AFRL-AFOSR-VA-TR-2024-0050

Practical Quantum Protocols

Gorjan Alagic
MARYLAND UNIV COLLEGE PARK
230 W 41ST STREET FL 7
NEW YORK, NY,
US

11/30/2023
Final Technical Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
20231130	Final	START DATE 20200701	END DATE 20230630

4. TITLE AND SUBTITLE
Practical Quantum Protocols

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
	FA9550-20-1-0108	61102F
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Gorjan Alagic

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MARYLAND UNIV COLLEGE PARK
230 W 41ST STREET FL 7
NEW YORK, NY
US

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR RTB1

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-VA-TR-2024-0050

12. DISTRIBUTION/AVAILABILITY STATEMENT
A Distribution Unlimited: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This is the final report for the AFOSR project ``Practical Quantum Protocols,'' led by PI Alagic and co-PIs Childs and Gorshkov. In the past few years, exciting new theoretical work has resulted in the development of interactive communication protocols taking place between a classical verifier (e.g., an end-user with a laptop) and a quantum prover (e.g., a quantum-capable cloud service), over a classical communication channel (e.g., the Internet.) These protocols have opened up possibilities for completely new functionality, such as verification of quantum-mechanical features and delegation of quantum-computational algorithms. The aim of this three-year project is to improve the state of the art of these protocols, and bring them closer to realistic implementation on near-term and medium-term quantum devices.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	UU	7

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
GRACE METCALFE	(703) 696-9740

Standard Form 298 (Rev.5/2020)
Prescribed by ANSI Std. Z39.18

AFOSR QIS: Practical Quantum Protocols Final Project Report

Gorjan Alagic Andrew Childs Alexey Gorshkov

November 2023

Abstract

This is the final report for the AFOSR project "Practical Quantum Protocols," led by PI Alagic and co-PIs Childs and Gorshkov. In the past few years, exciting new theoretical work has resulted in the development of interactive communication protocols taking place between a classical verifier (e.g., an end-user with a laptop) and a quantum prover (e.g., a quantum-capable cloud service), over a classical communication channel (e.g., the Internet.) These protocols have opened up possibilities for completely new functionality, such as verification of quantum-mechanical features and delegation of quantum-computational algorithms. The aim of this three-year project is to improve the state of the art of these protocols, and bring them closer to realistic implementation on near-term and medium-term quantum devices.

1 A brief project summary

The following is a brief, year-by-year summary of major events in the project.

In the first year, the project ramped up with the addition of several graduate students and the start of regular meetings and research projects. Some results were already achieved in this first year, including a theoretical result regarding so-called "non-interactive" protocols, and a practical result regarding efficient implementation of certain multi-qubit gates which may be applicable to the implementation of the protocols described above.

In the second year, existing research projects continued and new ones were started. One new publication appeared, on the topic of quantum-classical query complexity, addressing an important fundamental question on the power of quantum algorithms when they are forced to interact with certain parties over a classical channel – as is the case in the setting of our project. While some students left the project (e.g., due to graduation), we also hired a new postdoc (Alex Cojocaru) who specializes in multiparty protocols for quantum functionalities over classical channels.

In the third and final year, further progress was made on several research projects, while new ones were also initiated. Some students left the project, and others joined. We also had a new postdoc (Atul Mantri) who specializes in advanced quantum protocols, such as blind quantum computation.

We are very happy to report that both of our postdocs secured faculty positions after working on this project: Alex Cojocaru at the University of Edinburgh and Atul Mantri at Virginia Tech.

2 Logistical and personnel report

At the start of the project, PI Alagic and co-PIs Childs and Gorshkov began with recruiting graduate research assistants for the project. On the theory side, graduate students Shih-Han Hung and Manasi Shingane were hired. Shih-Han already had significant experience working on quantum protocols, while Manasi was starting as a first-year student. Manasi would continue to work on the project for all three years. On the practical side, PI Gorshkov hired Jim Garrison and (part-time) students Ron Belyansky and Oles Shtanko.

In the second year of the project, Shih-Han graduated and Jim Garrison worked briefly on the project before moving on to a position outside UMD. Towards the end of the year, we also hired Alex Cojocaru as a postdoc.

In the third and final year of the project, students Kaiyan Shi (theory) and Adam Ehrenberg and Jacob Bringewatt (theory-experiment interface) joined the project. We also hired Atul Mantri as a postdoc.

3 Publications and preprints under review

We have the following publications and preprints to report.

1. Non-interactive verification of quantum computations. The first publication is a collaboration between PI Alagic, co-PI Childs, student Shih-Han Hung (project-funded) and external researcher Alex Grilo [ACGH20]. In this work, we develop the first so-called "non-interactive" proofs of quantumness and delegated quantum computation protocols. The basis of this work are the well-known protocols by Mahadev and coauthors [Mah18, BCM+18] for "proofs of quantumness" (or PoQ) and verifying quantum computations.

In the case of PoQ, the goal is simply for a classical verifier V (e.g., an end-user with a laptop) to classically communicate (e.g., via e-mail) with another party P who claims to have a quantum computer, and thereby verify the claim. The most common way to do this at present is for P to perform a quantum supremacy experiment, and then send their data to V for verification. Unfortunately, verification of supremacy data is very difficult, and it is not possible to mathematically prove that some collection of measurement outcomes of P demonstrates that a supremacy experiment was indeed performed. By contrast, a PoQ allows for such a proof, and using very efficient computations on the part of V. This allows for greater confidence, and for handling larger quantum devices. In the aforementioned work, we showed that such PoQ can be performed using only *two messages*: a single challenge sent from V to P, followed by a proof sent from P to V. Previous protocols required many rounds of repetition.

Moreover, we also established that this "minimal interactivity" can be achieved for more advanced protocols, such as those where the goal of V is to actually delegate a useful (in fact, arbitrary) quantum computation to P. Our main techniques consist of removing the instance-dependent initial setup rounds, then applying parallel repetition. Parallel repetition theorems are typically quite difficult to prove, but we were able to establish that this form of repetition is indeed possible in this case. This work was published in TCC, a premier conference for cryptographic protocols [ACGH20]

2. Fast unbounded quantum fanout gates. The second publication is a collaboration between co-PIs Childs and Gorshkov and several local collaborators [GDC+21]. The standard circuit descriptions for the quantum protocols described above, like typical quantum algorithms, presume the ability to directly perform gates between arbitrary pairs of qubits. This is unlikely to be practical for large-scale experiments, and alternative gates are desirable for near-term implementations. Power-law interactions with strength decaying as $1/r^\alpha$ in the distance r, for

instance, provide an experimentally realizable resource for information processing, whilst still retaining long-range connectivity. In this work, we leveraged the power of these interactions to implement a fast quantum fanout gate with an arbitrary number of targets. These types of gates are potentially quite useful in simplifying the circuits involved in quantum protocols, which typically involve computing some function into a register B, controlled on the contents of a different register A.

Our implementation also allows the quantum Fourier transform (QFT) and Shor's algorithm to be performed on a D-dimensional lattice in time logarithmic in the number of qubits for interactions with $\alpha \leq D$. As a corollary, we show that power-law systems with $\alpha \leq D$ are difficult to simulate classically even for short times, under a standard assumption that factoring is classically intractable. Complementarily, we develop a new technique to give a general lower bound, linear in the size of the system, on the time required to implement the QFT and the fanout gate in systems that are constrained by a linear light cone. This allows us to prove an asymptotically tighter lower bound for long-range systems than is possible with previously available techniques.

3. Query complexity with mixed classical-quantum oracles. This publication is a collaboration between PI Alagic and UMD collaborators Chen Bai and Jonathan Katz, and Danish collaborator Christian Majenz [ABKM22].

One of the goals of this project is to understand how quantum cryptographic protocols are affected by certain communication channels are restricted to only carrying classical states. An interesting setting where this takes place is in quantum attacks on cryptography: if a quantum adversary wants to attack a party who uses a classical computation device, then it can only communicate with that device over a classical channel. At the same time, such an adversary may also have a quantum channel to other components of the cryptosystem. A particular example is when the cryptosystem uses a public hash function; in that case, the adversary can easily make *quantum queries* to that function.

The appropriate model for such an adversary is then a quantum algorithm with two oracles: one which only accepts classical inputs (and produces only classical outputs), and another which can be queried using arbitrary quantum states. Surprisingly, such a model had not been considered before by query complexity. In this work, we explore this model and give the first lower bounds. We demonstrate that this model is indeed relevant and interesting by applying our lower bounds to give the first proof of security (against quantum adversaries) for an important cryptosystem: the Even-Mansour cipher.

We remark that the Even-Mansour cipher is a fundamental building block in a wide array of symmetric-key cryptosystems in use today. It is also an ingredient in a number of current candidates for standardization for lightweight cryptography for Internet-of-Things devices [TMC+21].

4. Applications of mixed oracles (submitted). This is a collaboration between PI Alagic and UMD collaborators Chen Bai and Jonathan Katz, Danish collaborator Christian Majenz, and German collaborator Patrick Struck [ABK+23].

It is a continuation of the previous project, where we aimed to understand how quantum cryptographic protocols are affected by certain communication channels restricted to only carrying classical states [ABKM22]. Here we were able to apply our techniques to establish proofs of security for various practical schemes against attack by quantum computers. The schemes we proved secure include the MAC Chaskey (an ISO standard), the AEAD scheme Minalpher (a second-round CAESAR candidate), and the AEAD scheme Elephant (a finalist in the NIST lightweight cryptography competition [TMC+21].)

This result shows that our techniques can be applied to real-world protocols. We plan to continue using these techniques and exploring their limits in future work.

5. Hybrid search (submitted). This is a collaboration between postdoc Alex Cojocaru (funded) and collaborators Juan Garay and Fang Song [CGS23].

This project considered a problem closely related to that of the two research projects directly above ([ABKM22] and [ABK+23]). In those projects, the quantum device had access to two *related* oracles: one via a classical channel and the other one via a quantum channel. In the present project, we instead consider the case where the oracles are identical; stated differently, the device now has two *interfaces* to the same function: a classical interface and a quantum interface [CGS23]. Moreover, we assume that the device has a certain budget of queries for each interface. This is realistic, because classical queries are presumably significantly cheaper than quantum ones.

The particular problem we consider is simple: generalized unstructured search. As it turns out, lower bounds in the above hybrid model were not previously known for this generalized problem.

6. Permutation inversion problem (submitted). This is a collaboration between PI Alagic and UMD students Chen Bai and Kaiyan Shi (project-funded), as well as Caltech/MIT collaborator Alex Poremba [ABPS23].

The goal of the project is to establish certain fundamental limits on the computational power of quantum devices. The particular question here is about the tradeoff between the space (e.g., number of qubits) and time (e.g., depth of a circuit of gates) that such a device needs to solve a certain basic problem. In this case, we want to understand computations involving *preprocessing*, where the device is allowed to construct some arbitrarily complex (but size-limited) quantum state, and can then later make use of this state to perform some interesting computation. This "interesting computation" can take many forms, but in this project is the problem of *inverting a permutation*.

In this project, we establish new space-time tradeoffs for the permutation inversion problem, under a natural model motivated by (cryptographic) quantum protocols. In this model, the quantum device gets query access to both the permutation *and its inverse* (where the latter cannot be queried on the challenge input.) In some settings, our tradeoffs can be shown to be optimal. In others, they are suboptimal but are the first known bounds to be proved in this model.

5. Deterministic and verifiable blind quantum computing with trapped ions (experiment, submitted). This experiment is a collaboration between postdoc Atul Mantri (project-funded) and a group of scientists in France and the UK [DNM+23]. The experiment was performed in the group of D. M. Lucas at Oxford.

In this project, we present the first hybrid matter-photon implementation of verifiable blind quantum computing. We use a trapped-ion quantum server and a client-side photonic detection system connected by a fibre-optic quantum network link. The availability of memory qubits and deterministic quantum logic enables interactive protocols without post-selection – a requirement for any scalable blind quantum cloud server which previous realisations could not provide. Our apparatus supports guaranteed privacy with ¡ 0.001 leaked bits per qubit and shows a clear path to fully verified quantum computing in the cloud.

We demonstrate BQC using a trapped-ion quantum processor (server) that integrates a robust memory qubit encoded in 43Ca+ with a single-photon interface based on 88Sr+ to establish a quantum link to the client (photon detection system). We implement an interactive protocol, where the client can remotely prepare singlequbit states on the server adaptively from shot to shot using real-time classical feedforward control. The complexity needed for universal quantum computation is contained entirely within the server, while the client is a simple photon polarisation measurement device that is independent of the size and complexity of the algorithm and supports near-perfect blindness by construction. The client and the server are

controlled by independent hardware and connected only by a classical signalling bus and an optical fibre. The combined system of server and client achieves noise levels below a certain threshold for which arbitrary improvements to the protocol security and success rate (robustness) are theoretically possible.

4 Additional research progress

There are also several ongoing projects with partial progress to report.

Circuit synthesis. Arguably, the quantum protocols closest to practical realization are the so-called "proofs of quantumness." These protocols are in many ways superior to existing verification approaches based on quantum supremacy. Jim Garrison has done significant work on synthesizing concrete quantum circuits for some of these protocols, with particular attention to non-geometrically-local gates and the use of multiple-control multiple-qubit gates. At this time it seems that this work may have also been done in parallel by a group in Berkeley, unfortunately.

Certified randomness. Shih-Han Hung has been thinking about non-interactive certified randomness protocols. Certified randomness is an exciting potential application of quantum computers, potentially even including the case of near-term devices. Typically, certified randomness protocols require (i.) a high degree of interaction between the randomness-generating device and the user, and (ii.) the user being able to exert some control over the spatial position of the devices, e.g., to ensure the devices cannot coordinate via relativistic constraints. Recent work has managed to replace the second requirement with standard computational assumptions like Learning with Errors (LWE) [BCM+18]. However, these protocols still require many rounds of interaction (e.g., polynomial in the number of random bits needed), leading to impractical protocols. Shih-Han is investigating techniques for reducing this interaction and bringing these protocols closer to realistic practice.

Proofs of quantumness via simultaneous hardcore bits. Interactive protocols for demonstrating quantum computational advantage are commonly known as proof-of-quantumness protocols. The security of most existing proof-of-quantumness protocols is based on a cryptographic primitive known as trapdoor claw-free functions. A trapdoor claw-free function is a two-to-one function f that is claw-free, meaning that—unless one has access to a secret (trapdoor)—it is computationally hard to find a claw, i.e. a pair of inputs (x_0, x_1) that map to the same output, i.e., $f(x_0) = f(x_1)$.

In this project, we aim to demonstrate the existence of many simultaneous hardcore bits for a family of trapdoor claw-free functions. This would amount to constructing a function $h(x)$, whose output—the simultaneous hardcore bits—is a bit string of length greater than 1, such that, given x_0 and $f(x_0)$, it is hard to predict $h(x_1)$ better than random guessing.

We are also currently exploring whether these simultaneous hardcore bits can be used to create proof-of-quantumness protocols that are more suitable than existing protocols for implementation on NISQ devices. Here the idea would be that the "quantum-classical" gap would be amplified if multiple hardcore bits could be leveraged, resulting in a lower minimum fidelity requirement for the relevant quantum device.

Encrypted and secure sensing. Suppose that a server has access to a sensor network, where each node in the network is sensing a particular local field, and a user queries the server to learn some function of the fields. Entanglement between the nodes of the network can often be used to reduce the uncertainty in the measurement of field properties. In this project, we

are exploring whether ideas such as the Mahadev-type protocols (which we work on in our proof-of-quantumness project) can be used to make these sensing protocols encrypted and/or secure. In other words, we are exploring whether the user can get the desired result (1) while revealing to the server as little information as possible about the question asked and about the answer received (encryption) and (2) while ensuring, at least under some assumptions, that the server is doing what the user is asking the server to do (security/verification).

Classical-channel quantum MPC. We are currently investigating the possibility of performing secure multi-party quantum computations using only classical communication. In this setting, several parties have quantum computers but can only exchange classical messages, and would like to jointly compute a function (or prepare a quantum state) that depends on their inputs, while maintaining privacy and/or preventing the introduction of faults by dishonest parties. While the restriction to classical communication limits the possible state transformations that can be performed to those that can be realized through local operations and classical communication (the so-called "LOCC" class of channels), there are tasks that could benefit from the ability to perform quantum computation in this scenario. For example, the computation might be a quantum simulation of a process in which different parts of the setup are known to different parties. We are currently working to show that such computations can be carried out securely in the model of "specious" adversaries, which (informally) capture a situation in which the parties honestly follow the protocol but may try to extract information that should not be available to them. In future work, we will study stronger notions of security, introduce additional cryptographic functionalities, and reduce the resource requirements of our protocols.

Quantum network verification. As discussed above, this project was mainly about verifying individual quantum devices. Towards the end of the project, we began investigating the possibility of verifying not just one device, but an entire network (and possibly simultaneously the *layout* of the network). In a first attempt, we wanted to construct a protocol that would enable two parties to prove that they can exchange quantum states (equivalently, in a setting where they can communicate classically, that they share quantum entanglement) **and** are located at certain positions. At the moment, it looks like this can be done by a protocol that combines position verification and a CHSH game, but the security proof is harder than for either of those primitives alone. This warrants further research, which we hope to perform in a future project.

References

[ABK+23] Gorjan Alagic, Chen Bai, Jonathan Katz, Christian Majenz, and Patrick Struck. Post-quantum security of tweakable even-mansour, and applications. Cryptology ePrint Archive, Paper 2022/1097, 2023. https://eprint.iacr.org/2022/1097.

[ABKM22] Gorjan Alagic, Chen Bai, Jonathan Katz, and Christian Majenz. Post-quantum security of the even-mansour cipher. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 458–487. Springer, 2022.

[ABPS23] Gorjan Alagic, Chen Bai, Alexander Poremba, and Kaiyan Shi. On the two-sided permutation inversion problem, 2023.

[ACGH20] Gorjan Alagic, Andrew M Childs, Alex B Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation. In *Theory of Cryptography Conference*, pages 153–180. Springer, 2020.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Thorup [Tho18], pages 320–331.

[CGS23] Alexandru Cojocaru, Juan Garay, and Fang Song. Generalized hybrid search and applications. Cryptology ePrint Archive, Paper 2023/798, 2023. https://eprint.iacr.org/2023/798.

[DNM+23] P. Drmota, D. P. Nadlinger, D. Main, B. C. Nichol, E. M. Ainley, D. Leichtle, A. Mantri, E. Kashefi, R. Srinivas, G. Araneda, C. J. Ballance, and D. M. Lucas. Verifiable blind quantum computing with trapped ions and single photons, 2023.

[GDC+21] Andrew Guo, Abhinav Deshpande, Su-Kuan Chu, Zachary Eldredge, Przemyslaw Bienias, Dhruv Devulapalli, Yuan Su, and Andrew Childs. Implementing a fast unbounded quantum fanout gate using power-law interactions. *Bulletin of the American Physical Society*, 2021.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In Thorup [Tho18], pages 259–267.

[Tho18] Mikkel Thorup, editor. *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*. IEEE Computer Society, 2018.

[TMC+21] Meltem Sönmez Turan, Kerry McKay, Donghoon Chang, Cagdas Calik, Lawrence Bassham, Jinkeon Kang, John Kelsey, et al. Status report on the second round of the nist lightweight cryptography standardization process. *National Institute of Standards and Technology Internal Report*, 8369(10.6028), 2021.