Haut Conseil de l'Évaluation de la Recherche et de l'Enseignement Supérieur

DOCUMENT D'AUTOÉVALUATION

Équipe QI

LIP6

Campagne d'évaluation 2023-2024 — Vague D

Table des matières

1 INFORMATIONS GÉNÉRALES SUR L'ÉQUIPE QI **3**
1.1 Les thématiques scientifiques et leurs enjeux . . . 3
Protocoles d'information quantique . . . 4
Fondements de l'information quantique . . . 5
Démonstrateurs optiques d'information quantique . . . 5

2 INTRODUCTION DU PORTFOLIO **7**

3 AUTOÉVALUATION DU BILAN **8**
3.1 Autoévaluation de l'équipe . . . 8
Domaine 2. Attractivité . . . 8
Domaine 3. Production scientifique . . . 10
Domaine 4. Inscription des activités de recherche dans la société . . . 11

4 RÉFÉRENCES BIBLIOGRAPHIQUES EXTERNES **13**

5 RÉFÉRENCES BIBLIOGRAPHIQUES SIGNIFICATIVES DE QI **14**

A ANNEXE — MEMBRES PERMANENTS AU 31/12/2022 **17**

1 INFORMATIONS GÉNÉRALES SUR L'ÉQUIPE QI

Nom de l'équipe : Information Quantique (QI)

Responsable de l'équipe : Damian Markham (sur toute la période), Frédéric Grosshans (co-responsable depuis 2020)

	2017	2018	2019	2020	2021	2022
PR	0	0	0	0	0	0
MCF HDR	0	0	0	0	0	0
MCF	0	0	0	0	0	0
DR	0	0	1	2	2	2
CR HDR	1	3	2	1	1	1
CR	2	0	0	1	2	2
Total permanents	3	3	3	4	5	5
Émérites	0	0	0	0	0	0
Doctorants	6	9	17	17	20	16
Ingénieurs CDD ou hors tutelles	0	0	1	2	1	0
Post-doc, ATER, etc.	3	1	3	5	2	5
Stagiaires	1	5	2	4	7	12
Total non permanents	10	15	23	28	30	33
Total avec émérites	**13**	**18**	**26**	**32**	**35**	**38**
Equivalent temps plein recherche	3.0	3.0	3.0	4.0	5.0	5.0

TABLE 1 – Personnels QI sur la période 2017-2022 (au 1er juillet de chaque année)

1.1 Les thématiques scientifiques et leurs enjeux

L'information quantique repose sur le fait que les règles ou les lois du traitement de l'information dépendent des lois physiques sous-jacentes. C'est aussi le cas dans le monde classique, par exemple dans le coût énergétique fondamental de l'effacement de l'information, dit "principe d'effacement de Landauer". Cependant, dès les années 1980, il a été démontré que lorsque les porteurs de l'information sont quantiques, il est possible d'obtenir des avantages considérables par rapport à la meilleure approche classique possible en matière de traitement de l'information.

Cet avantage quantique a été démontré dans des domaines tels que l'accélération exponentielle de calculs, une sécurité, des communications et une précision fondamentale dans les mesures impossibles à obtenir par des moyens classiques.

Les travaux de l'équipe d'information quantique (QI) sont fondamentalement unifiés par le désir de comprendre, d'exploiter et de démontrer ces avantages quantiques, en particulier dans le cadre des réseaux distribués. Nous pouvons classer nos travaux en trois domaines de l'information quantique, interconnectés entre eux :

- *Protocoles.* Nous développons de nouveaux protocoles et algorithmes qui présentent un avantage quantique prouvé par rapport à toute approche classique.
- *Fondements.* Nous nous efforçons de comprendre et de caractériser les origines de l'avantage quantique.
- *Démonstrateurs optiques.* Nous démontrons expérimentalement l'avantage quantique dans des dispositifs d'optique quantique.

Ces trois domaines, répartis entre l'informatique théorique, la physique et l'ingénierie, sont implicitement liés les uns aux autres, ce qui constitue un avantage majeur de notre groupe interdisciplinaire, qui nous distingue des autres groupes du domaine en France, en Europe et au niveau international. L'objectif ultime est de développer, comprendre et démontrer l'avantage quantique. D'une part, le développement de protocoles quantiques donne des exigences pour leur mise en œuvre —en termes d'états, de mesures et de processus nécessaires—. D'autre part, la réalité expérimentale du bruit et des pertes nécessite souvent une adaptation des protocoles pour les prendre en compte tout en conservant l'avantage quantique —qu'il s'agisse de sécurité, de complexité ou autre—. Parallèlement, le développement de protocoles nous aide à identifier les caractéristiques essentiellement quantiques qui sont en jeu dans cet avantage quantique. Grâce à ces informations, nous pouvons développer de meilleurs protocoles, plus adaptés, et même trouver de nouvelles applications. Comprendre quelles sont les caractéristiques quantiques en jeu nous aide également à identifier de nouvelles façons, plus robustes, de démontrer l'avantage quantique.

Un exemple de ces liens peut être vu dans la délégation en aveugle et vérifiée de l'informatique quantique, inventée par un membre de l'équipe QI [Fitzsimons and Kashefi, 2017, 1, 3]. Dans ces travaux, un client quantique faible,

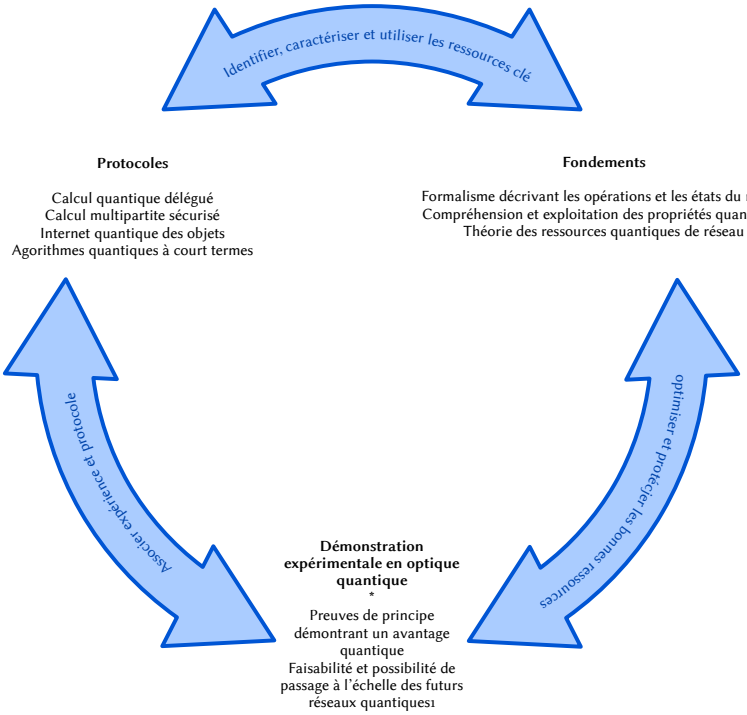

FIGURE 1 –

ayant seulement le pouvoir de préparer et d'envoyer des systèmes quantiques uniques, avec un ordinateur classique, peut promouvoir leur puissance à l'informatique quantique complète en accédant à distance à un serveur d'ordinateur quantique, d'une manière sécurisée –de sorte que le serveur ne connaisse ni les données ni l'algorithme exécuté, et que le client soit sûr d'obtenir le bon résultat—. Peu après ces premiers travaux, une autre approche avec un client entièrement classique a été présentée par Reichardt et al. [6] (RUV), qui nécessite toutefois deux serveurs qui ne sont pas autorisés à communiquer l'un avec l'autre. Bien qu'il s'agisse d'un résultat important, l'exigence de deux serveurs non communicants est difficile à justifier et à imposer en tant que mesure de sécurité. La question qui se pose alors est de savoir si l'on peut faire mieux, et quelles sont les exigences et les ressources nécessaires à la délégation. De ce point de vue, il s'agit d'une question fondamentale. D'une part, RUV utilise explicitement la non-localité de Bell — des corrélations quantiques uniques qui n'ont été démontrées expérimentalement que récemment, à des taux loin d'être applicables ; la non-localité de Bell est à l'origine du prix Nobel de physique 2022—. L'équipe QI a montré dans une série d'articles qu'il peut y avoir une correspondance entre les deux approches où les corrélations nécessaires pour la sécurité sont plus faibles que la non-localité de Bell, mais où les corrélations dites "de steering" suffisent [Gheorghiu et al., 2017b, 4]. Cela a ouvert la possibilité de démontrer l'existence du calcul quantique à l'aveugle vérifié en utilisant simplement des dispositifs optiques à variables continues (CV), où seules les opérations gaussiennes sont disponibles. En CV gaussiennes, on sait que les corrélations non locales de Bell sont impossibles, mais que les corrélations de steering sont possibles. Cela a considérablement élargi les voies potentielles de démonstration expérimentale du protocole.

Protocoles d'information quantique

Les protocoles développés par l'équipe QI sont divers, avec un message clair que l'avantage quantique va bien au-delà des deux exemples les plus connus de l'algorithme de factorisation de Shor [7] et de la distribution quantique de clés [2]. En effet, nous avons développé des protocoles pour le calcul quantique délégué [Fitzsimons and Kashefi, 2017, Kashefi and Pappa, 2017, Naveh et al., 2018, Cojocaru et al., 2019, Gheorghiu et al., 2018, Leichtle et al., 2021], la communication anonyme [Unnikrishnan et al., 2019], le partage de secrets [Arzani et al., 2019], le calcul multipartite sécurisé [Clementi et al., 2017], la délégation de capteurs quantiques [Shettell and Markham, 2022], les algorithmes quantiques NISQ [Coyle et al., 2020b], etc. Le thème commun est que, pour une tâche ou un problème donné, ils accomplissent quelque chose qui ne peut pas du tout être réalisé de manière classique (par exemple, le partage des secrets quantiques est une tâche intrinsèquement quantique) ou qui est plus efficace que ce qui est possible de manière classique.

Fondements de l'information quantique

En ce qui concerne les fondements, l'équipe QI a exploré le rôle et la caractérisation de différents comportements spécifiquement quantiques, notamment l'intrication, la non-localité, le steering et la non-contextualité. Généralement, ces comportements sont formulés en termes de corrélations impossibles à obtenir par des ressources classiques. Nous avons développé et montré la relation entre ces caractéristiques et l'avantage quantique, par exemple dans la délégation [4] et la communication [Meyer et al., 2022], et elles ont conduit à plusieurs nouvelles directions d'avantage quantique potentiel, par exemple dans le témoignage de dimension [Sohbi et al., 2021b, Sohbi et al., 2021a] et la sécurité [Mansfield and Kashefi, 2018].

L'équipe QI a également mis au point plusieurs techniques de certification et de vérification des états, comportements et avantages quantiques, c'est-à-dire des moyens de vérifier que le dispositif, le protocole ou l'algorithme quantique fonctionne comme il est censé le faire. Ces techniques vont de la vérification du calcul quantique [Fitzsimons and Kashefi, 2017], aux états quantiques [Markham and Krause, 2020], aux canaux [Unnikrishnan and Markham, 2020], etc. Nous travaillons à différents niveaux de confiance dans les dispositifs, de la confiance totale mais bruitée, par exemple dans l'approche tomographique et de benchmarking [Derbyshire et al., 2021] jusqu'au cas où les dispositifs sont supposés agir de manière malveillante en prétendant qu'ils donnent un bon résultat alors qu'ils ne le font pas — ce que l'on appelle l'indépendance des dispositifs [Unnikrishnan and Markham, 2019]. Nous avons été reconnus comme des experts dans ce domaine, invités à rédiger une revue qui est rapidement devenue une référence standard [Eisert et al., 2020].

Un autre domaine de recherche permettant des avancées fondamentales est l'exploration de l'information quantique à variables continues (CV). Cette dernière se distingue de l'information quantique standard par l'utilisation de systèmes dont la dimension est infinie. D'une part, ces systèmes offrent un grand potentiel en termes de mise en œuvre, par exemple avec une efficacité de mesure élevée et une génération d'intrication inégalée de millions de systèmes —bien au-delà des 10-20 possibles pour les systèmes quantiques à qubits standard—. D'autre part, la théorie des espaces états de dimension infinie présente des défis particuliers pour la formulation d'énoncés formels pour le traitement de l'information. Cette axe de travail a été mené en collaboration avec des collègues expérimentateurs du Laboratoire Kastler Brossel (LKB) —en effet, leurs systèmes, et d'autres systèmes similaires, constituent une grande motivation pour cette ligne de travail—. Au démarrage de cette direction recherche, l'équipe QI a montré que les versions CV du calcul sous-universel peuvent avoir un avantage quantique prouvé en termes de complexité de calcul [Douce et al., 2017] *(Portfolio 01)*. Il s'agissait de l'un des premiers résultats montrant un résultat de complexité pour un calcul authentiquement CV. Depuis, l'équipe QI a énormément augmenté la quantité de travail dans cette direction, significativement stimulée par l'arrivée dans l'équipe de l'inventeur de la distribution quantique de clés CV à états cohérents [5].Nous avons développé l'identification et la caractérisation des ressources clés [Chabaud et al., 2020b], en les utilisant pour comprendre [Chabaud et al., 2021b] et certifier l'avantage quantique [Chabaud et al., 2020a].Nous travaillons actuellement avec les équipes expérimentales du LKB en vue d'une démonstration expérimentale.

Démonstrateurs optiques d'information quantique

L'optique quantique expérimentale dans l'équipe QI suit deux directions principales, la première s'appuyant sur la mise en œuvre de la distribution quantique de clés, la seconde, la mise en œuvre de nouveaux protocoles et de nouvelles primitives démontrant l'avantage quantique.

Distribution quantique de clés. En distribution quantique de clés (QKD), l'objectif est d'établir une clé aléatoire sûre du point de vue de la théorie de l'information entre deux parties, en envoyant et en mesurant des systèmes quantiques élémentaires. Expérimentalement, cela fonctionne en utilisant des photons. À ce jour, de nombreuses expériences ont démontré la QKD, et plusieurs start-ups bien établies vendent des dispositifs. Les expériences de l'équipe QI travaillent dans le régime CV et ont permis d'augmenter considérablement la distance et l'efficacité grâce à une combinaison d'optimisations optiques, électroniques, logicielles et théoriques [Ghorai et al., 2019b, Piétri et al., 2022b].

Cependant, en raison des pertes et du bruit inéluctables, il existe des limites fondamentales à l'efficacité de la QKD sans infrastructure supplémentaire —essentiellement des répéteurs quantiques (nécessitant de bonnes mémoires quantiques) et des satellites—. L'équipe QI a réalisé plusieurs travaux explorant les exigences et le potentiel de l'utilisation de satellites [Dequal et al., 2021] pour la QKD et l'information quantique en général.

Nous explorons également le développement de mémoires quantiques en collaboration avec le groupe expérimental de Julien Laurat au LKB [Cavaillès et al., 2018], un élément qui sera également important pour les protocoles au-

delà de la QKD. Cette collaboration est également à l'origine de Welinq [1], une entreprise issue de l'équipe QI.

Nouveaux protocoles démontrant l'avantage quantique. Au-delà de la QKD, l'équipe QI a mis en œuvre la démonstration expérimentale de plusieurs protocoles quantiques. Ici, ces protocoles sont réalisés à l'aide d'encodages à variables discrètes.

Il s'agit notamment de démonstrations de la monnaie quantique [Bozzio et al., 2018, Bozzio et al., 2019], du steering [Orieux et al., 2018], de la complexité de la communication [Kumar et al., 2019] et de la vérification de problèmes NP complets [Centrone et al., 2021]. Dans tous ces cas, une attention particulière a dû être accordée à la gestion de bruits et de pertes réalistes. L'équipe QI explore également l'utilisation de puces intégrées qui offrent de grandes perspectives de miniaturisation des technologies quantiques [Piétri et al., 2022b, Appas et al., 2021, Moody et al., 2022].

1. https://welinq.fr

2 INTRODUCTION DU PORTFOLIO

Cette section identifie les éléments de portfolio présentés par l'équipe QI. Chaque élément disposant de sa propre fiche explicative, nous nous contentons ici d'en donner une liste simple :

- *Élément 1 (publication) :* [Douce et al., 2017] ; Continuous-Variable Instantaneous Quantum Computing is Hard to Sample démontrant la complexité algorithmique de l'optique quantique avec des variables continues et des détecteurs réalistes.
- *Élément 2 (publication) :* [Bredariol Grilo et al., 2021b] : Oblivious Transfer is in MiniQCrypt démontrant qu'une fonction à sens unique post-quantiquement sûre et des communications quantiques suffisent à construire un protocole de transfert inconscient, une primitive cryptographique importante et vraisemblablement impossible à construire dans le monde classique sous des hypothèses analogues.
- *Élément 3 (jeu de données consolidé) :* The Quantum Protocol Zoo, un référentiel ouvert de protocoles pour les réseaux quantiques, offrant un moyen compact et canonique d'explorer ces protocoles. Il facilite la communication entre informaticiens, ingénieurs et physiciens sur une plate-forme unique.
- *Élément 4 (logiciel) :* OptiQraft, jeu vidéo pédagogique sur l'optique quantique.

3 AUTOÉVALUATION DU BILAN

3.1 Autoévaluation de l'équipe

Domaine 2. Attractivité

Référence 1. L'unité est attractive par son rayonnement scientifique et s'insère dans l'espace européen de la recherche.

L'équipe QI présente un caractère interdisciplinaire unique, rare en Europe et même dans le monde. Le domaine de l'information quantique est fondé sur le lien entre l'informatique, la physique théorique et les réalités des dispositifs expérimentaux. Ces domaines très différents ne sont pas seulement importants d'un point de vue historique, mais les recherches les plus pointues sont menées à leurs frontières. Il est clair qu'ils sont tous les trois nécessaires pour parvenir à une utilisation réelle des technologies quantiques, et le fait de travailler à travers ces lignes de démarcation est de plus en plus considéré comme une clé de la réussite dans ce domaine. Ces trois domaines sont couverts par l'équipe QI. Cela couvre à la fois l'informatique théorique —théorie de la complexité, algorithmique et cryptographie— avec les fondements de l'avantage quantique, la physique théorique —intrication, non-classicalité, information quantique à variables continues— et l'optique quantique expérimentale —avec des expériences de démonstration de principe démontrant l'avantage et ouvrant la voie à une mise en œuvre dans le monde réel.

L'équipe QI est un leader européen et mondial reconnu dans le domaine de l'information quantique et des réseaux d'information quantique. Nous participons à de nombreux projets nationaux et européens (voir ci-dessus), dont 4 projets PEPR et 3 projets flagship de l'UE dans le domaine des technologies quantiques. Nous sommes également impliqués dans des actions au service de la communauté, et ce à tous les niveaux. Nous somme présents à la direction du Quantum Information Center Sorbonne[2] (QICS) —Institut de Sorbonne Université— et du Paris Center for Quantum Technologies[3] —qui coordonne les recherches en technologies quantiques à l'échelle de Paris Centre—. Nous sommes également membres du conseil consultatif pour la coordination du projet Flagship de l'UE pour la communication quantique, et du conseil de l'équipe Vision du projet Flagship de l'UE QIA —qui comprend 5 chercheurs permanents parmi plus de 100 dans le projet, chargés d'identifier une vision pour le futur internet quantique—. Au niveau régional, nous sommes présents au comité de pilotage des deux DIM financés successivement par la région Île-de-France, SIRTEQ[4] de 2017 à 2022, puis QuantTip[5].

Référence 2. L'unité est attractive par la qualité de sa politique d'accompagnement des personnels.

Stagiaires, doctorants et postdoctorants. Nous considérons comme essentiel l'accompagnement des membres de l'équipe —stagiaires, doctorants et postdoctorants—, actuels et anciens. Bien entendu, nous les accompagnons dans la préparation de leurs soutenances et auditions, dans la rédaction de leurs rapports, théses et dossiers de candidatures. Nous les conseillons dans leurs démarches et leur écrivons des lettres de recommandations, etc.

Nous sommes également attentifs à envoyer les jeunes chercheurs présenter leurs travaux dans des conférences aussi souvent que possible, afin de les aider à constituer un réseau professionnel. Dans cette optique, nous les encourageons —y compris, bien entendu, par un support financier sous forme de missions— aussi à faire des séjours dans d'autres équipes de recherche et à rendre visite à de futurs employeurs potentiels.

Le devenir des anciens membres de l'équipe est indiqué table 2. Les doctorants du LIP6 travaillant toujours en information quantique se répartissent comme suit : 10 sont postdocs, un est chargé de recherche à l'Inria, et cinq travailent dans l'industrie —Quandela, PsiQuantum et JP Morgan—. Trois docteurs ont choisi d'autres carrières (industrie, éducation nationale et travailleur indépendant). Les anciens postdocs de l'équipe, sauf un, sont restés dans le domaine de l'information quantique (3) ou de l'optique (3), sont 6/7 à avoir des postes permanents. Quatre d'entre eux sont dans l'industrie et trois dans des instituts de recherche.

Une attention toute particulière est accordée au maintien de la cohésion de l'équipe, ce qui semble avoir réussi malgré un accroissement conséquent de sa taille au cours de la période. Bien entendu, les spécialité de chacun des six permanents, étant différentes, des "sous-groupes" existent ; cependant, la porosité des frontières entre les sous-groupes est volontairement maintenue par le coencadrement de nombreux étudiants, des collaborations au sein de l'équipe trop nombreuses pour être énumérées —incluant des travaux de doctorants sans leur directeur

2. https://qics.sorbonne-universite.fr
3. https://www.pcqt.fr
4. https://www.sirteq.org
5. https://quantip.org/

	Domaine	Postdoc	Poste acad.	Entreprise	Sect. public	Total
Doc.	Quantique	10	1	5		**16**
	Optique					**0**
	Autre			2	1	**3**
	Total	**10**	**1**	**7**	**1**	**19**
Postdocs	Quantique		2	1		**3**
	Optique	1		2		**3**
	Autre			1		**1**
	Total	**1**	**2**	**4**	**0**	**7**

TABLE 2 – Dernier emploi connu (avril 2023) des docteurs et postdocs ayant quitté l'équipe QI entre 2017 et 2022.

de thèse [Grosshans et al., 2021, Chabaud et al., 2021a],voire sans permanent du tout [Booth et al., 2022]— et le mélange des sous-groupes dans les différents bureaux. À cela s'ajoute une journée annuelle en hiver (sauf en 2020 et 2021), où tous les membres de l'équipe présentent leur travail, et des workshops de trois jours loin de paris (en novemnbre 2021, en sortie de la pandémie, et en mai 2022) dont la vocation est essentiellement d'assurer la cohésion de l'équipe.

L'impression générale des permanents de l'équipe — confortée par les discussions avec les visiteurs — est que cette cohésion est excellente, et contribue fortement à l'attractivité de l'équipe.

En terme de politique de publications, bien entendu, tous les participants au travail sont auteurs, y compris les stagiaires [Landman et al., 2022, Sohbi et al., 2021b] et ingénieurs [Piétri et al., 2022b], et comme indiqué plus haut, il n'y a aucune obligation pour les doctorants d'inclure leur directeur de thèse. L'exemple le plus flagrant est une collaboration entre deux doctorants et un ancien doctorant [Booth et al., 2022], publiée dans Physical Review Letters, mais des collaborations directes avec des groupes extérieurs sont aussi encouragées [Booth and Carette, 2022, Ostermann et al., 2019, Streltsov et al., 2020].

Les postdoctorants, notamment seniors, en plus de leurs collaborations avec les permanents, continuent souvent à travailler indépendamment sur leur ligne de recherche propre, comme on le voit par exemple dans les publications suivantes [Dourdent et al., 2022, Jones et al., 2021, Emeriau et al., 2022].

Chercheurs permanents. Au cours de la période, l'équipe a grandi en passant de 3 à 6 permanents avec l'arrivée de deux chargés de recherche CNRS et d'un maître de conférences. Aucun permanent n'a quitté l'équipe pendant cette période, hormis pour des mobilités temporaires.

Environnement de travail. L'équipe s'est dotée en 2022 d'un *code de conduite* afin d'aider à garantir un environnement sûr pour chacun. Il a été élaboré sous l'impulsion d'un doctorant avec la participation de tous pendant les ateliers de l'équipe en 2021 et 2022. Les discussions durant sa rédaction ont été très intéressantes et animées, et nous tenons à garder ces moments de réflexion sur l'environnement de travail lors de nos prochains ateliers.

Référence 3. L'unité est attractive par la reconnaissance de ses succès à des appels à projets compétitifs.

L'équipe est impliquée dans de nombreux projets Européens — dont une ERC —, ANR et PIA.

Nous sommes au centre des activités françaises dans le domaine de l'information quantique, impliqués dans 4 PEPR et plusieurs autres projets France 2030, dont HQI et France QCI. Les PEPR sont essentiellement des projets de recherche qui soutiendront et accéléreront les activités de recherche actuelles sur les algorithmes et protocoles quantiques (EPiQ), l'informatique quantique photonique (NISQ2LSQ), la QKD indépendante des dispositifs (DIQKD) et la communication quantique (QuComTestBed). Les projets HQI et France QCI visent à développer des plates-formes. L'objectif du projet HQI est d'intégrer les processeurs de calcul quantique à l'infrastructure HPC classique. Le rôle de l'équipe QI est de développer l'utilisation de liens entre les processeurs quantiques et classiques et nous sommes le chef de file de ce WP. Nous sommes également le chef de file du CNRS dans le projet. L'objectif de QuCommTestbed est d'établir une plateforme de communication quantique en France.

HQI et France QCI sont tous deux liés à des efforts européens plus larges - EURO QCS et EURO QCI respectivement, et représentent la contribution de la France à ces objectifs globaux. La collaboration avec les partenaires européens sera donc un élément important de ces travaux.

L'équipe QI fait partie de trois projets "Flagship" de l'UE. En particulier, le projet QIA (quantum internet alliance) est le plus important en termes d'orientation future du groupe et concerne tous les membres de l'équipe QI. L'objectif

du projet QIA est de développer le futur internet quantique.

Référence 4. L'unité est attractive par la qualité de ses équipements et de ses compétences techniques.

Domaine 3. Production scientifique

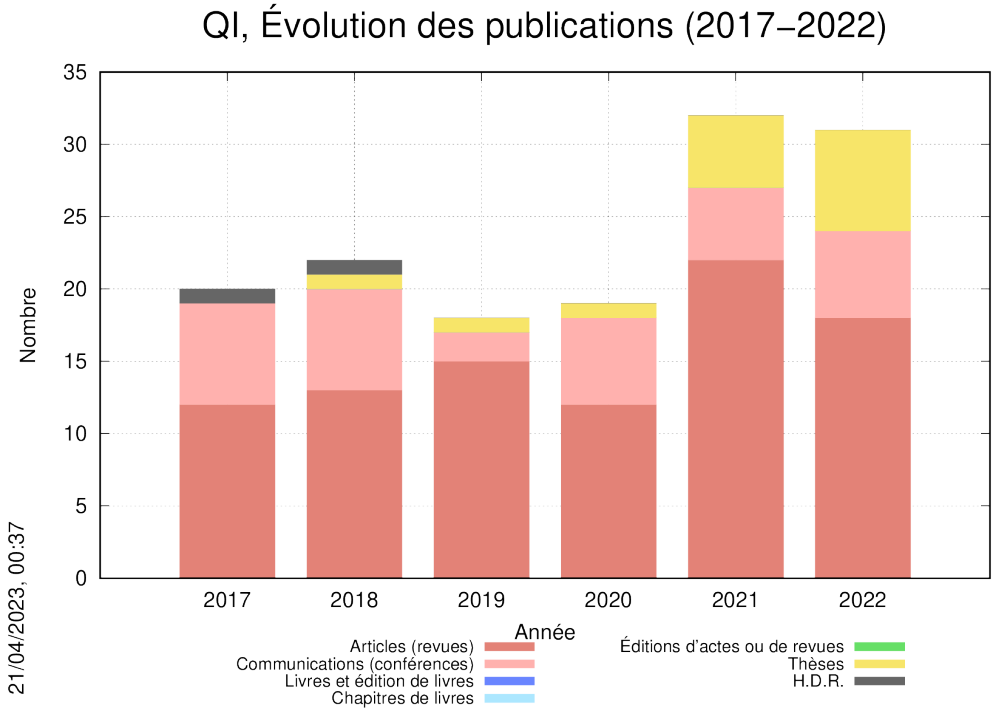

FIGURE 2 – Évolution des publications entre 2017 et 2022

	2017	2018	2019	2020	2021	2022
Articles (revues)	4.00	4.33	5.00	3.00	4.40	3.60
Communications (conférences)	2.33	2.33	0.66	1.50	1.00	1.20

TABLE 3 – Publications par ETPR par an entre 2017 et 2022

Référence 1. La production scientifique de l'unité satisfait à des critères de qualité.

L'équipe QI a régulièrement publié des articles de grande qualité dans des revues et des conférences de premier plan couvrant l'ensemble du domaine. Pendant la période d'évaluation, nous avons publiés 92 articles, 35 compte-rendus de conférences, 40 pré-publications, 19 thèses et deux HDR. Les articles incluent :

1 *Nature Reviews Physics* [Eisert et al., 2020],
2 *Nature Communications* [Centrone et al., 2021, Kumar et al., 2019],
10 *Physical Review Letters* [Booth et al., 2022, Cavaillès et al., 2018, Chabaud et al., 2020b, Douce et al., 2017, Dourdent et al., 2022, Jones et al., 2021, Mansfield and Kashefi, 2018, Shettell and Markham, 2020, Streltsov et al., 2020, Unnikrishnan et al., 2019],
1 *Physical Review X* [Ghorai et al., 2019b]

Soit 14 articles dans des revues de premier plan en physique

Les compte-rendus de conférence incluent :

2 FOCS [Arunachalam et al., 2022, Broadbent and Bredariol Grilo, 2020],
1 EuroCrypt [Bredariol Grilo et al., 2021b],

Soit 3 compte-rendus dans des conférences de premier plan en informatique.

Référence 2. La production scientifique de l'unité est proportionnée à son potentiel de recherche et correctement répartie entre ses personnels.

Les publications et l'activité de l'équipe QI sont globalement assez bien réparties entre les membres parmanents de l'équipe, compte tenu de la durée de présence de chaque permanent dans l'équipe.

En terme de politique de publications, bien entendu, tous les participants au travail sont auteurs, y compris les stagiaires [Landman et al., 2022, Sohbi et al., 2021b] et ingénieurs [Piétri et al., 2022b], et comme indiqué plus haut, il n'y a aucune obligation pour les doctorants d'inclure leur directeur de thèse. L'exemple le plus flagrant est une collaboration entre deux doctorants et un ancien doctorant [Booth et al., 2022], publiée dans Physical Review Letters, mais des collaborations directes avec des groupes extérieurs sont aussi encouragées [Booth and Carette, 2022, Ostermann et al., 2019, Streltsov et al., 2020].

Les postdoctorants, notamment seniors, en plus de leurs collaborations avec les permanents, continuent souvent à travailler indépendamment sur leur ligne de recherche propre, comme on le voit par exemple dans les publications suivantes [Dourdent et al., 2022, Jones et al., 2021, Emeriau et al., 2022].

L'équipe QI a accueilli en postdoc en 2019–2021 chercheur ayant interrompu sa carrière académique. Sa collaboration a abouti à deux prépublications et un article dans PRX Quantum [Leichtle et al., 2021], une excellente revue de physique. Cette collaboration se poursuit maintenant qu'il est dirige une équipe Inria à l'ENS.

Référence 3. La production scientifique de l'unité respecte les principes de l'intégrité scientifique, de l'éthique et de la science ouverte. Elle est conforme aux directives applicables dans ce domaine.

Bien entendu, nous respectons les principes de l'intégrité scientifique, et nous veillons à les transmettre à nos étudiants.

La quasi-totalité des travaux de l'équipe QI sont prépubliés sur arXiv, conformément à la pratique en inforation quantique. Nos publications sont également disponibles sur HAL [6].

L'équipe prête une attention particulière aux probèmes de discrimination, et s'est dotée en 2022 d'un *code de conduite*. Ce document est régulièrement discuté, ce qui permet d'éviter qu'il reste letlre morte.

Domaine 4. Inscription des activités de recherche dans la société

Référence 1. L'unité se distingue par la qualité et la quantité de ses interactions avec le monde non-académique.

L'équipe a des relations importantes avec le monde économique, notamment par la fondation de start-ups (VeriQloud et Welinq), des thèse co-encadrées avec l'industrie (Thalès Alenia Space, VeriQloud, Quandela, Naval Group, Pasqal, Nokia) ou l'ONERA, mais aussi le montage en commun de projets Européens et nationaux, où plus simplement des discussions avec des industriels pour identifier leurs cas d'usage. Plus généralement, l'équipe QI est convaincue que les technologies quantiques sont en train de se transformer d'un sujet de recherche purement académique à une technologie ayant de multiples applications économiques—de la cybersécurité aux mesures de précision, en passant par l'apprentissage automatique— et nous cherchons à favoriser l'adaptation des problèmes universitaires abstraits à ces applications, tout en identifiant de nouvelles problématiques dans ces applications.

L'équipe est également active dans la communication vers les entreprise, avec par exemple la co-animation de la conférence ⟨Q|C|B⟩ (Quantum Computing for Business) 2020, orgoanisée par BpiFrance, la participation d'un étudiant et d'un postdoc de l'équipe à la « core team » du Lab Quantique [7], de nombreuses participations à de tables rondes entre unversité et industrie, etc.

L'ensemble de ces actions a bénéficié d'un accompagnement de la DRV.

Référence 2. L'unité développe des produits à destination du monde culturel, économique et social.

L'équipe a fondé deux start-ups sur la période, VeriQloud et Welinq.

6. https://hal.science/search/index/q/*/structId_i/541726
7. https://lelabquantique.com/

Référence 3. L'unité partage ses connaissances avec le grand public et intervient dans des débats de société.

L'équipe QI interagit régulièrement avec le grand public, à travers des conférences, des interviews et d'autres activités, notamment

- *Fête de la science :* Depuis 2018, l'équipe QI est présente tous les ans[8] sur le stand du LIP6 à la Fête de la Science, avec des activité à destination des lycéens et du public des visiteurs. Celà inclut un stand présentant les prncipes de la distribution quantique de clés, des présentations et des posters, des visites de laboratoires, etc.
- *Vidéo et jeu vidéo* Les doctorants de l'équipe, en collaboration avec les doctorants d'autres laboratoires de Sorbonne Université ont, dans le cadre d'un cours organisé par le QICS créé deux vidéos et un jeu vidéo, optiqraft (cf élément 4 du portfolio) présentant des concepts de l'inforamtion quantique au grand public. Ces éléments sont diponibles en ligne et sont utilisé par le QICS à la Fête de la Science tous les ans.
- *Présentations et interviews* pendant la période, les membres de l'équipe ont donné 8 conférences au grand public et 6 interviews à la radio et à la télévision.
- *Public académique non-spécialiste* Les membres de l'équipe participent à des action de présentation de divers aspects domaine —aspects scientifique, mais aussi financiers, industriels et pédagogiques— vis à vis de public essentiellement académiques non-spécialiste d'information quantique, par des participations à plusieurs tables rondes et présentations orales chaque année. Dans le même esprit, au cours de la période, deux articles non-techniques ont été écrits dans Nature et Nature Physics [Diamanti, 2020, Diamanti and Kashefi, 2017]

8. Sauf pour l'édition 2020 qui a été reportée en ligne

4 RÉFÉRENCES BIBLIOGRAPHIQUES EXTERNES

[1] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *science*, 335(6066) :303–308, 2012.

[2] Charles H Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *arXiv preprint arXiv :2003.06557*, 2020.

[3] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009.

[4] Leonardo Disilvestro and Damian Markham. Quantum protocols within Spekkens' toy model. *Physical Review A : Atomic, molecular, and optical physics*, 95(5), May 2017. 25 pages, 3 figures ; Several changes from previous version, overall readability and structure improved. Many notation issues and typos fixed.

[5] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5) :057902, 2002.

[6] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446) :456–460, 2013.

[7] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2) :303–332, 1999.

5 RÉFÉRENCES BIBLIOGRAPHIQUES SIGNIFICATIVES DE QI

[Appas et al., 2021] Appas, F., Baboux, F., Amanti, M., Lemaítre, A., Boitier, F., Diamanti, E., and Ducci, S. (2021). Flexible entanglement-distribution network with an AlGaAs chip for secure communications. *npj Quantum Information*, 7(1).

[Arunachalam et al., 2022] Arunachalam, S., Bredariol Grilo, A., Gur, T., Oliveira, I., and Sundaram, A. (2022). Quantum learning algorithms imply circuit lower bounds. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 562–573, Denver, United States. IEEE.

[Arzani et al., 2019] Arzani, F., Ferrini, G., Grosshans, F., and Markham, D. (2019). Random coding for sharing bosonic quantum secrets. *Physical Review A*, 100(2) :022303.

[Booth and Carette, 2022] Booth, R. and Carette, T. (2022). Complete ZX-calculi for the stabiliser fragment in odd prime dimensions. In Szeider, S., Ganian, R., and Silva, A., editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24 :1–24 :15, Vienna, Austria. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 22 pages+ 30 pages of references and appendices.

[Booth et al., 2022] Booth, R., Chabaud, U., and Emeriau, P.-E. (2022). Contextuality and Wigner negativity are equivalent for continuous-variable quantum measurements. *Physical Review Letters*, 129(23) :230401. 21 pages + 4 pages of appendices, 1 figure.

[Bozzio et al., 2019] Bozzio, M., Diamanti, E., and Grosshans, F. (2019). Semi-device-independent quantum money with coherent states. *Physical Review A : Atomic, molecular, and optical physics*, 99(2) :022336.

[Bozzio et al., 2018] Bozzio, M., Orieux, A., Trigo Vidarte, L., Zaquine, I., Kerenidis, I., and Diamanti, E. (2018). Experimental investigation of practical unforgeable quantum money. *npj Quantum Information*, 4(1). 8 pages, 5 figures.

[Bredariol Grilo et al., 2021b] Bredariol Grilo, A., Lin, H., Song, F., and Vaikuntanathan, V. (2021b). Oblivious Transfer is in MiniQCrypt. In *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561, Zagreb, Croatia. Springer.

[Broadbent and Bredariol Grilo, 2020] Broadbent, A. and Bredariol Grilo, A. (2020). QMA-Hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge. In *IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, Virtual, United States. IEEE.

[Cavaillès et al., 2018] Cavaillès, A., Le Jeannic, H., Raskop, J., Guccione, G., Markham, D., Diamanti, E., Shaw, D., Verma, V. b., Nam, S. w., and Laurat, J. (2018). Demonstration of Einstein-Podolsky-Rosen Steering Using Hybrid Continuous- and Discrete-Variable Entanglement of Light. *Physical Review Letters*, 121(17).

[Centrone et al., 2021] Centrone, F., Kumar, N., Diamanti, E., and Kerenidis, I. (2021). Experimental demonstration of quantum advantage for NP verification with limited information. *Nature Communications*, 12(1) :850.

[Chabaud et al., 2020a] Chabaud, U., Douce, T., Grosshans, F., Kashefi, E., and Markham, D. (2020a). Building trust for continuous variable quantum states. In Flammia, S. T., editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3 :1–3 :15, Riga, Latvia. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[Chabaud et al., 2021a] Chabaud, U., Emeriau, P.-E., and Grosshans, F. (2021a). Witnessing Wigner Negativity. *Quantum*, 5 :471.

[Chabaud et al., 2021b] Chabaud, U., Ferrini, G., Grosshans, F., and Markham, D. (2021b). Classical simulation of Gaussian quantum circuits with non-Gaussian input states. *Physical Review Research*, 3(3) :033018.

[Chabaud et al., 2020b] Chabaud, U., Markham, D., and Grosshans, F. (2020b). Stellar representation of non-Gaussian quantum states. *Physical Review Letters*.

[Clementi et al., 2017] Clementi, M., Pappa, A., Eckstein, A., Walmsley, I. A., Kashefi, E., and Barz, S. (2017). Classical multiparty computation using quantum resources. *Physical Review A : Atomic, molecular, and optical physics*, 96(6) :062317.

[Cojocaru et al., 2019] Cojocaru, A., Colisson, L., Kashefi, E., and Wallden, P. (2019). QFactory : classically-instructed remote secret qubits preparation. In *ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*, volume 11921 of *Lecture Notes in Computer Science*, pages 615–645, Kobe, Japan. Springer. 51 pages, 4 figures.

[Coyle et al., 2020b] Coyle, B., Mills, D., Danos, V., and Kashefi, E. (2020b). The Born supremacy : quantum advantage and training of an Ising Born machine. *npj Quantum Information*, 6(1) :60.

[Dequal et al., 2021] Dequal, D., Trigo Vidarte, L., Roman Rodriguez, V., Vallone, G., Villoresi, P., Leverrier, A., and Diamanti, E. (2021). Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Information*, 7(1) :10. 10 pages, 12 figures.

[Derbyshire et al., 2021] Derbyshire, E., Mezher, R., Kapourniotis, T., and Kashefi, E. (2021). Randomized Benchmarking with Stabilizer Verification and Gate Synthesis. 18 pages, 3 figures.

[Diamanti, 2020] Diamanti, E. (2020). A step closer to secure global communication. *Nature*, 582(7813) :494–495.

[Diamanti and Kashefi, 2017] Diamanti, E. and Kashefi, E. (2017). Best of both worlds. *Nature Physics*, 13(1) :3–4.

[Douce et al., 2017] Douce, T., Markham, D., Kashefi, E., Diamanti, E., Coudreau, T., Milman, P., van Loock, P., and Ferrini, G. (2017). Continuous-Variable Instantaneous Quantum Computing is Hard to Sample. *Physical Review Letters*, 118(7).

[Dourdent et al., 2022] Dourdent, H., Abbott, A. A., Brunner, N., Šupić, I., and Branciard, C. (2022). Semi-device-independent Certification of Causal Nonseparability with Trusted Quantum Inputs. *Physical Review Letters*, 129(9) :090402. 5 + 17 pages, 1 figure.

[Eisert et al., 2020] Eisert, J., Hangleiter, D., Walk, N., Roth, I., Markham, D., Parekh, R., Chabaud, U., and Kashefi, E. (2020). Quantum certification and benchmarking. *Nature Reviews Physics*, 2 :382–390. Invited review for Nature Reviews Physics.

[Emeriau et al., 2022] Emeriau, P.-E., Howard, M., and Mansfield, S. (2022). Quantum Advantage in Information Retrieval. *PRX Quantum*, 3(2) :020307. 15 pages, 11 figures ; new presentation, additional figures and references.

[Fitzsimons and Kashefi, 2017] Fitzsimons, J. and Kashefi, E. (2017). Unconditionally verifiable blind quantum computation. *Physical Review A : Atomic, molecular, and optical physics*, 96(1) :012303.

[Gheorghiu et al., 2018] Gheorghiu, A., Hoban, M. J., and Kashefi, E. (2018). A simple protocol for fault tolerant verification of quantum computation. *Quantum Science and Technology*, 4(1) :015009.

[Gheorghiu et al., 2017b] Gheorghiu, A., Wallden, P., and Kashefi, E. (2017b). Rigidity of quantum steering and one-sided device-independent verifiable quantum computation. *New Journal of Physics*, 19(2) :023043.

[Ghorai et al., 2019b] Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A. (2019b). Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Physical Review X*, 9(2) :11.

[Grosshans et al., 2021] Grosshans, F., Centrone, F., and Parigi, V. (2021). Cost and Routing of Continuous Variable Quantum Networks. working paper or preprint.

[Jones et al., 2021] Jones, B. D., Šupić, I., Uola, R., Brunner, N., and Skrzypczyk, P. (2021). Network Quantum Steering. *Physical Review Letters*, 127(17) :170405.

[Kashefi and Pappa, 2017] Kashefi, E. and Pappa, A. (2017). Multiparty Delegated Quantum Computing. *Cryptography*, 1(2) :12.

[Kumar et al., 2019] Kumar, N., Kerenidis, I., and Diamanti, E. (2019). Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol. *Nature Communications*, 10 :4152.

[Landman et al., 2022] Landman, J., Thabet, S., Dalyac, C., Mhiri, H., and Kashefi, E. (2022). Classically Approximating Variational Quantum Machine Learning with Random Fourier Features. working paper or preprint.

[Leichtle et al., 2021] Leichtle, D., Music, L., Kashefi, E., and Ollivier, H. (2021). Verifying BQP Computations on Noisy Devices with Minimal Overhead. *PRX Quantum*, 2(4) :040302. 6+9 pages, 2 figures. Extends the results of arxiv :2011.10005 to BQP and refines the discussion on applicability.

[Mansfield and Kashefi, 2018] Mansfield, S. and Kashefi, E. (2018). Quantum Advantage from Sequential-Transformation Contextuality. *Physical Review Letters*, 121(23) :230401. 8 pages, 1 figure.

[Markham and Krause, 2020] Markham, D. and Krause, A. B. (2020). A simple protocol for certifying graph states and applications in quantum networks. *Cryptography*, 4(1) :3. 6 pages.

[Meyer et al., 2022] Meyer, U. I., Grosshans, F., and Markham, D. (2022). Inflated Graph States Refuting Communication-Assisted LHV Models. working paper or preprint.

[Moody et al., 2022] Moody, G., Sorger, V., Blumenthal, D., Juodawlkis, P., Loh, W., Sorace-Agaskar, C., Jones, A., Balram, K., Matthews, J., Laing, A., Davanco, M., Chang, L., Bowers, J., Quack, N., Galland, C., Aharonovich, I., Wolff, M., Schuck, C., Sinclair, N., Lončar, M., Komljenovic, T., Weld, D., Mookherjea, S., Buckley, S., Radulaski, M., Reitzenstein, S., Pingault, B., Machielse, B., Mukhopadhyay, D., Akimov, A., Zheltikov, A., Agarwal, G., Srinivasan, K., Lu, J., Tang, H., Jiang, W., Mckenna, T., Safavi-Naeini, A., Steinhauer, S., Elshaari, A., Zwiller, V., Davids, P., Martinez, N., Gehl, M., Chiaverini, J., Mehta, K., Romero, J., Lingaraju, N., Weiner, A., Peace, D., Cernansky, R., Lobino, M., Diamanti, E., Vidarte, L. T., and Camacho, R. (2022). 2022 Roadmap on integrated quantum photonics. *Journal of Physics : Photonics*, 4(1) :012501.

[Naveh et al., 2018] Naveh, Y., Kashefi, E., Wootton, J., and Bertels, K. (2018). Theoretical and practical aspects of verification of quantum computers. In *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 721–730, Dresden, Germany. IEEE.

[Orieux et al., 2018] Orieux, A., Kaplan, M., Venuti, V., Pramanik, T., Zaquine, I., and Diamanti, E. (2018). Experimental detection of steerability in Bell local states with two measurement settings. *Journal of Optics*, 20(4).

[Ostermann et al., 2019] Ostermann, L., Meignant, C., Genes, C., and Ritsch, H. (2019). Super- and subradiance of clock atoms in multimode optical waveguides. *New Journal of Physics*, 21(2) :025004.

[Piétri et al., 2022b] Piétri, Y., Trigo Vidarte, L., Schiavon, M., Grangier, P., Rhouni, A., and Diamanti, E. (2022b). A Versatile CV-QKD system with a PIC-based receiver. International Conference on Quantum Communication, Measurement and Computing. Poster.

[Shettell and Markham, 2020] Shettell, N. and Markham, D. (2020). Graph States as a Resource for Quantum Metrology. *Physical Review Letters*, 124(11) :110502.

[Shettell and Markham, 2022] Shettell, N. and Markham, D. (2022). Quantum Metrology with Delegated Tasks. *Physical Review A*, 106(5) :052427.

[Sohbi et al., 2021a] Sohbi, A., Markham, D., Kim, J., and Quintino, M. T. (2021a). Certifying dimension of quantum systems by sequential projective measurements. *Quantum*, 5 :472.

[Sohbi et al., 2021b] Sohbi, A., Ohana, R., Zaquine, I., Diamanti, E., and Markham, D. (2021b). Experimental Approach to Demonstrating Contextuality for Qudits. *Physical Review A*, 103(6) :062220.

[Streltsov et al., 2020] Streltsov, A., Meignant, C., and Eisert, J. (2020). Rates of Multipartite Entanglement Transformations. *Physical Review Letters*, 125(8) :080502.

[Unnikrishnan et al., 2019] Unnikrishnan, A., Macfarlane, I., Yi, R., Diamanti, E., Markham, D., and Kerenidis, I. (2019). Anonymity for Practical Quantum Networks. *Physical Review Letters*, 122(24).

[Unnikrishnan and Markham, 2019] Unnikrishnan, A. and Markham, D. (2019). Authenticated teleportation with one-sided trust. *Physical Review A : Atomic, molecular, and optical physics*, 100(3) :032314.

[Unnikrishnan and Markham, 2020] Unnikrishnan, A. and Markham, D. (2020). Authenticated teleportation and verification in a noisy network. *Physical Review A*, 102(4) :042401. 11 pages.

A ANNEXE — MEMBRES PERMANENTS AU 31/12/2022

La table ci dessous liste les membres permanents de l'équipe QI.

NOM	Prénom	Corps	Employeur
BREDARIOL GRILO	Alex	CR	CNRS
DIAMANTI	Eleni	DR	CNRS
GROSSHANS	Frédéric	CR	CNRS
KASHEFI	Elham	DR	CNRS
MARKHAM	Damian	CR (HDR)	CNRS
QUINTINO	Marco	MCF	Sorbonne Université