Quantum obfuscation

Gorjan Alagic and Bill Fefferman

September 24, 2015

Abstract

Encryption of data is fundamental to secure communication in the modern world. Beyond encryption of data lies *obfuscation*, i.e., encryption of functionality. It has been known for some time that the most powerful classical obfuscation, so-called "black-box obfuscation," is impossible. In this work, we initialize the rigorous study of obfuscating programs *via quantum-mechanical means,* and prove quantum versions of several foundational results in obfuscation.

In its most powerful "quantum black-box" instantiation, a quantum obfuscator would turn a description of a quantum program f into a quantum state ρ_f, such that anyone in possession of ρ_f can repeatedly evaluate f on inputs of their choice, but never learn *anything else* about the original program. We formalize this notion of obfuscation, and prove an impossibility result: such obfuscation is only possible in a setting where the adversary never has access to multiple obfuscations (of either the same program, or of different programs.) Nonetheless, we show that even in this remaining setting, some applications of obfuscations remain possible. These include CPA-secure quantum encryption, quantum fully-homomorphic encryption, and quantum money.

We also define quantum versions of indistinguishability obfuscation and best-possible obfuscation. We then show that these notions are equivalent, and that their perfect and statistical variants are impossible to achieve. The remaining (i.e., computational) variant would still have an application of interest: witness encryption for QMA.

1. Introduction

Obfuscation. Obfuscation is the ability to encrypt functionality, which is arguably the most powerful cryptographic ability that may yet be possible. It implies (with caveats) the ability to perform almost any other cryptographic task imaginable, including fully homomorphic encryption. A more mundane application is protecting intellectual property in software. In this setting, a developer wishes to publish their software without revealing any trade secrets. To this end, the software program is passed through an *obfuscator*, i.e. an algorithm satisfying

1. *functional equivalence:* does not change input/output functionality;
2. *polynomial slowdown:* maintains efficiency;
3. *obfuscation:* the code of the output program is "hard to understand."

The last condition can be formulated rigorously in a number of ways. The strongest is the so-called "virtual black-box" condition, which says that the obfuscated program is no more useful than an impenetrable box which simply accepts inputs and produces outputs.

Classical status. The first major result in classical obfuscation was the 2001 proof by Barak et al. that virtual black-box obfuscation is impossible, and that many of the applications are impossible to achieve generically [6, 7]. An important step in formulating alternative

notions of obfuscation was taken by Goldwasser and Rothblum; they defined *indistinguishability obfuscation* and *best-possible obfuscation* [20]. Indistinguishability requires that functionally-equivalent circuits are mapped to indistinguishable distributions; best-possible requires that circuits are mapped to the "least leaky" functionally equivalent circuit. Both definitions have perfect, statistical, and computational variants. In [20] it was shown that the two definitions are equivalent, and that the perfect and statistical versions are impossible (unless the PH collapses) [20].

In 2013, in a breakthrough result, Garg et al. proposed a convincing candidate for the one remaining possibility: computational indistinguishability obfuscation. Their proposal was based on the hardness of a certain problem in mutlilinear maps [16]. It was accompanied by another breakthrough: a range of applications so wide, that it was suggested that indistinguishability obfuscation might become a "'central hub' for cryptography" [26]. These two breakthroughs were followed by a flurry of new activity in the area, including several new proposals and applications [8, 11, 12, 13, 18, 22]. Unfortunately, the quantum security of the underlying hardness assumptions has recently been put into doubt [25].

Quantum status. Quantum obfuscation is essentially an unexplored topic, and the present work appears to be the first rigorous treatment of the foundational questions. The question of whether quantum obfuscation is possible was posed as one of Scott Aaronson's "semi-grand challenges" for quantum computation [1]. Since so little work on quantum obfuscation has appeared, we briefly discuss some related results. In [2], Aaronson proposed a *complexity-theoretic no-cloning theorem*; he also claimed that an oracle exists relative to which "software copy-protection" is possible. Unfortunately, a full version of [2] with proofs never appeared, although the complexity-theoretic no-cloning theorem was eventually proved in a paper on quantum money [3]. In related work, Mosca and Stebila proposed a black-box quantum money scheme, and suggested the possibility of using a quantum circuit obfuscator in place of the black box [24]. More recently, Alagic, Jeffery and Jordan proposed obfuscators for both classical (reversible) circuits and quantum circuits, based on ideas from topological quantum computation [4]. The proposed obfuscator satisfies indistinguishability for a restricted set of circuit equivalences; its usefulness is unclear at this time.

2. Our results

We now summarize our contributions; details are explained in the full technical version. In what follows, poly-time algorithms will be called PT, PPT, or QPT; these mean (respectively) classical deterministic, probabilistic, and quantum. For a quantum circuit C, the resulting unitary operator is U_C. Functions decaying faster than any inverse-polynomial are denoted $\mathrm{negl}(\cdot)$.

Quantum black-box obfuscation.

Definition 1. *A **black-box quantum obfuscator** is a pair of QPTs $(\mathcal{J}, \mathcal{O})$ such that for any n-qubit quantum circuit C, the state*[1] *$\mathcal{O}(C)$ satisfies:*

1. *(functional equivalence) $\left\|\mathcal{J}(\mathcal{O}(C)\otimes\rho) - U_C\rho U_C^\dagger\right\|_{\mathrm{tr}} \leq \mathrm{negl}(n)$ for all states ρ;*
2. *(virtual black-box) $\forall$ QPT $\mathcal{A}$ $\exists$ QPT $\mathcal{S}^{U_C}$ such that $|\Pr[\mathcal{A}(\mathcal{O}(C))=1] - \Pr[\mathcal{S}^{U_C}(0^n)=1]| \leq \mathrm{negl}(n)$.*

We say that an obfuscator is **reusable** if the reduced state on some output register of $\mathcal{J}$ contains a state which again satisfies the functional equivalence condition. Our first result places significant restrictions on quantum black-box obfuscators.

[1] The poly-slowdown property now asks that $\mathcal{O}(C)$ is poly(n)-qubit; this is ensured by $\mathcal{O}$ being QPT.

Theorem 1. *Reusable black-box quantum obfuscation is impossible for pairs: an adversary with access to two outputs of the obfuscator (even on the same input) can violate the black-box condition.*

Corollary 2. *Black-box obfuscation of quantum circuits into quantum circuits is impossible.*

The corollary is a quantum generalization of the main result of Barak et al. [6]. To prove Theorem 1, we give an explicit distribution of quantum circuit ensembles which cannot be obfuscated. The main technical obstacle is to show that the quantum states output by the obfuscator can be "executed on one another," without revealing certain secrets to simulators having only black-box access to the original circuits. A crucial ingredient in overcoming this obstacle is a notion of *chosen-ciphertext-secure quantum encryption.* To achieve this, we show:

Theorem 3. *If quantum-secure one-way functions (qOWF) exist, then so do IND-CCA1-secure symmetric-key quantum encryption schemes (qSKE).*

The above requires several new definitions (e.g., IND-CCA1 for quantum encryption) which we also provide. A complete treatment of the subject of quantum encryption with computational assumptions will soon appear in a joint work [5].

In addition, we provide several applications of quantum black-box obfuscation, which are still feasible (in some form) in spite of Theorem 1. They are briefly outlined as follows.

1. **IND-CPA-secure encryption.** Crucially, this demands only a quantum black-box obfuscator, but *not* one-way functions.
2. **qOWF imply IND-CPA public-key homomorphic encryption.** Start with qSKE via Theorem 3; public keys are obfuscations of encrypt circuits; evaluation keys are obfuscations of a universal decrypt-compute-encrypt circuit. Trapdoor permutations are not required.
3. **Public-key quantum money**. This was proposed by Mosca and Stebila [24], using a result of Aaronson and Christiano [2, 3]. As we show, a certain adaptation survives Theorem 1.

We emphasize that applications 1 and 2 also work for achieving *classical functionality* from a quantum obfuscator; however, they use quantum ciphertexts and quantum keys—another approach not considered before.

Quantum indistinguishability obfuscation. Following the classical approach of Goldwasser and Rothblum [20], we define a version of Definition 1 which guarantees indistinguishability of obfuscator outputs, by replacing condition (2.) with:

2. *(indistinguishability) if* $\|U_{C_1} - U_{C_2}\| \leq \mathrm{negl}(n)$, *then* $\|\mathcal{O}(C_1) - \mathcal{O}(C_2)\|_* \leq \mathrm{negl}(n)$.

We also define a notion of *quantum best-possible obfuscation*:

2. *(best-possible) if* $\|U_{C_1} - U_{C_2}\| \leq \mathrm{negl}(n)$, *then for all QPT* $\mathcal{A}$ *there exists a QPT* $\mathcal{S}$ *satisfying* $\|\mathcal{A}(\mathcal{O}(C_1)) - \mathcal{S}(C_2)\|_* \leq \mathrm{negl}(n)$.

Both definitions above have three variants, depending on the nature of the norm $\|\cdot\|_*$: perfect, statistical, and computational (against QPTs). We prove the following equivalence result.

Theorem 4. *A QPT is an indistinguishability obfuscator if and only if it is a best-possible obfuscator.*

We also show that these definitions are only achievable when the distinguishability is guaranteed only against computationally bounded (quantum) adversaries.

Theorem 5. *If quantum statistical-indistinguishability obfuscators exist, then coQMA* $\subseteq$ *QSZK.*

This leaves the indistinguishability approach to quantum obfuscation in a state of affairs similar to the classical world: computational obfuscation is the only surviving candidate. We end by showing that even such obfuscators would have an interesting application, namely quantum witness encryption for QMA. Witness encryption for a QMA language L provides for

encryption of a plaintext x to a potential instance l. The security guarantee is that (i.) if $l \in L$, then any valid witness allows for decryption of x, and (ii.) if $l \notin L$, then encryptions of different plaintexts are computationally indistinguishable. Classical witness encryption is known to have numerous applications [17]. We show the following.

Theorem 6. *If quantum computational-indistinguishability obfuscators exist, then so do witness encryption schemes for QMA.*

We conjecture that many of the other recently discovered classical applications also have interesting quantum analogues or extensions.

References

[1] Scott Aaronson. Ten semi-grand challenges for quantum computing theory. http://www.scottaaronson.com/writings/qchallenge.html, July 2005. Retrieved 09/15.

[2] Scott Aaronson. Quantum copy-protection and quantum money. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 229–242. IEEE, 2009.

[3] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60. ACM, 2012.

[4] Gorjan Alagic, Stacey Jeffery, and Stephen Jordan. Circuit obfuscation using braids. In *Proceedings of TQC 2014*, volume 27, pages 141–160, 2014.

[5] Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael StJules. Computational security for quantum encryption. *To appear.*, 2015.

[6] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 1–18, London, UK, UK, 2001. Springer-Verlag. ISBN 3-540-42456-3. URL http://dl.acm.org/citation.cfm?id=646766.704152.

[7] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6:1–6:48, May 2012. ISSN 0004-5411. doi:10.1145/2160158.2160159. URL http://doi.acm.org/10.1145/2160158.2160159.

[8] Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Protecting obfuscation against algebraic attacks. In PhongQ. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 221–238. Springer Berlin Heidelberg, 2014. ISBN 978-3-642-55219-9. doi:10.1007/978-3-642-55220-5_13. URL http://dx.doi.org/10.1007/978-3-642-55220-5_13.

[9] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933. URL http://dx.doi.org/10.1137/S0097539796300933.

[10] CharlesH. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In David Chaum, RonaldL. Rivest, and AlanT.

Sherman, editors, *Advances in Cryptology*, pages 267–275. Springer US, 1983. ISBN 978-1-4757-0604-8. doi:10.1007/978-1-4757-0602-4_26. URL http://dx.doi.org/10.1007/978-1-4757-0602-4_26.

[11] Nir Bitansky, Ran Canetti, Henry Cohn, Shafi Goldwasser, Yael Tauman Kalai, Omer Paneth, and Alon Rosen. The impossibility of obfuscation with auxiliary input or a universal simulator. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology CRYPTO 2014*, volume 8617 of *Lecture Notes in Computer Science*, pages 71–89. Springer Berlin Heidelberg, 2014. ISBN 978-3-662-44380-4. doi:10.1007/978-3-662-44381-1_5. URL http://dx.doi.org/10.1007/978-3-662-44381-1_5.

[12] Dan Boneh and Mark Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 480–499. Springer Berlin Heidelberg, 2014. ISBN 978-3-662-44370-5. doi:10.1007/978-3-662-44371-2_27. URL http://dx.doi.org/10.1007/978-3-662-44371-2_27.

[13] Zvika Brakerski and GuyN. Rothblum. Virtual black-box obfuscation for all circuits via generic graded encoding. In Yehuda Lindell, editor, *Theory of Cryptography*, volume 8349 of *Lecture Notes in Computer Science*, pages 1–25. Springer Berlin Heidelberg, 2014. ISBN 978-3-642-54241-1. doi:10.1007/978-3-642-54242-8_1. URL http://dx.doi.org/10.1007/978-3-642-54242-8_1.

[14] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. *Crypto 2015 (to appear)*, December 2015.

[15] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, pages 276–289, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1115-1. doi:10.1145/2090236.2090260. URL http://doi.acm.org/10.1145/2090236.2090260.

[16] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 40–49, Oct 2013. doi:10.1109/FOCS.2013.13.

[17] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 467–476, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2029-0. doi:10.1145/2488608.2488667. URL http://doi.acm.org/10.1145/2488608.2488667.

[18] Sanjam Garg, Craig Gentry, Shai Halevi, and Daniel Wichs. On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input. In JuanA. Garay and Rosario Gennaro, editors, *Advances in Cryptology CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 518–535. Springer Berlin Heidelberg, 2014. ISBN 978-3-662-44370-5. doi:10.1007/978-3-662-44371-2_29. URL http://dx.doi.org/10.1007/978-3-662-44371-2_29.

[19] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986. ISSN 0004-5411. doi:http://doi.acm.org/10.1145/6490.6503.

[20] Shafi Goldwasser and GuyN. Rothblum. On best-possible obfuscation. In SalilP. Vadhan, editor, *Theory of Cryptography*, volume 4392 of *Lecture Notes in Computer Science*, pages 194–213. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-70935-0. doi:10.1007/978-3-540-70936-7_11. URL http://dx.doi.org/10.1007/978-3-540-70936-7_11.

[21] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28:1364–1396, March 1999. ISSN 0097-5397. doi:http://dx.doi.org/10.1137/S0097539793244708. URL http://dx.doi.org/10.1137/S0097539793244708.

[22] Susan Hohenberger, Amit Sahai, and Brent Waters. Replacing a random oracle: Full domain hash from indistinguishability obfuscation. In PhongQ. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 201–220. Springer Berlin Heidelberg, 2014. ISBN 978-3-642-55219-9. doi:10.1007/978-3-642-55220-5_12. URL http://dx.doi.org/10.1007/978-3-642-55220-5_12.

[23] Dominik Janzing, Pawel Wocjan, and Thomas Beth. Non-identity check is qma-complete. In *International Journal of Quantum Information*, 2005.

[24] Michele Mosca and Douglas Stebila. Quantum coins. *Error-Correcting Codes, Finite Geometries and Cryptography*, 523:35–47, 2010.

[25] Chris Peikert. What does gchq "cautionary tale" mean for lattice cryptography? http://web.eecs.umich.edu/ cpeikert/soliloquy.html, June 2015. Retrieved 09/2015.

[26] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 475–484, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2710-7. doi:10.1145/2591796.2591825. URL http://doi.acm.org/10.1145/2591796.2591825.

[27] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, page 459. IEEE Computer Society, 2002. ISBN 0-7695-1822-2. doi:10.1109/SFCS.2002.1181970. URL http://dx.doi.org/10.1109/SFCS.2002.1181970.

[28] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[29] Mark Zhandry. How to Construct Quantum Random Functions. In *FOCS 2012*, pages 679–687. IEEE, 2012.