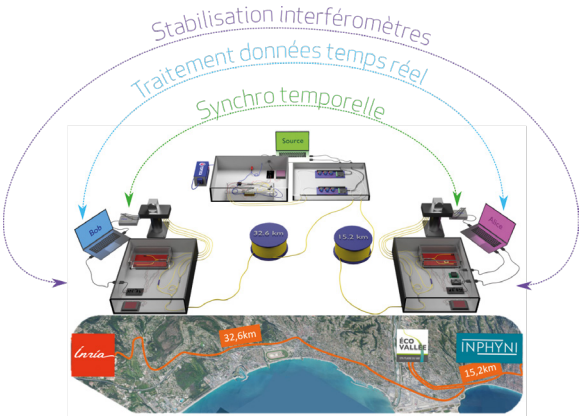
DISTRIBUTION QUANTIQUE DE CLEF SUR RÉSEAU DÉPLOYÉ : ENJEUX ET DÉFIS

Olivier ALIBART*, Virginia D'AURIA, Jean ETESSE, Laurent LABONTÉ, Anthony MARTIN, Yoann PELET, Tess TROISI, Éric PICHOLLE, Grégory SAUDER, Sébastien TANZILLI

Université Côte d'Azur, CNRS, Institut de Physique de Nice, Nice, France
*olivier.alibart@univ-cotedazur.fr



Les technologies quantiques s'aventurent aujourd'hui en dehors des laboratoires. Une équipe chinoise a même déjà distribué des clefs sur plusieurs milliers de km via un satellite. De telles annonces sensationnelles masquent cependant la partie immergée de l'iceberg : la seconde révolution quantique est constituée d'une multitude d'avancées scientifiques et technologiques très diverses, que nous souhaitons illustrer ici par la démonstration réalisée par l'équipe azuréenne : distribution quantique de clef sur 50 km basée sur l'intrication.

https://doi.org/10.1051/photon/202513035

CONTEXTE

Il aura fallu un peu moins d'un siècle pour passer de la "physique quantique" des pionniers aux "technologies quantiques". Ce changement de terminologie est lourd de sens. La première révolution quantique visait à comprendre le monde, et le rôle de l'observateur. Avec la seconde, l'heure est à la manipulation active des ressources pour concevoir des états quantiques spécifiques et développer de nouveaux dispositifs.

C'est dans ce cadre que se situe la preuve de principe de QKD sur 50 km réalisée par l'Institut de physique de Nice en collaboration avec Orange [1]. Si la distribution de l'intrication est désormais monnaie courante dans les salles d'expérimentation des laboratoires, il s'agit bel et bien ici de la distribuer entre deux sites distants de 50 km, *via* le réseau de fibres optiques d'un opérateur commercial, et de transformer ces corrélations quantiques en deux séries aléatoires de bits (0 et 1) parfaitement corrélées entre elles pour permettre à deux acteurs (Alice et Bob) de réaliser des échanges de données sécurisés par les lois de la physique quantique.

Nous renvoyons le lecteur aux articles de Sara Ducci et Nicolas Sangouard pour le détail de l'utilisation de l'intrication comme ressource pour la distribution quantique de clefs ; dans cet article, nous tâcherons de nous concentrer sur les enjeux et les défis à surmonter pour sortir du laboratoire et offrir un système opérationnel d'établissement de clefs secrètes à distance. Par ailleurs, de petits encarts évoqueront succinctement les enjeux et les défis liés au déploiement selon le ●●●

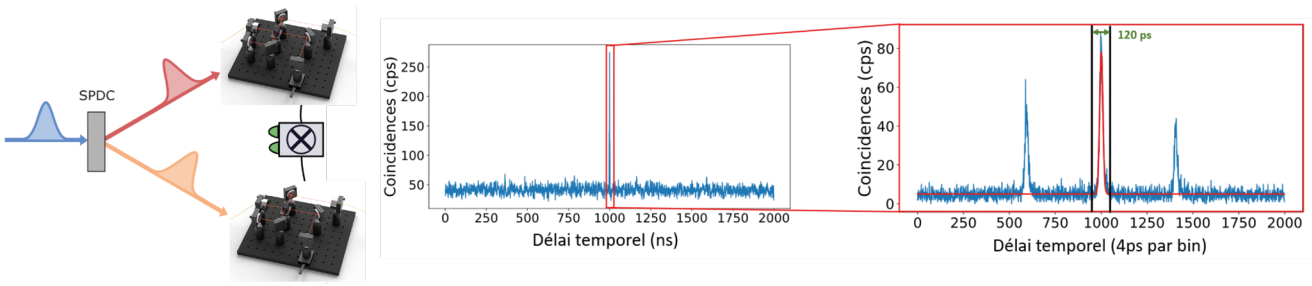


Figure 1. Principe d'une expérience de mesure de corrélations énergie-temps portées par des paires de photons intriqués. La réalisation sur table optique offre une souplesse permettant d'exploiter au mieux les composants d'optique traditionnelle et de mesurer les corrélations temporelles à l'aide d'un unique dispositif de datation. Les données recueillies donnent un histogramme des coïncidences duquel l'utilisateur reconstruit les statistiques permettant d'observer des corrélations quantiques. L'utilisation d'une paire d'interféromètres dit de "Franson" très fortement déséquilibrés (~50 cm), donne naissance à trois pics de coïncidences, parmi lesquels seul le pic central porte la signature de l'intrication. Il faut donc définir une fenêtre temporelle d'analyse des coïncidences d'une centaine de picosecondes qui établit la précision attendue pour la synchronisation des utilisateurs.

point de vue des autres composantes des technologies quantiques, comme la métrologie, les mémoires et les futurs protocoles de communication quantique émergeants mais aussi les questions humaines et sociales que le domaine peut susciter.

ENJEUX ET DÉFIS EN DEHORS DU LABORATOIRE

Une expérience d'optique quantique, c'est d'abord une bonne dose d'optique non-linéaire pour la génération de paires de photons intriqués et beaucoup d'interférométrie pour les manipuler, et analyser correctement les observables choisies (polarisation, énergie, temps d'émission, mode spatial…). Nos laboratoires sont autant de bulles privilégiées, à l'abri desquelles de nouveaux protocoles dont sont issus la distribution quantique de clefs, la téléportation quantique d'état, etc., ont pu émerger depuis une trentaine d'années. Toutefois, ces protocoles n'ont pas vocation à y rester confinés. Les chercheurs et les chercheuses ont également pour mission d'assurer le transfert technologique vers le monde réel. Pour cela, les dispositifs quantiques doivent aussi devenir compacts, résistants aux perturbations extérieures (vibration, humidité, température…), énergétiquement sobres, résilients, c'est-à-dire capables d'autodiagnostiquer les défaillances et de redémarrer seuls. Sacré cahier des charges ! S'y ajoutent d'autres contraintes fortes comme la gestion des flux d'information enregistrés et traités quasiment en temps réel ou les besoins de synchronisation et de stabilisation entre les dispositifs de mesure.

Prenons l'exemple d'une expérience de mesure d'intrication en énergie-temps. Sur table optique, il faut réunir un laser de pompe d'une grande longueur de cohérence, un cristal non linéaire et des analyseurs capables de mesurer les temps d'arrivée ou l'énergie de chaque photon de la paire. En pratique, les corrélations temporelles sont mesurées à l'aide d'un dispositif de datation (time-digital-converter) de haute

LE REGARD DE LA CRYPTANALYSE PAR ANTHONY MARTIN

La cryptanalyse est une part importante du développement des protocoles de distribution quantique de clefs de chiffrement. En pratique, les cryptanalystes vont décortiquer et étudier l'implémentation des systèmes d'échange de clefs quantiques afin de trouver des failles de sécurité en exploitant des imperfections de certains éléments des dispositifs, mais aussi à des manipulations malveillantes par le fournisseur d'équipement lui-même qui peut introduire des "portes dérobées". À titre d'exemple les protocoles BB84 ou BB92 sont qualifiés de sûrs selon certaines hypothèses qui portent notamment sur le principe de fonctionnement des équipements utilisés.

Une voie explorée par les scientifiques vise le développement de nouveaux protocoles dont la sécurité est indépendante des dispositifs (DIQKD), c'est à dire qu'elle ne nécessite aucune confiance dans les appareils utilisés. Le principe de la DIQKD repose sur des tests de non-localité quantique, tels que les inégalités de Bell, pour assurer la sécurité. En utilisant des corrélations quantiques qui ne peuvent pas être expliquées par des modèles locaux et déterministes, la DIQKD permet de détecter toute tentative d'espionnage ou de manipulation par un tiers. Ainsi, la sécurité de la clef générée dépend uniquement des lois fondamentales de la mécanique quantique.

La DIQKD offre ainsi une robustesse accrue face à des attaques sophistiquées et est considérée comme un pas important vers des communications quantiques ultra-sécurisées. Cependant, sa mise en œuvre hors des laboratoires pose encore des défis techniques importants, notamment en termes de taux de génération de clés et de tolérance aux pertes.

précision qui exploite une horloge ultraprécise (de l'ordre de la picoseconde) pour attribuer à chaque détection des étiquettes temporelles qui servent à identifier les corrélations en post-traitement (voir l'article photoniques [2]). Cette précision est couramment atteinte en laboratoire avec de simples horloges à base d'oscillateurs à quartz dont la stabilité de fréquence centrale est de l'ordre de 10^{-9} Hz. La même horloge étant utilisée pour dater tous les évènements, sa stabilité importe peu puisque les corrélations font intervenir les intervalles de temps relatifs entre des évènements quasi simultanés. Le problème est bien différent dès lors que l'on sort du laboratoire : chaque site de réception dispose de sa propre échelle de temps, dont la synchronisation relative, pourtant essentielle, n'est pas garantie au-delà de quelques secondes. Les opérateurs mobiles offrent le même genre de service à nos portables, ou les satellites à nos GPS, mais avec des précisions bien en-deçà des attendus pour les protocoles de communication quantique. Cet aspect technologique est un axe de recherche important du réseau de recherche en métrologie du temps FIRST-TF [3].

LE REGARD DE LA MÉTROLOGIE PAR LAURENT LABONTÉ

Les réseaux quantiques offrent une opportunité unique pour la métrologie quantique, permettant des avancées inaccessibles aux approches classiques ou aux états quantiques isolés. En reliant des capteurs distribués sur un territoire à l'aide d'états intriqués au sein d'un réseau quantique, il devient possible de mesurer des paramètres globaux avec une précision surpassant celle obtenue par des capteurs indépendants. Ce principe repose sur l'exploitation des corrélations quantiques établies entre les capteurs, autorisant une estimation collective plus performante.
Par exemple, un réseau de gravimètres quantiques ou de capteurs optiques intriqués pourrait détecter des variations infimes de gravité ou d'activités sismiques sur de vastes régions, permettant d'envisager l'anticipation des catastrophes naturelles en géophysique ou de meilleures performances en navigation inertielle. De même, la synchronisation d'horloges atomiques réparties sur un réseau pourrait révolutionner les systèmes GPS et les communications, en offrant une précision sans précédent [4]

En ce qui concerne les corrélations en énergie, on mesure la somme des énergies de chaque photon de la paire *via* une paire d'interféromètres fortement déséquilibrés mais identiques. Il s'agit alors de stabiliser les interféromètres l'un par rapport à l'autre. En laboratoire, à l'abri de toutes perturbations, il est assez facile d'obtenir deux interféromètres avec une stabilité relative meilleure que $\lambda/100$ sur quelques heures. Mais dès lors que les interféromètres sont placés dans deux laboratoires différents, cette stabilité relative devient un casse-tête… On entre alors sur les platebandes du projet REFIMEVE qui s'attache d'assurer le transfert d'une fréquence optique ultra-stable sur longue distance.

Le dernier point à mettre en avant est le flux de données échangées au cours d'une expérience de distribution quantique de clef. ● ● ●

Figure 2. Plan du réseau Quantum@UniCA. Il s'étend sur une centaine de kilomètres avec 4 nœuds offrant tout l'équipement nécessaire pour produire et détecter des photons intriqués mais aussi analyser les corrélations temporelles inter-nœuds.

Un calcul rapide montre qu'une dizaine de millions de détections de photons dont l'heure d'arrivée (à la picoseconde près) et le numéro d'identification codés sur 64 bits requiert un débit d'information d'environ 640Mbit/s, facilement assuré par une connexion USB3 courte distance mais moins trivialement assuré *via* une connexion ethernet sur des kilomètres. Si par ailleurs le traitement des clefs se fait à la volée, il faut donc y ajouter les étapes classiques de réconciliation, d'estimation et de correction des erreurs qui sont très gourmandes en données.

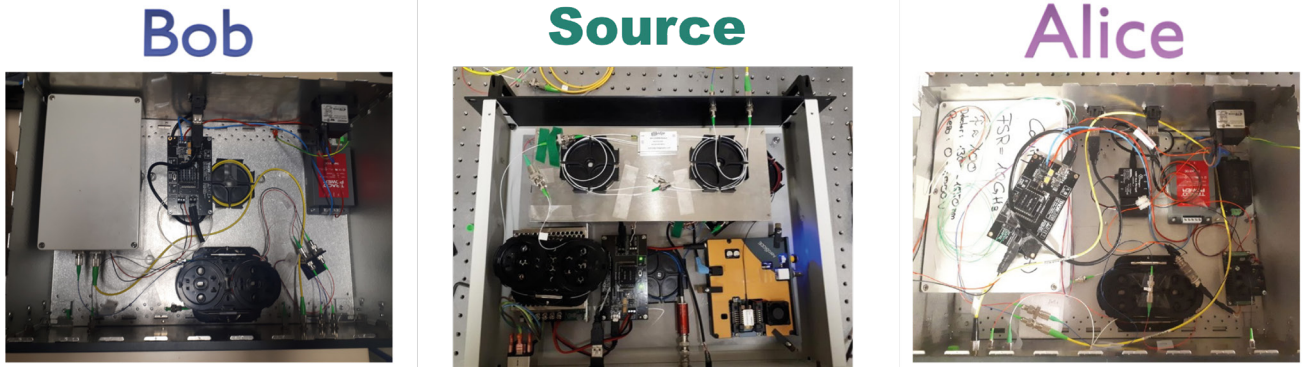
LE RÉSEAU QUANTUM@UNICA

Il s'agit d'un réseau de fibres optiques dédié aux expériences de communication quantique. Ces fibres évitent donc soigneusement tout appareillage télécom (switch, amplificateur...) et ne transportent aucun autre type de signal optique que des états quantiques. C'est un véritable banc d'essai fourni par Orange aux chercheurs d'INPHYNI qui relie les sites d'Université Côte d'Azur (campus Valrose à Nice centre, campus Plaine du Var à Nice ouest), le centre INRIA à Sophia-Antipolis et enfin le laboratoire GéoAzur de l'observatoire de la Côte d'Azur à Caussol (voir figure 2). En pratique, il est constitué d'une centaine de brins de fibre optique standard aboutés les uns aux autres pour obtenir un unique lien de 100 km présentant des pertes totales de 35 dB, c'est-à-dire à l'état de l'art mondial. Trois des quatre nœuds sont équipés de détecteurs de photons, d'un système de datation temporelle et des moyens de communication très haut débit. Les sites de l'éco-vallée et de l'INRIA sont de simples salles serveur, tandis que les sites de Nice-centre et de GéoAzur sont de véritables laboratoires. En outre, le nœud de Caussol est connecté au télescope d'observation astronomique pour préparer les futurs liens spatiaux par satellite.

PRÉPARATION DE DISPOSITIFS QUANTIQUES POUR UNE UTILISATION HORS LABORATOIRE

La première contrainte rencontrée est le standard d'intégration des équipements électroniques qui impose l'utilisation de boîtes de dimension 425 × 245 mm, et de composants à fibre optique pour la miniaturisation, ainsi que la gestion des flux thermiques afin de garantir la stabilité des interféromètres. Il faut également garder à l'esprit que ces boîtes sont difficiles d'accès en temps réel pour assurer leur réglage et leur diagnostic. Tous les paramètres

Figure 3. Travail d'intégration sur la source et les analyseurs de corrélation énergie-temps. La boîte "source" contient un laser à 780 nm, un guide d'onde non linéaire et des composants de routage/filtrage. Les boîtes "Alice" et "Bob" contiennent des interféromètres à base de fibre optique nichés dans des boitiers thermiquement stabilisés. La partie électronique, pilotable à distance, qui gère la stabilisation en température, la puissance du laser et la phase des interféromètres est commune aux trois boîtes. Crédit image Y. Pelet (INPHYNI/CNRS).



LE REGARD DES MÉMOIRES PAR JEAN ETESSE

Les distances sur lesquelles il est possible de réaliser des protocoles de communication quantique sont limitées, et pour repousser celles-ci les liens peuvent être fractionnés en liens élémentaires plus courts. C'est le principe des 'répéteurs quantiques', nécessitant une capacité de synchronisation. Les mémoires quantiques, dispositifs capables de stocker et de réémettre les excitations photoniques à la demande, lèvent ce verrou et des preuves de concept voient actuellement le jour dans les réseaux quantiques.
Les mémoires quantiques photoniques à l'état de l'art sont actuellement développées dans les cristaux dopés avec des ions de terres rares d'une part et avec des atomes alcalins refroidis d'autre part, permettant, selon la technologie, d'atteindre des temps de stockage de plusieurs heures ou des efficacités de stockage de plus de 90%. L'enjeu actuel de ces technologies est de concentrer sur une plateforme unique les performances requises pour un développement à grande échelle [5].

(puissance du laser, polarisation de sortie, phase des interféromètres, température…) doivent donc être pilotables à distance *via* un ordinateur connecté à internet.

LA SYNCHRONISATION DES UTILISATEURS

Il ne s'agit pas à proprement parler de synchronisation mais de syntonisation des deux horloges : celles-ci n'affichent pas forcément la même heure mais la durée d'une seconde doit être la même. Il est toutefois impossible que cette durée soit rigoureusement identique entre les horloges, et nous devons donc nous demander : quel écart-type est acceptable pour notre expérience ? Et par conséquent, quel est le temps caractéristique de rétroaction nécessaire ? L'écart-type acceptable est défini par la largeur de la fenêtre d'analyse des coïncidences (voir figure 1) qui est de l'ordre d'une centaine de picosecondes. Puisqu'il n'est pas suffisant de faire appel aux signaux GPS dont la précision est de l'ordre de la nanoseconde, nous avons choisi d'utiliser des horloges rubidium locales. La stabilité de ces dernières, de l'ordre d'une dizaine de picosecondes par seconde, permet un asservissement à l'échelle de la seconde. Cela permet d'exploiter directement les corrélations quantiques pour mesurer le glissement des horloges et effectuer la correction nécessaire sur l'une des deux horloges. Ce choix impose des contraintes fortes sur la partie optique et sur le traitement des données. Il faut en effet disposer de suffisamment d'échantillons de détection et d'un ordinateur suffisamment puissant pour calculer une fonction de corrélation significative, le tout en moins d'une seconde ! Les pertes à la propagation qui limitent le taux de détection, représentent le principal facteur limitant la distance maximale atteignable du réseau azuréen.

LA STABILISATION DES INTERFÉROMÈTRES

Les interféromètres (de type Mach-Zehnder) fortement déséquilibrés, formant un interféromètre dit de « Franson », agissent comme des « analyseurs en énergie » pour chaque paire de photons. L'intrication se cache dans la dépendance des corrélations à la somme des phases respectives de chaque interféromètre. Il s'agit donc d'asservir la phase d'un interféromètre sur l'autre pour que la somme des déséquilibres soit en permanence un multiple de 2π. Là encore, nous avons choisi d'optimiser la stabilisation passive des interféromètres (vibration, température, humidité…) afin de limiter le décalage en phase de quelques π par jours et de directement exploiter les corrélations quantiques pour mesurer le glissement des phases. C'est la mesure des corrélations en énergie qui est • • •

LE REGARD DES VARIABLES CONTINUES PAR VIRGINIA D'AURIA

L'encodage de bits d'information quantique sur les photons uniques n'est pas le seul possible. Il est également possible d'exploiter les aspects de la lumière davantage liés à sa nature ondulatoire (encodage à variables continues) et ainsi d'hybrider les deux types d'encodage. Ce dernier type d'approche se base sur la manipulation d'états de la lumière grâce à l'association des détecteurs capables de compter des photons et d'interféromètres homodyne optiques, proches de ceux utilisés, par exemple, dans les radios du passé.
Cette technique permet d'obtenir des états de la lumière hautement non-classiques, tels que des chatons de Schrödinger, ainsi que des états intriqués dit « hybrides », qui donnent la possibilité de tirer profit des deux types d'encodage. Les états hybrides optiques sont étudiés, entre autres, pour la préparation à distance d'états quantiques, ainsi que comme des ressources prometteuses permettant de réduire l'impact des pertes à la propagation dans les protocoles de téléportation et, plus en général, d'interfacer des technologies quantiques différentes situées aux nœuds d'un réseau quantique [6].

LE QUANTIQUE AU CRIBLE DES SCIENCES HUMAINES ET SOCIALES PAR ERIC PICHOLLE

Les défis posés aux sciences humaines et sociales sont multiples, de la caractérisation d'un changement de paradigme au moment même où il s'opère aux problèmes méthodologiques inédits qu'il suscitera inévitablement.
Une technologie qui sort de sa "bulle" académique se trouve rapidement confrontée à de nouvelles contraintes. Techniques, on l'a vu, mais aussi humaines et sociales. Économiques, bien sûr : le Plan Quantique National dit assez le sérieux des enjeux de la seconde révolution quantique. Mais aussi éducatives et didactiques (Comment former au quantique ses futurs techniciens de terrain ? Peut-on en parler dès le lycée ? Voire le collège ?) ; juridiques (Qui est responsable d'une information encore indéterminée ? Pour anticiper les risques de technologies encore largement spéculatives, comme l'ordinateur quantique, vaut-il mieux un droit "dur", des normes explicites — mais lesquelles ? —, ou un droit "souple", avec des règles procédurales adaptatives à définir par les entreprises elles-mêmes ?) ; le modèle de développement de pépites quantiques à la française est-il comparable, en termes d'anthropologie d'entreprise, à celui des start-up de la Silicon Valley d'hier, ou même des jeunes pousses de l'IA ?

utilisée pour calculer le signal de rétroaction à appliquer sur un des deux interféromètres imposant par conséquent les mêmes contraintes sur le traitement des données que pour la synchronisation.

LES DÉFIS LIÉS AU POST-TRAITEMENT TEMPS RÉEL

Un protocole de QKD ne se réduit pas à l'échange entre Alice et Bob des temps associés aux photons détectés, qui représentent déjà plusieurs centaines de Mbits par seconde. Si l'objectif est d'établir des clefs entre sites distants en temps réel, il s'agit de traiter simultanément la réconciliation des bases de mesures, d'effectuer la correction des erreurs éventuelles et enfin d'effectuer l'amplification de la sécurité (voir article de N. Sangouard). Du fait de ces processus itératifs, la bande passante effectivement requise est, pour ce réseau, d'environ 1 Gbit/s. Au moindre ralentissement, c'est toute la chaîne de traitement de données qui s'effondre et le protocole qui s'arrête. Il faut donc s'assurer d'une connexion optique très haut débit de bout en bout.

LA RÉSILIENCE PAR L'AUTOMATISATION

Un des aspects novateurs de l'expérience azuréenne réside dans son autonomie. La liste des erreurs qui interrompent le protocole de QKD est en effet assez longue : le taux d'erreur (QBER) au-delà de 11%, perte de la synchronisation ou de l'asservissement des interféromètres, arrêt momentané des détecteurs… Un important travail de programmation sous LabVIEW a été mis en place pour assurer la détection et le diagnostic des erreurs, ainsi que le redémarrage de l'ensemble du protocole de QKD le cas échéant. Nous avons ainsi pu maintenir un échange de clefs pendant plus de 300 h sans intervention humaine [1].

CONCLUSION

Le tour de force de l'expérience de QKD azuréenne va bien au-delà de l'exploitation des idées issues de la physique quantique : c'est tout un ensemble de technologies habilitantes, "classiques" pour la plupart, qui permettent aux technologies quantiques de sortir du laboratoire. Sans les développements expérimentaux sur le partage de référence de fréquence ou de référence de temps, il eût été impossible d'imaginer un lien de communication quantique déployé sur quelques dizaines kilomètres. Les liaisons haut-débit au sol sont désormais largement disponibles, mais d'importants efforts sont maintenant attendus par tous les acteurs (académiques comme industriels) pour partir à la conquête de l'espace et de ses satellites, pour lesquels toutes ces questions de synchronisation, de stabilisation et de flux de données se compliquent encore en raison de l'effet doppler et des corrections relativistes qui ne sont plus alors négligeables. C'est cette quête du dépassement qui réunit les chercheurs, les ingénieurs, les techniciens de l'optique, de l'électronique et du spatial autour des technologies quantiques.

RÉFÉRENCES

[1] Y. Pelet, G. Sauder, M. Cohen, L. Labonté, O. Alibart, A. Martin, S. Tanzilli, Phys. Rev. Applied **20**, 044006 (2023)

[2] O. Alibart, V. D'Auria, G. Sauder, L. Labonte, S. Tanzilli, Photoniques **91**, 38 (2018)

[3] https://first-tf.fr/

[4] Liu, Li-Zheng *et al,* Nature Photonics **15**, 137 (2021)

[5] D. Lago-Riviera *et al.*, Nat. Comun. **14**, 1889 (2023)

[6] . G. Guccione *et al.*, Sci. Adv. 6, eaba4508 (2020).