Performances des protocoles QKD, BB84 et SARG04 pour les communications quantiques sous-marines

Nour RIZK Angélique DREMEAU Arnaud COATANHAY

Lab-STICC, UMR CNRS 6285, ENSTA, Institut Polytechnique de Paris, 2 rue François Verny, 29806 Brest Cedex 9, France

Résumé – Dans le contexte des communications sous-marines sécurisées et plus précisément des transmissions de clés de cryptage par un processus quantique (Underwater Quantum Key Distribution - UQKD), cette étude cherche à mettre en évidence l'influence du canal de propagation sur l'efficacité de la transmission. Nous comparons ainsi deux protocoles de QKD à variables discrètes : BB84 et SARG04, en fonction de la distance de propagation, des caractéristiques d'eau de mer (claire, côtière et trouble) et des conditions atmosphériques. Le critère principal de comparaison consiste en une analyse quantitative du taux d'erreur de bit quantique (Quantum Bit Error Rate - QBER). Nous nous basons pour cela sur une expression analytique déjà établie et connue de la littérature et proposons une simulation numérique en fonction des paramètres du modèle de mer.

Abstract – In the context of secure underwater communications, particularly the transmission of encryption keys via a quantum process (Underwater Quantum Key Distribution - UQKD), this study aims to highlight the influence of the propagation channel on transmission efficiency. We compare two discrete-variable QKD protocols: BB84 and SARG04, as a function of propagation distance, seawater characteristics (clear, coastal and turbid) and atmospheric conditions. The main comparison criterion is a quantitative analysis of the Quantum Bit Error Rate (QBER). To this end, we rely on an existing analytical expression and provide a numerical simulation as a function of the sea model parameters.

1 Introduction

Qu'il s'agisse d'échanges entre des drones, des stations fixes ou des bâtiments de surface, les communications sous-marines peuvent servir à transmettre des données extrêmement sensibles. L'une des voies les plus fiables pour sécuriser ces échanges consiste à chiffrer ces échanges en utilisant des clés de chiffrement privées. La difficulté devient alors de diffuser des clés en garantissant qu'aucune d'entre elles n'a été interceptée par un tiers malveillant. Dans ce contexte, la physique quantique offre une réponse idéale à ce problème. En effet, il est par nature impossible de recopier, en dessous sans un minimum d'erreurs, un bit quantique ou qubit (un photon polarisé par exemple) dès lors que l'on ne connaît pas la base (polarimétrique) dans lequel celui-ci a été préparé, c'est à dire encodé [15]. Ainsi, par la simple estimation d'un taux d'erreur, il est possible de garantir ou pas l'absence de toute interception entre deux agents, appelés Alice et Bob, par un espion, classiquement nommée Ève.

Le protocole BB84, proposé par Bennett et Brassard [2] en 1984, est le premier protocole de QKD capable de démontrer en théorie un parfait niveau de sécurité sous un seuil maximal de taux d'erreur en transmission. Il a par la suite donné lieu à une multitude d'applications [5], sur fibre optique ou en espace libre. Toutefois, en conditions expérimentales, ce protocole présente un certain nombre de vulnérabilités et plusieurs protocoles plus sophistiqués ont depuis vu le jour [7]. Parmi ceux-là, on peut citer le protocole SARG04, beaucoup plus robuste, dans la mesure où il pallie en partie le caractère non-idéal de la source de photons.

Dans tous les cas, la maîtrise du taux d'erreur des bits quantiques (Quantum Bit Error Rate - QBER) joue un rôle fondamental pour la garantie de sécurité des protocoles. Or pour des contextes sous-marins (Underwater QKD - UQKD), la problématique doit prendre en compte la salinité, la turbidité ou autres caractéristiques de l'eau de mer qui provoquent une absorption et une diffusion très significatives des photons. Dans la logique des très récents travaux de Paglierani et al. [10] et de Raouf et al. [6], notre article cherche à quantifier l'influence du milieu sous-marin, pour différents types d'eau de mer (claire, côtière et trouble) et sous différentes conditions d'éclairement, sur le QBER des protocoles BB84 et SARG04.

2 Protocoles de QKD

2.1 Protocole BB84

Le protocole BB84 [2] s'appuie sur l'utilisation de qubits encodés dans deux bases de polarisation orthogonales : la base rectiligne Z (associée aux états orthonormaux $|0\rangle$ et $|1\rangle$) et la base diagonale X (associée aux états orthonormaux $|+\rangle$ et $|-\rangle$). Lors de l'échange, Alice choisit aléatoirement l'une des deux bases, encode son information binaire sur la polarisation d'un photon dans cette base et l'envoie à travers un canal quantique. Bob mesure ensuite le photon reçu selon une base également choisie aléatoirement. A posteriori, ils confrontent leurs différents choix de bases et ne conservent les mesures des photons que lorsque leurs bases correspondent (ce sont les bits "tamisés", "sifted bits" en anglais). En théorie, Bob collecte donc des photons lus sans erreur et utiliser les bits conservés comme clé de chiffrage. Avec un canal parfait, une erreur de transmission s'interprète alors comme un qubit intercepté et mal retransmis par Ève qui se trouve, en raison des principes de la physique quantique, dans l'impossibilité de reproduire un qubit avec taux d'erreur nul. Pour le protocole BB84, le QBER est ainsi défini par [10] :

$$\mathrm{QBER}_{\mathrm{BB84}} = \frac{\text{nombre de bits tamisés erronés}}{\text{nombre total de bits tamisés}} \qquad (1)$$

Par des considérations de théorie de l'information, il peut être montré que le QBER minimal induit par Ève est de 11% [5].

2.2 Protocole SARG04

Le protocole BB84 fait l'hypothèse d'une émission unitaire de photons. Dans la réalité, les systèmes utilisent donc des lasers fortement atténués, générant des impulsions multiphotons qui suivent une distribution de Poisson, définie par la formule $P(i) = \frac{\mu^i}{i!}e^{-\mu}$, où i représente le nombre de photons par impulsion et μ est le nombre moyen de photons, avec $0 \leq \mu \leq 1$. Ces photons surnuméraires induisent une faille potentielle qui peut être utilisée par Ève. Pour limiter ce risque, Scarani et al. ont introduit un protocole de distribution quantique de clés (QKD) plus robuste, nommé SARG04 [13]. Comme dans BB84, Alice sélectionne toujours une base de polarisation aléatoire et envoie un photon unique, mais dans le cas de SARG04, Alice annonce uniquement à Bob l'un des 4 couples d'états non-orthogonaux choisis : $\{|0\rangle, |+\rangle\}, \{|0\rangle, |-\rangle\}, \{|1\rangle, |+\rangle\}, \{|1\rangle, |-\rangle\}$. Bob, de son côté, réalise une mesure en choisissant aléatoirement une base de détection, puis compare le résultat obtenu avec l'ensemble annoncé. Si l'état mesuré est orthogonal à l'un des états de l'ensemble, il peut identifier avec certitude l'état envoyé par Alice et sa mesure est dite "concluante". Dans le cas contraire, la mesure est non concluante. Comme Alice n'annonce pas directement la base utilisée, ce protocole nécessite pour Ève un stockage de qubits plus important et ses tentatives de recopie induisent un QBER théorique supérieur à 14.9% [1]. Le QBER est ici défini par :

$$\text{QBER}_{\text{SARG04}} = \frac{\text{nombre de bits concluants incorrects}}{\text{nombre total de bits concluants}} \quad (2)$$

Notons que dans les deux cas (BB84 ou SARG04), le QBER correspond au ratio entre les bits mal lus par Bob sur le nombre de bits que Bob aurait dû lire correctement d'après un protocole donné, appelé gain total.

2.3 Sources photoniques de bruit

Quel que soit le protocole choisi, BB84 ou SARG04, les mesures réalisées par Bob ne peuvent être considérées comme parfaites. D'une part, Bob est soumis à un bain de n_B photons ambiants qui peuvent être confondus avec les photons envoyés par Alice. Il faut donc supposer l'existence d'un bruit de fond induit par ces photons.

Par ailleurs, indépendamment de toute illumination, tout système photonique génère nécessairement des photons parasites notés n_D qui se créent avec un certain courant I_{dc} ("dark current" en anglais) [10, 12]. L'intensité de ce courant ("dark count rate") est décrite par un nombre de photons par seconde et est généralement exprimée en Hz.

3 Effet du canal sous-marin sur la transmission quantique

Dans un contexte sous-marin, les performances des protocoles de QKD sont très sensibles aux caractéristiques du canal. Deux éléments jouent en particulier un rôle majeur : l'atténuation du signal quantique, en fonction de la salinité et la turbidité de l'eau, et l'irradiance sous-marine qui quantifie le flux de photons ambiants.

3.1 Atténuation sous-marine

Le faisceau laser étant considéré comme collimaté, on néglige les pertes géométriques de propagation. Ainsi, l'atténuation du signal quantique dans un canal sous-marin est principalement due à l'absorption et la diffusion des photons par les molécules d'eau et autres particules en suspension. Le coefficient d'absorption $a(\lambda)$ quantifie la perte d'énergie due aux interactions photon-molécule, tandis que le coefficient de diffusion $b(\lambda)$ décrit la déviation des photons causée par les particules en suspension. L'atténuation totale est décrite par le paramètre d'extinction $\alpha(\lambda) = a(\lambda) + b(\lambda)$ [9] qui dépend de la longueur d'onde λ et varie en fonction du type d'eau (claire, côtière ou turbide). En effet, chaque type d'eau présente des caractéristiques d'absorption et de diffusion distinctes, ce qui modifie le coefficient d'atténuation et par conséquent, la transmission du signal. Le coefficient d'atténuation global $A(L, \lambda)$ lié à la propagation sur une distance L est modélisé par la loi de Beer-Lambert [3] :

$$A(L, \lambda) = \exp\left(-\alpha(\lambda)L\left(\frac{d_1}{\theta L}\right)^T\right) \quad (3)$$

où $\theta = 6°$ est l'angle de divergence total du faisceau émis par l'émetteur, T est un facteur de correction dépendant du type d'eau, comme indiqué dans Table 1, d_1 est le diamètre de l'ouverture de l'émetteur et L est la distance de transmission.

3.2 Irradiance sous-marine

L'irradiance sous-marine dépend des conditions d'ensoleillement. Elle représente l'intensité lumineuse ambiante qui constitue une source de bruit dans les systèmes de QKD. Elle se caractérise par un rapport signal sur bruit (SNR) qui affecte directement le taux d'erreur de bit quantique (QBER). L'irradiance sous-marine se modélise par l'expression :

$$R(z, \lambda) = R_0(\lambda)e^{-K_\infty z} \quad (4)$$

où $R_0(\lambda)$ est l'irradiance à la surface pour une longueur d'onde donnée λ, K_∞ coefficient d'atténuation d'irradiance et z la profondeur sous-marine [9].

4 QBER pour BB84 et SARG04 en milieu sous-marin

La mise en oeuvre opérationnelle de ces protocoles recourt à des sources cohérentes laser fortement atténuées dont le nb de photons à chaque impulsion suit une loi de Poisson d'espérance μ. Le protocole SARG04 a été développé précisément dans ce contexte ; celui de BB84 en revanche considérait dans sa version initiale une source monophotonique idéale [6]. La contribution [8] s'attache à développer au premier ordre les expressions des QBER (1) et (2) dans le cas opérationnel d'une source de photons suivant une loi de Poisson. Elles requièrent pour cela deux quantités clés : la probabilité d'événements photoniques émanant du bruit de fond y_0, et la probabilité globale de transmission notée η :

$$\text{QBER}_{\mu,\text{BB84}} = \frac{1}{Q_{\mu,\text{BB84}}} \left(e_0 y_0 + e_{det}(1 - e^{-\eta\mu}) \right) \quad (5)$$

$$\text{QBER}_{\mu,\text{SARG04}} = \frac{1}{Q_{\mu,\text{SARG04}}} \left[\frac{1}{4} y_0 e^{-\eta\mu} + \frac{e_{det}}{2}(1 - e^{-\eta\mu}) \right] \quad (6)$$

où $Q_{\mu,\text{BB84}}$ (resp. $Q_{\mu,\text{SARG04}}$) représente le gain total associé au protocole BB84 (resp. SARG04), défini comme :

$$Q_{\mu,\text{BB84}} = y_0 + 1 - e^{-\eta\mu} \quad (7)$$

$$Q_{\mu,\text{SARG04}} = \frac{1}{4} y_0 e^{-\eta\mu} + \left(\frac{e_{det}}{2} + \frac{1}{4} \right) (1 - e^{-\eta\mu}) \quad (8)$$

e_{det} désigne la probabilité qu'un photon envoyé par Alice soit détecté avec erreur et $e_0 = 0.5$ la probabilité qu'un photon de bruit induise une détection erronée.

En sous-marin, les définitions de y_0 et η dépendent des paramètres d'atténuation et irradiance définies en section 3.

Nombre moyen de photons de bruit y_0 Pour réaliser la mesure de l'état de polarisation d'un photon, Bob doit utiliser 2 APDs en mode Geiger (chacune avec un filtre polarisé) pour chaque base, soit 4 diodes en tout. D'après [10, 6], on peut estimer que le nombre moyen de photons de bruit, photons ambiants et photons de bruit liés au système de mesure (dark current), qui atteint les 4 détecteurs de Bob, provoqué par une impulsion d'une durée Δt écoutée durant une durée $\Delta t'$, est donné par l'expression [11] :

$$y_0 = 4\left(n_D + \frac{n_B}{2}\right) = 4 I_{dc}\,\Delta t + \frac{R\,S\,\Delta t'\,\lambda\,\Delta\lambda\,\Omega}{h_p c_{\text{light}}} \quad (9)$$

où I_{dc} est le dark current, R l'irradiance définie selon (4), $S = \pi\,(d_2/2)^2$ la surface de l'ouverture du récepteur avec d_2 le diamètre de la lentille réceptrice, $\Omega = 2\pi\,(1 - \cos\,(\delta/2))$ son angle solide avec δ l'angle d'ouverture du capteur, h_p la constante de Planck, c_{light} la vitesse de la lumière et $\Delta\lambda$ la largeur spectrale du filtre.

Probabilité globale de transmission η La probabilité globale de transmission η combine la probabilité de détection par Bob (η_{Bob}) et les pertes dans le canal quantique sous-marin. Elle peut être formulée comme suit [4] :

$$\eta = \eta_{\text{Bob}} \cdot A(L, \lambda) \quad (10)$$

où $A\,(L, \lambda)$ est l'atténuation définie selon (3), comprise ici comme la probabilité que le photon émis par Alice arrive effectivement à Bob.

Dans la section suivante, nous proposons de valider numériquement ces expressions par des simulations de Monte-Carlo.

5 Simulations numériques

En se basant sur les formules présentées dans la section précédente, nous pouvons examiner l'impact de divers paramètres du canal sous-marin non turbulent, tels que le type d'eau et les conditions d'ensoleillement, sur les performances du QBER des protocoles BB84 et SARG04. Pour cela, nous reprenons les expressions analytiques de QBER données précédemment et les comparons à des simulations de type Monte-Carlo. Pour ce faire, nous considérons 10000 paquets de 1000 photons initialement émis par Alice et appliquons ensuite des choix probabilistes élémentaires modélisant la chaîne de transmissions complète de la procédure de QKD. Les courbes théoriques et les résultats de simulations numériques présentées ci-dessus reposent sur un sous-ensemble de paramètres figurant dans Table 1.

TABLE 1 : Paramètres du système et du canal [6].

Paramètre	Définition	Valeur
δ	Ouverture du capteur	180 degrés
$\Delta\lambda$	Largeur spectrale	30 nm
λ	Longueur d'onde	530 nm
Δt	Période de bit	35 ns
$\Delta t'$	Temps de porte	200 ps
η_{Bob}	Efficacité de détection	0.5
e_{det}	Détection avec erreur	3.3%
I_{dc}	dark count rate	60 Hz
K_∞	Coefficient d'atténuation	0.08 m^{-1}
z	Profondeur	100 m
T	Coefficient de correction	0.16
d_1	Diamètre émetteur	10 cm
d_2	Diamètre récepteur	10 cm
y_0	Probabilité de bruit	8.67 $\times 10^{-6}$
α	Coefficient d'extinction	
	Eau claire	0.151 m^{-1}
	Eau côtière	0.398 m^{-1}
	Eau trouble	2.190 m^{-1}

5.1 Effets du type d'eau

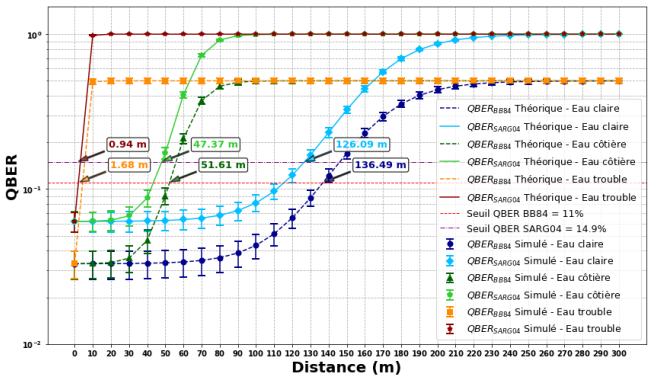

FIGURE 1 : $\text{QBER}_{\text{BB84}}$ et $\text{QBER}_{\text{SARG04}}$ théorique et simulé en fonction de la distance pour différents types d'eau.

La Figure 1 présente les résultats de simulation du QBER en fonction de la distance pour les protocoles BB84 et SARG04 dans un environnement sous-marin non turbulent, en considérant trois types d'eau "claire, côtière et trouble" selon la classification de Mobley [9]. Les courbes simulées et théoriques correspondent presque parfaitement, confirmant la validité des modèles utilisés. Il est observé que le $\text{QBER}_{\text{SARG04}}$ est environ deux fois plus élevé que le $\text{QBER}_{\text{BB84}}$ à toutes les distances [14]. En outre, l'analyse des écarts types des résultats simulés révèle une variabilité plus faible pour SARG04 par

rapport à BB84. L'étude des distances maximales atteignables en fonction des seuils définis en section 2 montre que les distances limites obtenues pour BB84 sont supérieures à celles de SARG04 dans toutes les conditions : 1.68 m, 51.61 m et 136.49 m pour BB84, contre 0.94 m, 47.37 m et 126.09 m pour SARG04. Ces résultats montrent clairement que le type d'eau a un impact significatif sur les performances du système. À mesure que la turbidité augmente, l'atténuation du signal devient plus importante, entraînant une diminution marquée de la distance de transmission. Cette réduction de portée est plus prononcée pour SARG04, qui est davantage affecté par les erreurs induites par le canal sous-marin.

5.2 Effets des conditions atmosphériques

Les cinq scénarios suivants modélisent des conditions atmosphériques diverses, influençant l'irradiance sous-marine :
- Scénario 1 : Atmosphère claire avec une lune pleine près du zénith, $R_0(\lambda) = 10^{-3}\,\mathrm{W/m^2},\ y_0 = 2.65 \times 10^{-7}$,
- Scénario 2 : Ciel nuageux, soleil près de l'horizon, $R_0(\lambda) = 10\,\mathrm{W/m^2},\ y_0 = 2.65 \times 10^{-3}$,
- Scénario 3 : Atmosphère brumeuse, soleil près de l'horizon, $R_0(\lambda) = 50\,\mathrm{W/m^2},\ y_0 = 1.32 \times 10^{-2}$,
- Scénario 4 : Ciel nuageux, soleil au zénith, $R_0(\lambda) = 125\,\mathrm{W/m^2},\ y_0 = 3.31 \times 10^{-2}$,
- Scénario 5 : Atmosphère claire, soleil au zénith, $R_0(\lambda) = 500\,\mathrm{W/m^2},\ y_0 = 1.32 \times 10^{-1}$.

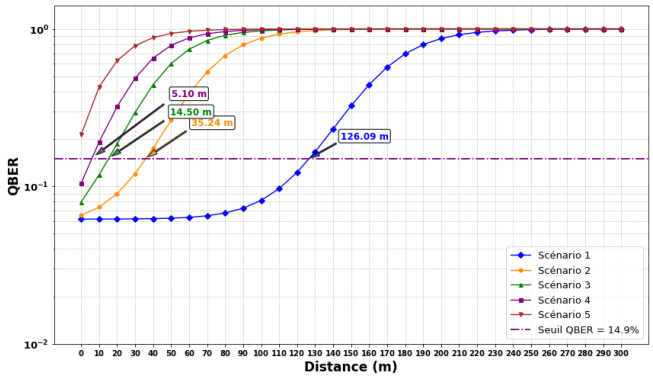

FIGURE 2 : $\mathrm{QBER}_{\mathrm{SARG04}}$ en fonction de la distance pour différents scénarios dans l'eau claire.

Dans la Figure 2, on observe que l'irradiance R a un impact direct sur le QBER en raison de l'augmentation du bruit de fond causé par l'ajout de photons indésirables. Dans le cadre des simulations pour le protocole SARG04 dans l'eau claire, il est observé que la distance de transmission maximale diminue considérablement en journée par rapport à la nuit, en raison de l'augmentation du bruit de fond. Par exemple, la distance maximale atteinte dans le Scénario 1 est de 126.09 m, tandis que dans le Scénarios 5, la distance tombe rapidement sous le seuil de QBER, les valeurs décroissant à mesure que l'irradiance augmente. Cela montre l'impact significatif du bruit de fond sur la portée de transmission.

6 Conclusion

Nous avons simulé et comparé les performances de la distribution quantique de clés sous-marine (UQKD) pour les protocoles BB84 et SARG04 en fonction du taux d'erreur de bit quantique (QBER) et de la distance de transmission. Les résultats montrent que le QBER de SARG04 est plus élevé que celui de BB84 et sa distance maximale de transmission sécurisée est plus courte.

Dans des travaux futurs, nous envisageons d'autres protocoles, notamment impliquant de l'intrication quantique, pour lesquels l'effet du canal sous-marin reste à modéliser.

Références

[1] C. BRANCIARD et AL. : Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3):032301–032318, 2005.

[2] G. BRASSARD et C. H. BENNETT : Quantum cryptography : Public key distribution and coin tossing. *In International conference on computers, systems and signal processing*, pages 175–179, 1984.

[3] M. ELAMASSIE et AL. : Performance characterization of underwater visible light communication. *IEEE Transactions on Communications*, 67(1):543–552, 2018.

[4] C. FUNG et AL. : Performance of two quantum-key-distribution protocols. *Physical Review A—Atomic, Molecular, and Optical Physics*, 73(1):012337, 2006.

[5] N. GISIN et AL. : Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[6] A. HOSSEIN et F. RAOUF : Performance analysis of quantum key distribution in underwater channels. *arXiv preprint arXiv :2208.11493*, 2022.

[7] A. KUMAR et S. GARHWAL : State-of-the-art survey of quantum cryptography. *Archives of Computational Methods in Engineering*, 28:3831–3868, 2021.

[8] X. MA et AL. : Practical decoy state for quantum key distribution. *Physical Review A*, 72:012326, Jul 2005.

[9] C. D. MOBLEY : *Light and water : radiative transfer in natural waters*. Academic Press Inc, 1994.

[10] P. PAGLIERANI et AL. : A primer on underwater quantum key distribution. *Quantum Engineering*, 2023(1): 7185329, 2023.

[11] D. J. ROGERS et AL. : Free-space quantum cryptography in the h-alpha fraunhofer window. *In Proceedings of SPIE*, volume 6304, page 630417, 2006.

[12] B. E. A. SALEH et M. Carl TEICH : *Fundamentals of Photonics*. Wiley-Interscience, 2nd édition, 2007.

[13] V. SCARANI et AL. : Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review letters*, 92(5):057901, 2004.

[14] H. SINGH et AL. : Quantum key distribution protocols : a review. *Journal of Computer Engineering*, 16(2):1–9, 2014.

[15] W. K. WOOTTERS et W. H. ZUREK : A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.