Shared photonic laboratory for research on quantum security and beyond

Nella WAWRYNIUK
Kozminski University, Jagiellonska St., Warsaw, Poland

Why quantum computing?
It is an emerging technology, gaining a lot of attention from experts from different fields across the world. Although quantum computers are not expected to make the classical ones obsolete, they will definitely be a game-changer. For now they are nearly a very sophisticated tool for specific and quite advanced problems, but the expected future impact is obviously enormous. It will most likely be used mostly in industries which are requiring this huge computing power to work with big databases and improve their production processes. It will definitely be visible and play the leading role in the development of medicine, automotive industry, machine learning, finance and cybersecurity, with the possibility of being a disruptive technology.

But where exactly is it useful?
It is absolutely great for simulations. Thanks to quantum computing pharmaceutical companies and researchers will have the possibility to work with very complicated processes, which were not possible to simulate on classical computers. It can lead to groundbreaking progress in this area, such as discovering new molecules. The development in the automotive industry and machine learning is quite self-explanatory. The shortage of time needed for running operations in these fields will have enormous impact on advancements within them. The most intriguing solution are connected with so called Distributed Quantum Computation (DQC), e.g. Anshu et al. [1], Cicconetti et al. in [2], or Cuomo et al. [3]. In terms of cybersecurity, can it be considered as a security threat? Well, most encryptions both private and governmental rely on quite complicated mathematic resolutions, which are simply too complex to solve for classical computers (and people for that matter). Not anymore! Quantum computers will have the ability to solve those calculations in just seconds. Scared yet? Well, we have a little bit time, since now we are in the post-quantum era indeed. However, the quantum computers, despite of rapid grows of qubit number, are still in the so called NISQ (Noisy, intermediate scale Quantum computing). The main problem is not to produce more and more qubits but the noise caused by many factors including *decoherence*. This results in fidelities of quantum gates on the level of 0.97-0.99. It seems to be high, however if we consider 100 such gates applied one by one, we'll see that the whole fidelity falls to the level of 0.366, which makes the computation impossible. The specialists claims that this era will end in the perspective of 10-15 years, and we'll step in in so called *beyond NISQ* era, which is not really defined yet. Nevertheless the preparation for this era is in progress and many researchers works on the post-quantum algorithms for cyber security – see Qui et al. [4], or Oliveira et al. [5].
The OptiQ project, in a long term, will bring new products and services to the market in the form of application of quantum security, it will increase the security of communication services offered by Envelo (it might be the first commercial application of quantum technologies on European market!). It will most likely become crucial in banking and financial sector.

What are we focusing on?
The main goal is influencing and spurring the technological development and innovation, not only in Europe, but across the world. We want to make an impact, both short-term and long term, especially on image and video representation in quantum optical circuit (transmitting huge videos with the tiny number of qubits required would be groundbreaking in space imaging, creation of optical sensors and medicine image diagnostics), and optimization of complex chemical processes by quantum algorithms (improving the branch of industrial processes investigation and simulation).
In the area of quantum processing on NISQ computers, the proposed project will contribute to scientific advances across the quantum computation and computer vision by creating new branch of quantum methods for image and video processing basing on the research of our Partner – Silesian University of Technology ([6]–[8]). Those methods will be characterized by three advantageous properties: (1) they will not have classical part (non-hybrid), (2) they will not be merely

implementations of classical methods, and (3) they will be founded on quantum sampling-based computation. Therefore, this approach by utilizing the most of the quantum nature of quantum computers (i.e. both, the model and generation of the results), gives the scientific advantage as compared to hybrid or classically inspired methods. Hence, we can expect that such methods will outperform hybrid models (where a part of computations is done on a classical computer) or models inspired by classical methods (e.g., CNN) and mapped to the quantum computer (which is not always possible or efficient and needs additional assumptions, often times).
The quantum image representation in quantum optical circuit will give a scientific advantage in the area of optical processing of the image. Currently, in this field we can extract features and proceed it on classical computers, which in the era of CNN is disputable, since the input to those networks are raw images rather than features. The idea to process those features on optical computers (non-quantum) hasn't become widespread. However, in the light of recent study on quantum holography (ibidem, [8]), the quantum image representation within its further processing in photonic circuits become an interesting subject for further interdisciplinary studies intersecting the physics, computer science and electronic disciplines. Such approach opens possibility to generate fully optical (photonics) and quantum methods of image and video processing and classification, applicable in such devices like cameras, microscopes, medical imaging devices, etc. In the future, it can be alternative or collaboration units for silicon computation units used nowadays, introducing quantum technology to the practical devices directly. Moreover, such processing doesn't need the phase of classical – quantum data transfer, which nowadays is a bottleneck.

Conclusions

Our involvement in OptiQ project will allow us to build a laboratory shared with two other project participants: Silesian University of Technology and Boson Energy. It will allow to conduct research in the area of quantum computation, especially on quantum image processing, on quantum simulation for our Partners. For us the most important are possible research in the area of post-quantum security and in quantum security. At the end – we wish to invite all of you to cooperation.

References

[1] A. Anshu, Z. Landau, i Y. Liu, „Distributed Quantum inner product estimation", w *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Rome Italy: ACM, cze. 2022, s. 44–51. doi: 10.1145/3519935.3519974.

[2] C. Cicconetti, M. Conti, i A. Passarella, „Resource Allocation in Quantum Networks for Distributed Quantum Computing", w *2022 IEEE International Conference on Smart Computing (SMARTCOMP)*, Helsinki, Finland: IEEE, cze. 2022, s. 124–132. doi: 10.1109/SMARTCOMP55677.2022.00032.

[3] D. Cuomo, M. Caleffi, i A. S. Cacciapuoti, „Towards a distributed quantum computing ecosystem", *IET Quantum Commun.*, t. 1, nr 1, s. 3–8, 2020, doi: 10.1049/iet-qtc.2020.0002.

[4] F. Qi *i in.*, „Quantum Vulnerability Analysis to Accurate Estimate the Quantum Algorithm Success Rate". arXiv, 28 lipiec 2022. doi: 10.48550/arXiv.2207.14446.

[5] D. Oliveira, E. Giusto, B. Baheri, Q. Guan, B. Montrucchio, i P. Rech, „A Systematic Methodology to Compute the Quantum Vulnerability Factors for Quantum Circuits". arXiv, 13 listopad 2021. doi: 10.48550/arXiv.2111.07085.

[6] K. Wereszczyński, A. Michalczuk, D. Pęszor, M. Paszkuta, K. Cyran, i A. Polański, „Cosine series quantum sampling method with applications in signal and image processing", *ArXiv201112738 Quant-Ph*, lis. 2020, Dostęp: 5 grudzień 2020. [Online]. Dostępne na: http://arxiv.org/abs/2011.12738

[7] K. Wereszczyński, A. Michalczuk, M. Paszkuta, i J. Gumiela, „High-Precision Voltage Measurement for Optical Quantum Computation", *Energies*, t. 15, nr 12, s. 4205, cze. 2022, doi: 10.3390/en15124205.

[8] K. Wereszczyński i K. Cyran, „Two-Rail Photonic Qubit Utilizing the Quantum Holographic Imaging Idea", w *Holography - Recent Advances and Applications*, P. J. Rosen, Red., Rijeka: IntechOpen, 2022. doi: 10.5772/intechopen.106889.