MULTISS : un protocole de stockage confidentiel à long terme sur plusieurs réseaux QKD

Thomas Prévost
Université Côte d'Azur
I3S - CNRS
Sophia-Antipolis, France
thomas.prevost@univ-cotedazur.fr

Olivier Alibart
Université Côte d'Azur
InPhyNi - CNRS
Nice, France
olivier.alibart@univ-cotedazur.fr

Anne Marin
VeriQloud
marin@veriqloud.fr

Marc Kaplan
VeriQloud
kaplan@veriqloud.fr

***Résumé*—Cet article présente MULTISS, un nouveau protocole pour le stockage à long terme, distribué sur plusieurs réseaux de distribution quantique de clé (Quantum Key Distribution, QKD). Ce protocole est une extension de LINCOS, un protocole de stockage sécurisé qui utilise le partage de secret de Shamir pour le stockage de secret sur un seul réseau QKD. Notre protocole utilise le partage de secret hiérarchique pour distribuer un secret entre plusieurs réseaux QKD tout en garantissant la sécurité parfaite. Notre protocole permet en outre de mettre à jour les partages sans avoir à reconstruire tout le secret. Nous prouvons également que MULTISS est strictement plus sécurisé que LINCOS, qui demeure vulnérable lorsque son réseau QKD est compromis.**

***Index Terms*—stockage sécurisé, sécurité parfaite, long terme, distribution quantique de clé, interpolation de Birkhoff.**

I. Introduction

Certaines informations sont classées confidentielles sur le long terme, au moins plusieurs décennies. C'est le cas par exemple de certains secrets industriels, de secrets d'État ou de données médicales. Ces secrets ont donc besoin d'une garantie de confidentialité et de disponibilité à long terme. Les primitives cryptographiques actuelles sont cependant inadaptées pour de tels usages. En effet, la technologie et la cryptanalyse évoluent rapidement. On sait par exemple que les primitives de chiffrement à clé publique utilisées majoritairement aujourd'hui, c'est-à-dire RSA ou ECC, seront vulnérables aux attaques par ordinateur quantique [1], [2]. De même, la cryptographie « post-quantique » sera susceptible d'être vulnérable à la cryptanalyse dans un futur plus ou moins éloigné [3]. On peut donc légitimement craindre qu'un acteur malveillant écoute les communications chiffrées, dans le but de les déchiffrer lorsque la cryptanalyse dont il disposera le permettra. Ce type d'attaque est appelé « Harvest now, decrypt later » [4].

Claude Shannon a proposé en 1949 le principe de « sécurité parfaite » (ou inconditionnelle) [5] (Information Theoretic Secrecy, *ITS*). Cela signifie que la confidentialité est assurée peu importe la puissance de calcul de l'attaquant. En d'autres termes, « il est aussi difficile pour un attaquant de trouver la clé que de découvrir le message par hasard ». La confidentialité à long terme ne saurait être garantie que par un protocole qui garantit la sécurité parfaite tout au long de son exécution.

Si la sécurité parfaite est généralement proposée par un « masque jetable » (One Time Pad), c'est à dire une clé parfaitement aléatoire non réutilisée de la même taille que le message, la distribution quantique de clé [6] est une méthode originale de transmission garantissant ce même niveau de sécurité. Ce mécanisme ne repose plus sur la limite de puissance de calcul de l'attaquant, mais sur la possibilité de détecter celui-ci à la volée lorsqu'il écoute le message. Puisque l'attaquant n'est même pas en mesure d'écouter les communications, une attaque de type « Harvest now, decrypt later » n'est pas envisageable.

Le protocole LINCOS [7] permet de conserver un secret sur un réseau de distribution quantique de clé. Il utilise pour cela le partage de secret de Shamir [8], afin de répartir le secret sur les différents nœuds du réseau QKD. Le partage de secret de Shamir garantissant lui-même la sécurité parfaite [9], le protocole LINCOS offre le même niveau de confidentialité tant que l'attaquant n'a pas compromis un nombre de nœuds équivalent au seuil de déchiffrement.

Cependant, la transmission quantique de clé sur laquelle repose le protocole LINCOS est limitée par une distance géographique maximale, de l'ordre de quelques centaines de kilomètres. Les implémentations de LINCOS, en Europe [10] comme en Asie [11], limitent la portée du réseau à une surface métropolitaine. De plus, les différents nœuds d'un réseau QKD partagent généralement le même sous-réseau informatique. Ainsi, des pirates informatiques qui prendraient le contrôle du réseau, ou bien une entité étatique qui pourrait saisir légalement le matériel, serait en mesure de reconstruire le secret.

Nous proposons donc une extension de LINCOS, nommée MULTISS [12], permettant d'étendre le stockage de secret sur plusieurs réseaux de distribution quantique distants. Notre protocole conserve les propriétés de sécurité parfaite de LINCOS, tout en garantissant la confidentialité du secret contre un attaquant en mesure de prendre le contrôle de l'ensemble d'un des réseaux de QKD.

This work has been conducted within the framework of the French government financial support managed by the Agence Nationale de la Recherche (ANR), within its Investments for the Future programme, under the Stratégie Nationale Quantique through the project of the PEPR-quantum QComtestbeds (ANR 22-PETQ-0011) and with fundings from the EUROPE HORIZON-FPA project QSNP and the EUROPE DIGITAL project FranceQCI.

II. La distribution quantique de clé

En cryptographie classique, la transmission de secrets entre deux entités distantes repose généralement sur la combinaison du chiffrement à clé publique et du chiffrement à clé secrète, le chiffrement à clé publique permettant d'échanger la clé de chiffrement symétrique qui sera utilisée pour chiffrer effectivement le secret. La sécurité de ce type de protocoles est dite « calculatoire et sémantique », c'est à dire qu'elle repose sur la difficulté, pour un attaquant aux ressources de calcul bornées, de retrouver la clé privée à partir de la clé publique ou bien de retrouver le secret à partir du chiffré, dans un délai raisonnable. Les participants sont contraints de faire une hypothèse sur la puissance de calcul de l'attaquant qui, nécessairement, augmente avec le temps.

La distribution quantique de clé fonctionne tout à fait différemment. La sécurité est assurée par un principe fondamental de la physique quantique, le *théorème de non-clonage* [13]. Le théorème stipule qu'il est impossible de cloner parfaitement un qubit arbitraire (la représentation de base de l'information quantique) sans modifier son état.

Les protocoles de QKD fonctionnent ainsi soit par la transmission directe de qubits entre les participants, comme c'est le cas pour le protocole BB84 [14], soit avec une source intermédiaire qui envoie deux qubits intriqués vers les deux participants, comme pour le protocole E91 [15]. Lorsqu'un adversaire intercepte un qubit pour lire son état, alors il modifie nécessairement ledit état (comme stipulé par le théorème de non-clonage). Les participants sont alors en mesure de détecter cette modification et peuvent interrompre l'échange. En général, les bits échangés par la QKD vont servir de masque jetable pour chiffrer les données : $C = S \oplus K$, avec S le message secret, K les bits de clé échangés par la QKD, et C le chiffré.

Demeure néanmoins la problématique d'authentifier les participants honnêtes, afin d'empêcher un attaquant de réaliser une attaque dite de « l'Homme du milieu » (Man-in-the-Middle, MitM). Cette authentification est généralement réalisée grâce à la cryptographie classique. On utilise soit un échantillon d'une clé échangée antérieurement, soit un mécanisme d'authentification à clé publique. Ces mécanismes d'authentification seraient bien entendu vulnérables contre un attaquant qui disposerait d'une puissance de calcul illimitée *au moment de l'échange*. En fait, nous définissons notre modèle d'attaquant avec une puissance de calcul limitée et connue, mais qui pourrait évoluer indéfiniment par la suite. On parle alors de « sécurité éternelle » (everlasting security). Pour simplifier, dans la suite de cet article, nous qualifierons de « liens à sécurité parfaite », ou « liens ITS », les liaisons QKD entre deux nœuds.

En général, la représentation du qubit utilisée pour la distribution quantique de clé est l'état quantique d'un photon (par exemple sa polarisation). Le photon est transporté au sein d'une « fibre noire », protégée contre les interférences extérieures. Cependant, les pertes de la fibre optique limitent la portée maximale de la QKD à quelques centaines de kilomètres au maximum [16], puisque le théorème de non-clonage interdit l'usage d'un répéteur.

III. Le partage de secret

A. Partage de secret direct

Le partage de secret est une primitive découverte simultanément par Adi Shamir [8] et George Blakley [17] en 1979. Nous utilisons ici la primitive proposée par Shamir. Elle permet à une personne, le *dealer*, de distribuer un secret entre n participants, chaque fraction du secret s'appelant un « partage ». Le dealer définit un seuil k de participants qui devraient mettre leurs partages en commun afin de reconstruire le secret initial.

Dans le partage de secret de Shamir, on définit $S \in \mathbb{N}$ le secret initial, $n \in \mathbb{N}^*$ le nombre de participants et $k \in \mathbb{N}^*$ le seuil minimal de déchiffrement, défini par le dealer. N'importe quel sous ensemble de k participants doit être en mesure de retrouver le secret en mettant leurs partages en commun, tandis que s'il n'y a que $k-1$ participants, ces derniers ne disposent d'aucune information sur le secret.

Le dealer commence par choisir un grand nombre premier q, tel que $q > S$. Par la suite, toutes les opérations sont effectuées dans le corps fini $\mathbb{F}_q$. Le dealer génère un polynôme aléatoire $P \in \mathbb{F}_q[X]$ de degré $deg(P) = k-1$, tel que $P(0) = S$, le secret initial. Il distribue ensuite les évaluations du polynôme $P(1), P(2), \ldots, P(n)$ aux n participants, qui ont chacun connaissance du degré du polynôme. Si k participants parmi n mettent leurs partages en commun, ils sont en mesure de reconstruire le polynôme P par interpolation lagrangienne [18], et donc de retrouver le secret $S = P(0)$.

B. Partage de secret hiérarchique

On peut étendre le concept de partage de secret pour y ajouter une notion de hiérarchisation des participants [19]. Imaginons par exemple un directeur de banque qui souhaiterait un minimum de 3 employés pour ouvrir le coffre. Le partage de secret hiérarchique lui permettrait d'exiger au minimum 3 employés, **dont** au moins un responsable d'agence parmi eux.

De même que pour le partage de secret de Shamir, le dealer génère un polynôme aléatoire $P \in \mathbb{F}_q[X]$ de degré $deg(P) = k-1$, tel que $P(0) = S$. Il calcule ensuite le polynôme dérivé de P par rapport à X, P'. Il distribue alors à chacun des managers les évaluations du polynôme primitif $P(1), P(2), \ldots, P(m)$, puis aux employés les évaluations du polynôme dérivé $P'(1), P'(2), \ldots, P'(n)$, avec m le nombre de managers et n le nombre d'employés.

Ainsi, k employés **dont** 1 manager sont en mesure de reconstruire le polynôme P par interpolation de Birkhoff [20], et donc de retrouver le secret $S = P(0)$.

IV. Le protocole LINCOS

Le protocole LINCOS [7], sur lequel est basé MULTISS, est composé de deux procédures distinctes, comme décrit Fig. 1 :

— COPRIS, le protocole d'intégrité et d'authenticité ;

— le protocole de confidentialité à long terme.

C'est ce dernier protocole que nous entendons étendre avec MULTISS, le protocole COPRIS restant inchangé.

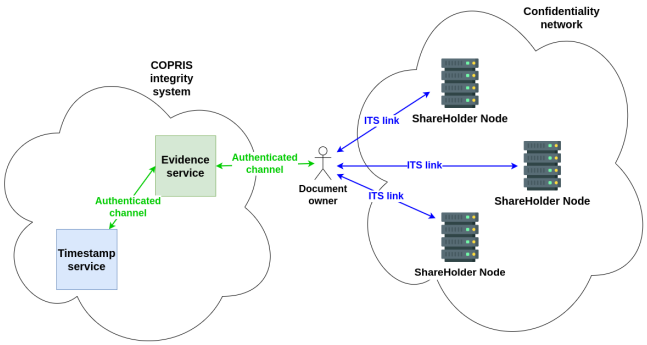

FIGURE 1. Le protocole LINCOS, avec à gauche COPRIS, en charge de l'intégrité et de l'authentification, et à droite le stockage du document par partage de Shamir entre les différents nœuds du réseau QKD.

A. COPRIS, pour l'intégrité et l'authenticité

Afin de garantir l'intégrité et l'authenticité d'un document, son propriétaire peut utiliser COPRIS, afin de prouver que le document a existé à un instant t, tout en gardant ce document secret. Pour cela, le propriétaire envoie un *engagement* à l'« Evidence service ». Ce dernier fait une requête d'horodatage courant au « Timestamp service ». A partir de l'horodatage reçu, l'evidence service créé un enregistrement.

Puisque le propriétaire refait régulièrement des requêtes d'engagement, il est en mesure de prouver qu'un document S existait bien à un instant t.

B. Le protocole de confidentialité à long terme

Dans le protocole LINCOS, le propriétaire du document dispose d'un lien ITS avec chacun des nœuds du réseau QKD. En pratique, il existe un lien quantique (une fibre noire en général) entre le propriétaire du document et les nœuds. Le propriétaire et le nœud échangent une clé aléatoire grâce à la distribution quantique de clé, puis utilisent cette même clé comme un masque jetable pour chiffrer leurs communications. C'est donc un lien de confidentialité parfaite, compatible avec la confidentialité à long terme.

Afin de stocker son document S au sein du réseau de QKD, le propriétaire choisit un seuil de déchiffrement k, en fonction de ses besoins de disponibilité et de la confiance qu'il accorde au réseau. Il génère alors des partages du document S à partir de la primitive de Shamir, avec un seuil de déchiffrement de k, tel qu'expliqué en section III. Il envoie alors les partages $P(1), P(2), \ldots, P(n)$ aux différents nœuds du réseau. Il faudra alors mettre en commun au moins k partages pour retrouver le document S.

Le propriétaire du document doit en outre régulièrement mettre à jour les partages sur les différents nœuds, afin de rendre improbable l'exploitation de potentielles fuites de données successives, c'est à dire si un attaquant était en mesure de prendre le contrôle de plusieurs nœuds à des moments distincts. Afin de ne pas reconstruire le document secret à chaque mise à jour des partages, le propriétaire génère un nouveau polynôme aléatoire $Q \in \mathbb{F}_q[X]$ de degré $k-1$, tel que $Q(0) = 0$. Il envoie alors les évaluations $Q(1), Q(2), \ldots$ aux différents nœuds, qui vont additionner les valeurs reçues à leurs anciennes valeurs (toujours dans le corps fini $\mathbb{F}_q$). Ainsi, il sera toujours possible de reconstruire un polynôme $R = P + Q$, avec $R(0) = P(0) + Q(0) = S + 0 = S$, à partir d'au moins k partages.

V. HYPOTHÈSES ET MODÈLE D'ADVERSAIRE

A. Hypothèses de sécurité

Le protocole MULTISS permet d'étendre le protocole LINCOS sur plusieurs réseaux de QKD, de sorte que la compromission d'un réseau entier n'affecte pas la confidentialité du secret. Dans le protocole LINCOS, le propriétaire du fichier est relié par un « lien ITS » avec le réseau de QKD. Ce lien ITS consiste en une liaison de distribution quantique de clé vers les nœuds du réseau, bien que nous pourrions par exemple imaginer un PDG d'entreprise qui amènerait en personne son document secret dans un mallette sécurisée. Puisque les différents sous-réseaux du protocole MULTISS sont censés se trouver très éloignés géographiquement, alors nous faisons l'hypothèse que le propriétaire du document est relié par un lien ITS à un seul de ces sous-réseaux. Les autres étant hors de portée des liens quantiques, ils sont reliés au propriétaire du document par un lien n'autorisant que la cryptographie classique. On appellera par la suite « réseau mère » le sous-réseau relié au client par un lien ITS, et « réseaux filles » les autres sous-réseaux. À noter cependant que cette dénomination varie en fonction de l'emplacement géographique des propriétaires : le sous-réseau métropolitain parisien sera le réseau mère pour un client français, mais un réseau fille pour un client japonais.

De plus, nous formulons l'hypothèse raisonnable que les mécanismes d'authentification utilisés ne sont pas vulnérables au moment où les messages sont échangés. Ainsi, on suppose que l'authentification est parfaite, et qu'il est donc impossible pour un adversaire de réaliser une attaque de l'Homme du milieu.

B. Compromission d'un réseau entier par un adversaire

De par la limitation géographique de la QKD, les « réseaux ITS » se déploient généralement sur une surface métropolitaine. Ils sont en outre souvent gérés par la même entité administrative, par exemple un laboratoire de recherche ou une entreprise, et donc connectés au même sous-réseau IP. Il est ainsi possible qu'un attaquant qui a réussi à prendre le contrôle d'un des nœuds puisse aisément se déplacer dans le réseau interne. La limitation géographique de l'étendue de ces réseaux de QKD pose aussi un problème juridictionnel. Un état aujourd'hui démocratique pourrait ne pas le rester à l'avenir, et un dictateur pourrait ordonner la saisie « légale » de tous les nœuds du réseau, découvrant ainsi le secret.

MULTISS permet de se protéger contre un adversaire qui pourrait potentiellement prendre le contrôle d'un sous-réseau ITS entier.

C. Harvest now, decrypt later

Puisque le propriétaire du document n'est relié par un lien ITS qu'à un seul des sous-réseaux, le réseau mère, alors la communication avec les autres sous-réseaux filles se fait nécessairement par cryptographie classique. Le protocole MULTISS garantit la confidentialité persistante contre un adversaire « Harvest now, decrypt later », qui serait en mesure d'écouter puis de déchiffrer ultérieurement les communications passées par des liens classiques.

D. Incompatibilité des deux modèles d'adversaires

Les deux modèles d'adversaire décrits ci-avant sont incompatibles entre eux. Un adversaire qui aurait écouté toutes les communications sur les liens classiques qu'il serait ensuite en mesure de déchiffrer (sect. V-C), puis qui prendrait le contrôle du réseau ITS mère (sect. V-B) serait forcément en mesure de retrouver le document secret initial, puisqu'il disposerait de l'ensemble de l'information existante. MULTISS ne permet de se protéger que d'un seul de ces deux adversaires à la fois.

Cela ne devrait cependant pas poser un problème pour la garantie de confidentialité à long terme. En effet, la compromission du sous-réseau ITS mère (par voie « légale » ou piratage informatique) a peu de chances de demeurer discrète sur le long terme pour le propriétaire du document. Celui-ci aura alors le temps de prendre les dispositions nécessaires pour invalider le contenu du document. De même, si le chiffrement utilisé sur les canaux classique venait à devenir vulnérable, le propriétaire finirait aussi par en être informé.

VI. Description du protocole MULTISS

MULTISS utilise deux niveaux de partage de secret. De plus, à la différence de LINCOS, le propriétaire ne doit plus définir un mais trois seuils distincts :

- t_{nodes} le nombre minium de nœuds à contrôler pour retrouver le secret, tous sous-réseaux confondus ;
- $t_{networks}$ le nombre minimum de sous-réseaux à compromettre pour retrouver le secret. Un sous-réseau est considéré comme « compromis » dès lors qu'un seul de ses nœuds a été compromis ;
- t_{fail} le nombre minimum de nœuds à arrêter pour que le secret ne soit plus accessible.

En fonction de ces seuils, le propriétaire définira les degrés des différents polynômes, comme nous le verrons plus tard. À noter qu'il est possible de ne choisir qu'un certain nombre de combinaisons de seuils, en fonction de la topologie du réseau.

Le propriétaire du document commence par générer un polynôme aléatoire $P \in \mathbb{F}_q[X]$, tel que $P(0) = S$, le document secret. Puis le propriétaire génère l polynômes $Q_i \in \mathbb{F}_q[X]$ tels que $Q_0(0) = P(1)$, et $Q_i(0) = P'(i)\ \forall i \in [\![1, l-1]\!]$, avec l nombre de sous-réseaux, et P' dérivé de P. Finalement, le propriétaire répartit les évaluations $Q_0(1), Q_0(2), \dots$ sur les nœuds du réseau mère, et chaque évaluation $Q_i(1), Q_i(2), \dots$ sur les nœuds de chaque sous-réseau fille i.

Pour reconstruire le secret, le propriétaire aura besoin des partages $Q_j(0), j \in [\![0, l-1]\!]$ d'au moins $deg(P) - 1$ sous-réseaux **dont** ceux du sous-réseau mère. Dans chaque sous-réseau N_j, il faut au moins $deg(Q_j)-1$ partages pour retrouver $Q_j(0)$.

Nous pouvons alors déterminer les différents seuils en fonction des degrés de nos polynômes. Tout d'abord, le nombre de réseaux $t_{networks}$ à compromettre dépend entièrement de P :

$$t_{networks} = T(P) \tag{1}$$

Avec T le « seuil de déchiffrement d'un polynôme », c'est à dire son degré moins un. Le nombre de nœuds, tous réseaux confondus, nécessaires pour retrouver le secret est

$$t_{nodes} = T(Q_0) + min\left\{ \sum_{i \in I} T(Q_i) \middle| I \subset \{1, \dots, l-1\}, |I| = T(P) - 1 \right\} \tag{2}$$

Enfin, un attaquant qui voudrait rendre le secret inaccessible devrait soit

- éteindre $t_{f_0} = n_0 - T(Q_0) + 1$ nœuds dans le réseau mère, avec n_0 le nombre de nœuds dans le réseau mère ;
- éteindre $n_i - T(Q_i) + 1$ nœuds dans x réseaux filles, avec $x = l - 1 - T(P) + 1$, et n_i le nombre total de nœuds dans le sous-réseau i.

On a alors

$$t_{f_1} = min\left\{ \sum_{i \in I} n_i - T(Q_i) + 1 \middle| I \subset \{1, \dots, l-1\}, |I| = l - T(P) \right\} \tag{3}$$

et donc

$$t_{fail} = min\{t_{f_0}, t_{f_1}\} \tag{4}$$

Le renouvellement des partages s'effectue comme pour le protocole LINCOS, tel que décrit en section IV-B. Pour chaque sous-réseau, le propriétaire du document génère un nouveau polynôme $R_i \in \mathbb{F}_q[X], i \in [\![0, l-1]\!]$, tel que $R_i(0) = 0$, et distribue les évaluations de chaque polynôme R_i aux différents nœuds du réseau i.

VII. Conclusion

Dans cet article, nous proposons un nouveau protocole de stockage confidentiel à long terme sur plusieurs réseaux de distribution quantique de clé. Notre protocole, MULTISS, est une extension du protocole LINCOS, permettant de garantir la confidentialité à long terme y compris contre un adversaire en mesure de prendre le contrôle de tout un réseau de QKD.

En outre, notre protocole garantit la sécurité parfaite du document secret, c'est à dire que sa confidentialité ne pourra pas être altérée par l'évolution future de la puissance de calcul de l'attaquant.

Remerciements: T. Prevost remercie l'UCA pour son financement de thèse. Les auteurs sont reconnaissants à Bruno Martin (https://webusers.i3s.unice.fr/~bmartin/) pour son support théorique.

RÉFÉRENCES

[1] V. Bhatia and K. Ramkumar, "An efficient quantum computing technique for cracking RSA using Shor's algorithm," in *2020 IEEE 5th international conference on computing communication and automation (ICCCA)*. IEEE, 2020, pp. 89–94.

[2] J. Wohlwend, "Elliptic curve cryptography : Pre and post quantum," *http://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf*, 2016.

[3] N. Kaluderovic, "Attacks on some post-quantum cryptographic protocols : The case of the Legendre PRF and SIKE," EPFL, Tech. Rep., 2022.

[4] S. Paul, "On the transition to post-quantum cryptography in the industrial Internet of things," 2022.

[5] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, 1949.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing," *Theoretical computer science*, 2014.

[7] J. Braun, J. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki, and A. Waseda, "Lincos : A storage system providing long-term integrity, authenticity, and confidentiality," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.

[8] A. Shamir, "How to share a secret," *Communications of the ACM*, 1979.

[9] C. L. Corniaux and H. Ghodosi, "An entropy-based demonstration of the security of Shamir's secret sharing scheme," in *2014 International Conference on Information Science, Electronics and Electrical Engineering*. IEEE, 2014.

[10] (2020, December) Medical data successfully protected by quantum cryptography in Graz. [Online]. Available : https://tinyurl.com/bdzyadu5

[11] M. Fujiwara, H. Hashimoto, K. Doi, M. Kujiraoka, Y. Tanizawa, Y. Ishida, M. Sasaki, and M. Nagasaki, "Secure secondary utilization system of genomic data using quantum secure cloud," *Sci Rep*, vol. 15, no. 18530, 2022.

[12] T. Prévost, O. Alibart, A. Marin, and M. Kaplan, "Mutliss : a protocol for long-term secure distributed storage over multiple remote QKD networks," *Cryptology ePrint Archive*, 2024.

[13] B. Zygelman and B. Zygelman, "No-cloning theorem, quantum teleportation and spooky correlations," *A First Introduction to Quantum Computing and Information*, 2018.

[14] C. Bennett and G. Brassard, "Quantum cryptography : Public-key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. IEEE Computer Society Press, Los Alamitos, 1984.

[15] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, 1991.

[16] Y. Pelet, G. Sauder, M. Cohen, L. Labonté, O. Alibart, A. Martin, and S. Tanzilli, "Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers," *Phys. Rev. Appl.*, vol. 20, p. 044006, Oct 2023. [Online]. Available : https://link.aps.org/doi/10.1103/PhysRevApplied.20.044006

[17] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing requirements knowledge, international workshop on*. IEEE Computer Society, 1979.

[18] E. Waring, "Vii. problems concerning interpolations," *Philosophical transactions of the royal society of London*, 1779.

[19] T. Tassa, "Hierarchical threshold secret sharing," in *Theory of Cryptography Conference*. Springer, 2004.

[20] G. D. Birkhoff, "General mean value and remainder theorems with applications to mechanical differentiation and quadrature," *Transactions of the American Mathematical Society*, 1906.