles.

L'évaluation des applications va consister à choisir deux ou trois logiciels qui seront recommandés pour la mise en œuvre de la cryptographie post-quantique afin d'assurer la protection des données. Des critères d'évaluation devront être définis et contenu dans un référentiel.

Après cette étape, nous recommandons que l'opportunité soit donnée aux entreprises ou aux particuliers qui le souhaitent de proposer ultérieurement de nouvelles implémentations des algorithmes de cryptographie post-quantique. Nous pensons que cela permettra d'améliorer de façon continuelle les logiciels proposés.

### 3.2. Résultats attendus

Le principal résultat attendu est l'obtention des applications logicielles de cryptographie post-quantique. A la fin du processus, le comité en charge de la sélection devra fournir les résultats concernant les applications logicielles de cryptographie post-quantique retenues. Les meilleures applications retenues à l'étape 3 devront être présentées au publique. Un plan de communication devra être proposé afin d'une part de faire connaître les logiciels retenus. D'autre part, le plan de communication devra avoir aussi pour objectif de permettre une appropriation des applications logicielles présentées par les entreprises privées, les administrations publiques et les particuliers. Nous pensons que l'utilisation régulière des applications cryptographiques post-quantiques proposées va accroître le

niveau de sécurité des données sensibles ou non en Côte d'Ivoire. De plus, l'utilisation de ces logicielles de cryptographie post-quantique permettra de minimiser le risque qu'une organisation publique ou privée en Côte d'Ivoire soit victime d'un *ransomware*.

## Conclusion

Dans cet article, nous avons montré que les organisations publiques ou privées utilisent en générale des systèmes de cryptographie classique afin d'assurer la protection de leurs données. Nous avons aussi présenté les risques que cours ces organisations et même les particuliers fasse à l'évolution des ordinateurs quantiques. En effet, la protection des données qui déjà connaissait une faiblesse devant l'évolution des ordinateurs classique sera encore plus fragilisée grâce à la puissance des ordinateurs quantiques qui ont déjà commencé à être déployés dans le monde. Afin d'accroître de façon significative la protection des données en Côte d'Ivoire nous avons proposé une méthodologie qui permettra à la Côte d'ivoire de disposer d'applications logicielles de cryptographie post-quantique. La cryptographie post-quantique est à l'heure actuelle le seul système qui assure le plus haut niveau de protection des données. Il sera aussi très opportun, pour de future travaux, d'étudier la manière dont doit se faire la transition permettant le passage à la cryptographie post-quantique en Côte d'Ivoire.

**Soumission** : **03/06/2025** **Acceptation : 01/07/2025** **Publication** : **25/08/2025**

Références bibliographiques

[1] Banque Mondiale ; Individus utilisant Internet (% de la population) - Afrique subsaharienne, Côte d'Ivoire ; Union Internationale des Télécommunication (UIT) ; 2022. https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&locations=ZG-CI&start=1990&view=chart 15/08/2023 : 09h04.

[2] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel and Atul, "Post quantum cryptography: Techniques challenges standardization and directions for future research", *arXiv:2202.02826*, 2022.

[3] CI-CERT Newsletter N°5

[4] Rivest R.L., A. Shamir et L. Adleman, « A method for obtaining digital signatures and public key cryptosystems », Communications of the ACM, vol. 21, n°2, 1978, p. 120–126.

[5] Jean-Christophe Deneuville, Contributions à la cryptographie post-quantique. Cryptographie et sécurité, Thèse, Université de Limoges, 2016.

[6] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5):1484–1509, 1997.

[7] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996, pages 212–219, 1996.

[8] Daniel J. Bernstein, Nadia Heninger, Paul Lou et Luke Valenta, Post Quantum RSA," in Post-Quantum Cryptography, Springer International Publishing AG 2017
[9] René Trégouët ; L'ordinateur quantique va révolutionner l'informatique ; Dans HegelHegel 2012/4 (N° 4)2012/4 (N° 4), pages 1 à 3 Éditions ALN éditionsALN éditions ; ISSN 2269-0530 ; DOI 10.4267/2042/48705
[10] OLPED, 2012, Le Code de déontologie du journaliste en Côte d'Ivoire
[11] MALLET-POUJOL Nathalie, 2009, Les traitements de données personnelles aux fins de journalisme in Legion, vol.2, n°43, pp. 69-81
[12] BENE Jean-Baptiste, 2004, Régulation des réseaux internationaux de transmission de donnnées et de cryptologie [thèse de doctorat soutenue à Montpellier 1, sous la direction de Mallet-Poujol]
[13] E. BARKER et *al*. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. National Institute of Standards and Technology, 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3
[14] E. BARKER et *al*. Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography. National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.SP.800-56Br2
[15] Federal Information Processing Standards Publication 186-5, DIGITAL SIGNATURE STANDARD (DSS), 2023, https://doi.org/10.6028/NIST.FIPS.186-5
[16] National Institute of Standards and Technology (2016) Submission requirements and evaluation criteria for

**Soumission** : **03/06/2025** **Acceptation** : **01/07/2025** **Publication** : **25/08/2025**

the post-quantum cryptography standardization process. Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[17] G. ALAGIC et *al*. Status report on the second round of the NIST post-quantum cryptography standardization process. US Department of Commerce, NIST, 2020, vol. 2. https://doi.org/10.6028/NIST.IR.8309

[18] D. Apon et *al*., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, US Department of Commerce, NIST, 2022, https://doi.org/10.6028/NIST.IR.8413-upd1

[19] M. HORKHEIMER, T. ADORNO, La Dialectique de la raison, Paris, Gallimard