ÉLÉMENT DE PORTFOLIO 03

Jeu de données consolidées

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : The Quantum Protocol Zoo

URL de l'élément : `https://wiki.veriqloud.fr`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Ce dépôt ouvert de protocoles sur réseau, sous la forme d'un site web, démarré en 2018 et toujours actif, est emblématique de la volonté de l'équipe d'accompagner la recherche au delà de la simple publication académique, en analysant les protocoles de communication quantique —une cinquantaine de protocoles et une vingtaine de fonctionalités— publiés, et en le présentant sous une forme normalisée et modulaire, afin de faciliter son analyse (preuves de sécurité, cas d'usage), l'évaluation des ressources nécéssaires à son implémentation afin d'être utile à diverses communautés — cryptographes, concepteurs de protocoles, développeurs de réseaux, développeurs de codes et expérimentateurs — dans les mondes académique et industriels.

Cet élément est aussi emblématique d'autres traits caractéristiques de l'équipe :

- une recherche importante sur les réseaux quantiques sous toutes leurs formes
- collaboration étroite avec l'industrie — en l'occurrence la start-up VeriQloud, issue des recherches de l'équipe
- collaboration très intégrée avec Édimbourg : au delà d'Elham Kashefi qui émarge, à la fois au LIP6 et à Edimbourg, le LIP6 y a participé avec un développeur web (Cyril Castagnet), 4 stagiaires (Natansh Mathur, Rhea Parekh, Gözde Üstün, Shraddah Singh), un postdoc (Harold Ollivier) et Édimbourg avec une doctorante (Mina Doosti) et trois postdoctorants (Mashid Delavar, Atul Mantri et Niraj Kumar)
- plus généralement, il est au cœur des collaborations internationales de l'équipe, par le biais des contrats ANR internationale VanQuTe et des contrats européens liés à la Quantum Internet Alliance (QIA) — il fait d'ailleurs partie des quatre ressources mises en avant par QIA sur `https://quantum-internet.team/resources/`
- Il participe des action de vulgarisations scienctifique de l'équipe : il a été utilisé par un public non-spécialiste dans le premier *Pan-European Hackathon*, co-organisé par l'équipe en novembre 2019, démontrant son utilité.

3 PRÉSENTATION DE CET ÉLÉMENT

Le *Quantum Protocol Zoo* est un référentiel ouvert de protocoles pour les réseaux quantiques. Il offre un moyen compact et canonique d'explorer ces protocoles. En outre, il facilite la communication entre informaticiens, ingénieurs et physiciens sur une plateforme unique.

Après avoir collecté 78 protocoles dans la littérature, ils ont été soigneusement étudiés, notamment en leur fonctionnalité en les regardant les éléments d'un système modulaire d'application. Leur sécurité, efficacité et les ressources matérielles nécessaires sont aussi déterminées. Les protocoles sont décrits sous une forme textuelle normalisée, qui permet une compréhension simple du proctocole, mais facilite aussi son anayse par des outils informatiques.

Ainsi, une analyse en terme de graphe de connaissance a permis de développer un nouveau concept de visualisation des ressources pour les protocoles quantiques, qui comprend deux interfaces : l'une pour identifier les exigences de mise en œuvre d'un protocole donné (voir Fig. 1), et l'autre pour identifier les protocoles accessibles lorsque certaines ressources physiques ou fonctionnalités sont disponibles.

Ce cadre est utile pour analyser la sécurité des protocoles, concevoir et optimiser des protocoles complexes, concevoir l'architecture du réseau et mettre en œuvre les protocoles à la fois dans le logiciel et le matériel, respectivement.

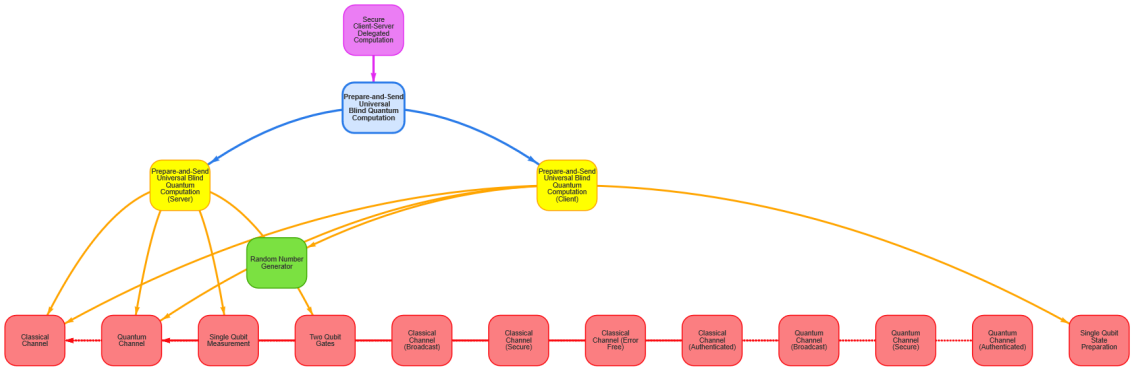

FIGURE 1 – Exemple de l'inteface graphique identifiant les resources nécessaires à la mise en œuvre d'un protocole, en l'occurrence, un protocol de calcul quantique universel aveugle