AFRL-AFOSR-JP-TR-2019-0001

Quantum primitives for secure computing

Joseph Fitzsimons
Singapore University of Technology and Design
287 GHIM MOH ROAD
Singapore, 279623
SG

12/19/2018
Final Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Asian Office of Aerospace Research and Development
Unit 45002, APO AP 96338-5002

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
19-12-2018	Final	02 Sep 2015 to 01 Sep 2018

4. TITLE AND SUBTITLE
Quantum primitives for secure computing

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA2386-15-1-4082

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Joseph Fitzsimons

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Singapore University of Technology and Design
287 GHIM MOH ROAD
Singapore, 279623 SG

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AOARD
UNIT 45002
APO AP 96338-5002

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-JP-TR-2019-0001

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The PI has had very good success in this project. The project investigated new building blocks for quantum secure computing applications. The PI has developed a number of new secure computing protocols: A multi-client variant of blind quantum computation; several information theoretically secure protocols for somewhat homomorphic quantum encryption, with one experimentally implemented in collaboration with colleagues in Vienna; a protocol for noisy quantum one-time which can enable single-use delegation of digital signatures; Several protocols which allow for the verification of quantum computation; the first blind computing protocol to require only classical communication; and a protocol for securely computing on shared secrets without an honest majority. The PI has published 17 papers as a direct result of the grant.

15. SUBJECT TERMS
Blind computation, AOARD, Quantum secure computation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			CHEN, JERMONT
Unclassified	Unclassified	Unclassified	SAR		19b. TELEPHONE NUMBER *(Include area code)* 315-227-7007

Quantum Primitives for Secure Computing
FA2386-15-1-4082

Final Technical Report

Abstract

This project investigated new building blocks for quantum secure computing applications. We have developed a number of new secure computing protocols: A multi-client variant of blind quantum computation; several information theoretically secure protocols for somewhat-homomorphic quantum encryption, with one experimentally implemented in collaboration with colleagues in Vienna; a protocol for noisy quantum one-time which can enable single-use delegation of digital signatures; Several protocols which allow for the verification of quantum computation; the first blind computing protocol to require only classical communication; and a protocol for securely computing on shared secrets without an honest majority.

Background and Objectives

Quantum cryptography has long been synonymous with quantum key distribution (QKD) protocols, which allow for a short secret key shared between two parties to be extended arbitrarily through communication over an insecure channel that allows for the transmission of quantum states. Unlike classical protocols for key agreement, QKD protocols strive to be information theoretically secure, avoiding reliance on computational assumptions. The utility of quantum information processing in cryptography extends beyond key agreement, however. In particular, it is known that quantum communication can allow for information theoretically secure delegated computation protocols. These protocols allow a user to delegate a (quantum) computation to a remote quantum server while guaranteeing the privacy and integrity of the computation, even if the server acts maliciously. Protocols guaranteeing privacy are generally referred to as blind quantum computation protocols, while protocols guaranteeing the integrity of the computation are known as verifiable quantum computing protocols. The objective of the current project was to uncover new cryptographic methods relevant to secure computing, both extending the functionality of blind and verifiable quantum computing, and uncovering entirely new primitives. Our aim was to uncover new cryptographic protocols and other techniques which could be used as building blocks to construct more complex secure distributed computing systems.

Approach

The approach envisioned in the original project proposal was divided into three distinct tasks. The first task was to extend blind quantum computation protocols to the multi-user setting, allowing multiple users to delegate interacting quantum computations to a single untrusted server while maintaining privacy and integrity. This task was pursued using the abstract cryptography framework to use standard single-user blind and verifiable computing protocols as building blocks of a more complex multi-user protocol. The second task was to uncover new quantum primitives which may have cryptographic applications. This task was approached from a number of angles. Two in particular stand out. A mechanism previously considered for quantum random access codes was considered for use as a cryptographic building block and was used to construct probabilistic one time programs. These are essentially an encoding of computer programs into quantum systems such that they can only be run once. The resulting programs are imperfect, yielding incorrect results with non-vanishing probability, but can be used to build reliable secure systems such as a one-time delegated signature scheme. The second approach was to consider a quantum approach to homomorphic encryption based on mixing input states with other input in a way that commutes with the computation to be performed. The third task was focused on the

development of few qubit protocol, which would have the lowest technological barrier to adoption.

This approach was followed throughout the project, with the majority of research results emerging from the second task. While the first task was accomplished with relatively little cross pollination from other tasks, the development of few qubit protocols (the third task) benefited from new primitives discovered during work on the second task, and in particular from the use of quantum random access codes to encode one-time programs.

Key Results

Below we highlight key results emerging from the project. A significant number of publications emerged from the supported research [1-18], with additional incidental results discovered by supported researchers which were outside the scope of the original research proposal [19-31]. These are listed at the end of this report. The description provided here is only at a high level, and preprints and open access journal articles containing the detailed technical results are attached with the report.

Multi-User Blind Quantum Computation (Task 1)

The extension of blind quantum computing protocols to a setting in which multiple users could delegate interacting computations to a remote server was the main objective of Task 1. A key result of the project is a meta protocol which uses any single user secure delegation protocol (a protocol providing both blind and verifiable quantum computation) and any quantum authentication code to construct a secure system in which multiple users can perform interacting quantum computations. This protocol allows for the computations to be performed without being revealed to the server or to one another, resulting in security equivalent to the case where each user runs the computation locally and users are able to communicate pairwise over secure communications channels. This result is reported in [1].

Probabilistic One Time Programs (Tasks 2 and 3)

Another key outcome of the research was the development of a quantum primitive for probablistic one time programs based on insights from quantum random access codes. By encoding quantum information in the expectation values of anti-commuting observables of a quantum state it is possible to enforce the constraint that learning about some part of the information encoded comes at the cost of erasing some other part of the information. We were able to use this insight to construct a cryptograph protocol enabling programs which can only be run once with some non-zero error probability. While the presence of error makes this result less powerful than an error-free one time program, the error free equivalent is excluded by a pre-existing no-go result. Furthermore, we were able to show that, even using these error-prone one-time programs, it was possible to realise new (error-free) cryptographic functionalities such as the one-time delegation of digital signature authority. These results are the subject of a pending patent application and are reported in [2].

Quantum Analogues of Homomorphic Encryption (Tasks 2 and 3)

One particularly fruitful research direction related to quantum analogues of homomorphic encryption. It has been established that quantum mechanics does not allow for unconditionally secure fully homomorphic encryption schemes. Our approach to this problem was to consider somewhat homomorphic encryptions schemes where the allowed class of computations (privacy homomorphisms) commuted with the encryption and decryption operations. It had previously been shown, by the PI and others [Physical Review A, 88 (2) 022310], that it was possible to encode boson sampling instances (the sampling of the output of an interferometer into which a set of single photons has been injected) in such a way that the location of the injected photons

was partially hidden without affecting the outcome of the computation. This is achieved by inserting additional dummy photons with an orthogonal polarisation to the injected photons in the unencrypted case and then performing the same keyed rotation on the polarisation of each photon. The original protocol hid only a vanishingly small fraction of the encoded information for large boson sampling instances. In [3] we extended this protocol, considering particles with more than two internal states (for example encoding photons using temporal modes rather than polarisation modes), leading to a dramatic improvement in security and an extension of the allowed class of computations which could be performed without interaction. We collaborated with the group of Philip Walther in Vienna to realise an experimental demonstration of this scheme, reported in [4]. We were also able to abstract this idea away from the boson sampling setting, introducing a homomorphic encryption scheme that allows for the evaluation of circuits containing an arbitrary number of Clifford group gates and a bounded number of non-Clifford gates, while achieving information theoretic security (as characterised by vanishing trace distance between any pair of encoded inputs). These results were reported in [5], and a weaker scheme allowing the processing of optical coherent states was reported in [6].

Computing on Shared Secrets (Tasks 2)

Another area in which new cryptographic primitives were identified related to performing computation on shared secrets. A shared secret is a piece of information that has been shared between several parties in such a way that it can only be accessed if some threshold group come together to compare their shares. Using insights obtained in the development of quantum analogues of homomorphic encryption described above, and in particular the scheme described in [5], we were able to construct an unconditionally secure scheme which allowed for secrets to be shared between N parties in such a way that arbitrary quantum computation could be performed on the shared secret without compromising the privacy of the information and without any user having to turn over their share of the information. Our protocol reported in [7] has a threshold of N, which was maintained throughout the computation, and is secure as long as even a single user was honest. This was subsequently extended another group to allow for arbitrary access structures.

Post-hoc Verification Protocols (Tasks 2)

Another productive area under the project was the development of a new approach to verifying quantum computation based on verifying a witness state that certifies the correctness of a quantum computation. The key insight underlying post-hoc verification is that quantum computations can be efficiently encoded as the ground states of known local Hamiltonians using Feynman-Kitaev clock states. By exploits an approach to interactive proofs for the local Hamiltonian problem introduced by Fitzsimons and Vidick [ITCS 2015, p. 103–112], which allowed for the ground states of local Hamiltonians using log-length classical queries to several entangled quantum provers and fixed length quantum responses (of at most two qubits per prover), and a subsequent extension by Ji, which replaced the quantum response with a classical response, we presented a verification protocol using entangled quantum provers which could verify a quantum computation using only a witness state. This result, reported in [8], was the first verification protocol to avoid the need for interaction while the computation is being performed. We also presented an alternate verification method for such states, based on a single prover and a verifier with the ability to measure single qubit states, in [9]. The results were published in a combined form in Physical Review Letters in [10]. This approach to verification is a key step in the recently proposed computationally secure verification scheme of Mahadev [arXiv:1804.01082] which allows verification of a single quantum processor by a purely classical user.

Continuous Variable (CV) Quantum Computing Verification Protocols (Task 2)

Beyond post-hoc verification, we also considered mechanisms for verifying continuous variable quantum computation. This approach to quantum computation has certain practical advantages over the more conventional discrete variable approach. We introduced two protocols to verify quantum computation based on the verification of resource states. In [11] a verification scheme

was introduced for the continuous variable analogue of graph states and hyper-graph states. The use of Serfing's bound allowed for verification without any additional assumptions about independence on the distribution of resource states. An alternate approach to verifying continuous variable quantum computation based on the verification of resource states for non-Gaussian operations (the most difficult task in CV computation), was reported in [12] and presented at QCMC. This latter approach did make use of an independence assumption, however it is likely that insights from the results in [11] can be used to remove this dependence.

Flow Ambiguity (Tasks 2)

Aside from verification protocols, we also considered the possibility of blind computation without quantum communication. It had previously been shown by Aaronson et al [arXiv:1704.08482] that such a task was unlikely to be achievable if perfect secrecy was required. In [13], published in Physical Review X, we showed that it was possible to create classes of quantum circuits which were perfectly indistinguishable if the logic for choosing measurement bases in a measurement-based computation was kept secret. To do this we introduced the notion of flow ambiguity, which captured the fact that the flow patterns which determine how feed-forward corrections are applied within a measurement-based computation are not uniquely identifiable from the measurement bases and results alone, yet are required to identify the computation. As a stepping stone to this result, we proved the universality of XY-plane measurements on cluster states, a problem which had remained open since cluster states were first introduced in 2001. This additional result was reported in [14].

Entangled Multi-Prover Interactive Proofs for Any Computation (Tasks 2 and 3)

Continuing in the vein of interactive proofs, along with Ji, Vidick and Yuen, we studied the power of interactive proofs using multiple entangled provers. We were able to prove for the first time that the power of such systems grows without bound as their completeness-soundness gap shrinks. While this is a largely technical result, it means that such quantum proof systems show an advantage over classical interactive proofs for verifying tough decision problems (i.e. problems beyond the complexity class NEXP). This result is reported in [18] and have been accepted for a talk at QIP 2019.

Outcome

Overall, the project has produced a wide range of new cryptographic techniques. Several of the research results stemming from the project have influenced other researchers, leading to follow-up variations on our protocols for homomorphic encryption, computing on shared secrets and post-hoc verification from other research groups. Post-hoc verification has enabled a key result for classical verification from Mahadev, while the works on homomorphic encryption has been influential in an emerging literature on the topic of quantum homomorphic encryption. The project also led to a comprehensive review paper on blind and verifiable quantum computation which appeared in npj Quantum Information [17].

Publications and Preprints

Results in support of primary project objective

1. Houshmand, M., Houshmand, M., Tan, S.-H., & Fitzsimons, J. F. (2018). Composable secure multi-client delegated quantum computation. *arXiv preprint arXiv:1811.11929.*
2. Roehsner, M. C., Kettlewell, J. A., Batalhão, T. B., Fitzsimons, J. F., & Walther, P. (2018). Quantum advantage for probabilistic one-time programs. *Nature Communications*, *9*(1), 5225.
3. Tan, S. H., Kettlewell, J. A., Ouyang, Y., Chen, L., & Fitzsimons, J. F. (2016). A quantum approach to homomorphic encryption. *Scientific reports*, *6*, 33467.

4. Zeuner, J., Pitsios, I., Tan, S. H., Sharma, A. N., Fitzsimons, J. F., Osellame, R., & Walther, P. (2018). Experimental Quantum Homomorphic Encryption. *arXiv preprint arXiv:1803.10246*.
5. Ouyang, Y., Tan, S. H., & Fitzsimons, J. F. (2018). Quantum homomorphic encryption from quantum codes. *Physical Review A*, *98*(4), 042334.
6. Tan, S. H., Ouyang, Y., & Rohde, P. P. (2018). Practical somewhat-secure quantum somewhat-homomorphic encryption with coherent states. *Physical Review A*, *97*(4), 042308.
7. Ouyang, Y., Tan, S. H., Zhao, L., & Fitzsimons, J. F. (2017). Computing on quantum shared secrets. *Physical Review A*, *96*(5), 052333.
8. Fitzsimons, J. F., & Hajdušek, M. (2015). Post hoc verification of quantum computation. *arXiv preprint arXiv:1512.04375*.
9. Morimae, T., & Fitzsimons, J. F. (2016). Post hoc verification with a single prover. *arXiv preprint arXiv:1603.06046*.
10. Fitzsimons, J. F., Hajdušek, M., & Morimae, T. (2018). Post hoc verification of quantum computation. *Physical Review Letters*, *120*(4), 040501.
11. Takeuchi, Y., Mantri, A., Morimae, T., Mizutani, A., & Fitzsimons, J. F. (2018). Resource-efficient verification of quantum computing using Serfling's bound. *arXiv preprint arXiv: 1806.09138*.
12. Liu, N., Demarie, T. F., Tan, S. H., Aolita, L., & Fitzsimons, J. F. (2018). Client-friendly continuous-variable blind and verifiable quantum computing. *arXiv preprint arXiv:1806.09137*.
13. Mantri, A., Demarie, T. F., Menicucci, N. C., & Fitzsimons, J. F. (2017). Flow ambiguity: A path towards classically driven blind quantum computation. *Physical Review X*, *7*(3), 031004.
14. Mantri, A., Demarie, T. F., & Fitzsimons, J. F. (2017). Universality of quantum computation with cluster states and (X, Y)-plane measurements. *Scientific Reports*, *7*, 42861.
15. Houshmand, M., Houshmand, M., & Fitzsimons, J. F. (2018). Minimal qubit resources for the realization of measurement-based quantum computation. *Physical Review A*, *98*(1), 012318.
16. Demarie, T. F., Ouyang, Y., & Fitzsimons, J. F. (2018). Classical verification of quantum circuits containing few basis changes. *Physical Review A*, *97*(4), 042319.
17. Fitzsimons, J. F. (2017). Private quantum computation: An introduction to blind quantum computing and related protocols. *npj Quantum Information*, *3*(1), 23.
18. Fitzsimons, J., Ji, Z., Vidick, T., & Yuen, H. (2018). Quantum proof systems for iterated exponential time, and beyond. *arXiv preprint arXiv:1805.12166*.

Incidental results from supported researchers

19. Pisarczyk, R., Zhao, Z., Ouyang, Y., Vedral, V. and Fitzsimons, J.F., 2018. Causal limit on quantum communication. *arXiv preprint arXiv:1804.02594*.
20. Zhao, L., Perez-Delgado, C. A., Benjamin, S. C., & Fitzsimons, J. F. (2017). A measurement driven analog of adiabatic quantum computation for frustration-free Hamiltonians. *arXiv preprint arXiv:1706.02559*.
21. Benjamin, S. C., Zhao, L., & Fitzsimons, J. F. (2017). Measurement-driven quantum computing: Performance of a 3-SAT solver. *arXiv preprint arXiv:1711.02687*.
22. Zhao, Z., Dunjko, V., Fitzsimons, J. K., Rebentrost, P., & Fitzsimons, J. F. (2018). A note on state preparation for quantum machine learning. *arXiv preprint arXiv:1804.00281*.
23. Fitzsimons, J. K., Osborne, M. A., Roberts, S. J., & Fitzsimons, J. F. (2016). Improved stochastic trace estimation using mutually unbiased bases. *arXiv preprint arXiv:1608.00117*.
24. Zhao, Z., Pisarczyk, R., Thompson, J., Gu, M., Vedral, V., & Fitzsimons, J. F. (2018). Geometry of quantum correlations in space-time. *Physical Review A*, *98*(5), 052312.
25. Tan, S. H., Krivitsky, L. A., & Englert, B. G. (2016, October). Photon-number-resolving detectors and their role in quantifying quantum correlations. In *Quantum Communications and Quantum Imaging XIV* (Vol. 9980, p. 99800E). International Society for Optics and Photonics.
26. Zhao, Z., Fitzsimons, J. K., Osborne, M. A., Roberts, S. J., & Fitzsimons, J. F. (2018). Quantum algorithms for training Gaussian Processes. *arXiv preprint arXiv:1803.10520*.
27. Bradshaw, M., Assad, S. M., Haw, J. Y., Tan, S. H., Lam, P. K., & Gu, M. (2017). Overarching framework between Gaussian quantum discord and Gaussian quantum illumination. *Physical Review A*, *95*(2), 022333.
28. Batalhao, T. B., Gherardini, S., Santos, J. P., Landi, G. T., & Paternostro, M. (2018). Characterizing irreversibility in open quantum systems. *arXiv preprint arXiv:1806.08441*.

29. Peterson, J. P., Batalhão, T. B., Herrera, M., Souza, A. M., Sarthour, R. S., Oliveira, I. S., & Serra, R. M. (2018). Experimental characterization of a spin quantum heat engine. *arXiv preprint arXiv:1803.06021*.
30. Tan, S. H., & Rohde, P. P. (2018). The resurgence of the linear optics quantum interferometer---recent advances & applications. *arXiv preprint arXiv:1805.11827*.
31. Bouland, A., Fitzsimons, J. F., & Koh, D. E. (2018, June). Complexity Classification of Conjugated Clifford Circuits. In *33rd Computational Complexity Conference*.