All graph state verification protocols are composably secure

Léo Colisson [1], Damian Markham[2], and Raja Yehia [3]

[1]QuSoft and Centrum Wiskunde & Informatica, Science Park 123, 1098 XG Amsterdam, Netherlands
[2]Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France
[3]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Spain

Abstract

Graph state verification protocols allow multiple parties to share a graph state while checking that the state is honestly prepared, even in the presence of malicious parties. Since graph states are the starting point of numerous quantum protocols, it is crucial to ensure that graph state verification protocols can safely be composed with other protocols, this property being known as *composable security*. Previous works [YDK21] conjectured that such a property could not be proven within the abstract cryptography framework: we disprove this conjecture by showing that *all* graph state verification protocols can be turned into a composably secure protocol with respect to the natural functionality for graph state preparation. Moreover, we show that any *unchanged* graph state verification protocol can also be considered as composably secure for a slightly different, yet useful, functionality. Finally, we show that these two results are optimal, in the sense that any such generic result, considering arbitrary black-box protocols, must either modify the protocol or consider a different functionality.

Along the way, we show a protocol to generalize entanglement swapping to arbitrary graph states that might be of independent interest. We derive our results using the scalable ZX-calculus formalism, providing one of the first application of this formalism to cryptography.

Link to full paper: https://arxiv.org/abs/2402.01445

1 Introduction

Quantum networks enhance today's networks capabilities by providing a higher level of security, based on the inviolable laws of physics, but also by enabling the emergence of new protocols impossible to obtain classically. The spectrum of quantum protocols is wide, starting from quantum teleportation [BBC+93] to delegated and multiparty computation [BFK09, FK17, DNS12, DGJ+20], anonymous transmission [CW05, UMY+18], copy-protection [Aar09], coin flipping [Gan09, BCK+20], and more. A large fraction of these protocols, including quantum teleportation, requires parties to share multipartite entangled quantum states before the beginning of the protocol. These states are typically Bell pairs, GHZ states, or, more generally, arbitrary *graph states*. The task of preparing and securely distributing these states among all parties is typically achieved using a so-called *graph state verification protocol*.

Graph state verification protocols should be resilient to deviations from possibly malicious parties, whether they are controlling the source of quantum states or not. Such security properties are usually proven in a game-based model, in which we study and prove resilience against specific malicious strategies. In this model, we can only prove guarantees on the final quantum state, but we cannot obtain any guarantee on the behavior of the protocol when it is repeated or

composed with other protocols, or when the adversary is allowed to run attacks in parallel. This is insufficient for protocols that are used as building blocks, such as graph state verification.

As a consequence, it is often unclear if the security of a protocol using graph states is preserved when the graph state is obtained via a *graph state verification protocol* instead of being honestly generated by a trusted third party. This leads to the natural question:

Is it safe to compose any arbitrary protocol with any arbitrary graph state verification protocol? Is it still secure if the adversary can run multiple attacks in parallel?

The study of the composition of protocols is typically done in a security framework where the notion of *functionality* or *resource* is introduced in order to abstract the properties of a given protocol [Can01, Unr10, MR11a, Mau12]. A functionality can be seen as a trusted third party: a protocol is said to realize a given functionality if it is impossible to distinguish a run of the protocol from a use of the functionality. With this concept in mind, creating new protocols from sub-protocols is a breeze: we just need to prove that the protocol is secure when the sub-protocol is implemented by a functionality, and we are automatically guaranteed that the protocol will still be secure if we use a sub-protocol realizing this functionality, even if the adversary is allowed to run attacks in parallel. Composing functionalities is therefore fundamental when designing protocols, since many more advanced protocols are often obtained by composing simpler sub-protocols. This use of functionalities as black-boxes with definite input and outputs increases the reusability of protocols. When using the terminology of these frameworks, the above questions can be reformulated as follows:

Do composable graph state verification protocols exist?

Previous works were only able to show limited results regarding this question. Notably, [YDK21] was considering the setting where only the source can be malicious, and conjectured that there might not exist a single composable state verification protocol.

2 Our results

In this work we refute this conjecture by answering positively to this interrogation, actually proving that *any* secure graph state verification protocol is composable. More specifically:

- We present a method to turn any arbitrary graph state verification protocol, secure in the game-based model, into a composably secure protocol realizing the natural[1] functionality $\mathcal{V}_{|G\rangle}$ for graph state verification. This "compilation" only adds one round of classical communication at the end of the protocol, and mostly preserves the guarantees of the original protocol. More precisely, if the final state obtained in the real protocol is supposed to be ε-close to the target graph state for some notion of closeness, then the protocol ε-realizes $\mathcal{V}_{|G\rangle}$. Our results are expressed in the abstract cryptography framework [MR11a].
- We also show that any *unchanged* graph state verification protocol is also composably secure for a slightly different, yet useful, functionality $\mathcal{V}^{f}_{|G\rangle}$. This functionality differs from $\mathcal{V}_{|G\rangle}$ by allowing the adversary to apply a limited set of corrections (characterized by f) on the qubits owned by the honest parties.
- We show that it is *impossible* to prove that any arbitrary unchanged protocol realizes $\mathcal{V}_{|G\rangle}$ having only black-box access to the protocol, without either changing the protocol, or the functionality, showing that the above results are optimal.

[1] More precisely, $\mathcal{V}_{|G\rangle}$ distributes the graph state $|G\rangle$ between all parties, giving first this state to malicious parties. The adversary is only allowed to make the functionality abort before sending the shares of $|G\rangle$ belonging to the honest parties.

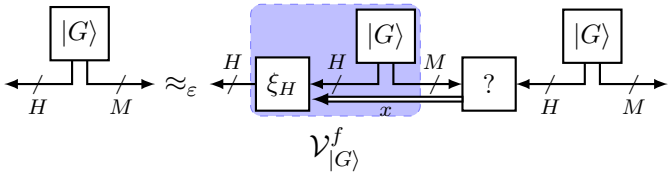
- As an application, we show that our result can be applied to existing protocols, in particular we show that [PCW+11] and [UM22] are composably secure.
- Along the way, we show a protocol to generalize entanglement swapping to arbitrary graph states, which might be of independent interest. Since graph-state manipulation can be challenging using the usual density matrix formalism, we use scalable ZX-calculus [CK17, CHP19] to prove our results, asserting the relevance of this language for complex graph state manipulation, including in the context of quantum cryptography.

3 Quick overview and main techniques

Our result are expressed in the Abstract Cryptography framework (AC) [MR11a], in which we prove the realisation of an ideal resource $\mathcal{V}^f_{|G\rangle}$ by any concrete graph state verification protocol. $\mathcal{V}^f_{|G\rangle}$ is a black-box functionality that shares a graph state while allowing dishonest parties to apply some corrections to it (limited by the function f). We also show how to transform concrete protocols so that they realise a more natural ideal functionality $\mathcal{V}_{|G\rangle}$ simply sharing graph states to n parties.

To prove the realisation of an ideal functionality in the AC framework, we need to construct so-called simulators. Along the proof, we find that it is necessary for the simulators to perform a *merging* operation that transform two copies of a graph state $|G\rangle$ into one while only accessing a partition of the qubits from the two copies of $|G\rangle$. If the graph $|G\rangle$ is a simple Bell pair, this is known as entanglement swapping. Unfortunately, such an operation is not know to exist for generic graphs.

We can show that it is impossible to find such a map to realise $\mathcal{V}_{|G\rangle}$ without breaking non-signaling, leading to our first impossibility result. Therefore, the simulator must communicate some corrections to apply to the other part of the graph state, leading to the functionality $\mathcal{V}^f_{|G\rangle}$. We therefore construct two maps: a correction map ξ_H, performed by the functionality, and $\boxed{?}$, performed by the simulator such that:



(1)

where the LHS represents the *concrete* world and the RHS represents the *ideal* world. We say that a state $|G\rangle$ is *mergeable* if there exist such ξ_H and $\boxed{?}$. Studying the set of mergeable states is therefore fundamental since being mergeable is a necessary condition for composability.

In the full version of the article, we show that **all graph states are mergeable**, by providing a non-trivial construction relying on the rank of the adjacency matrix of the graph state. We were able to obtain and prove the correctness of this construction **using the scalable ZX-calculus** [CHP19], providing one of the first application of this formalism to cryptography. Using this property, we are then able to prove the composable security of any graph state verification protocol.

Finally, by relying on some fundamental properties of graph states, we show that these corrections can instead be applied directly by the simulator instead of the functionality, at the cost of adding an additional round of communication, where all parties apply a random stabilizer to their state. By adding this extra round, we can thus transform any graph state verification protocol into a protocol that realises the natural graph state verification functionality $\mathcal{V}_{|G\rangle}$.

References

[Aar09] S. Aaronson. Quantum Copy-Protection and Quantum Money. In *2009 24th Annual IEEE Conference on Computational Complexity*. 2009 24th Annual IEEE Conference on Computational Complexity, pages 229–242, July 2009.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 29, 1993.

[BBD+09] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, January 2009.

[BCK+20] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti. Quantum weak coin flipping with a single photon, 2020.

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal Blind Quantum Computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. 2009 50th Annual IEEE Symposium on Foundations of Computer Science, pages 517–526, October 2009.

[BOT+18] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti. Experimental investigation of practical unforgeable quantum money. *npj Quantum Information*, 4(1), January 2018.

[Can01] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. Proceedings 42nd IEEE Symposium on Foundations of Computer Science, pages 136–145, October 2001.

[Car20] T. Carette. A note on diagonal gates in SZX-calculus, December 17, 2020.

[CD08] B. Coecke and R. Duncan. Interacting Quantum Observables. In L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, editors, *Automata, Languages and Programming*, Lecture Notes in Computer Science, pages 298–310, Berlin, Heidelberg. Springer, 2008.

[CDK22] F. Centrone, E. Diamanti, and I. Kerenidis. Practical quantum electronic voting. *Phys. Rev. Applied*, 18:014005, 2022.

[CHP19] T. Carette, D. Horsman, and S. Perdrix. SZX-calculus: Scalable Graphical Quantum Reasoning. 2019.

[CK17] B. Coecke and A. Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, Cambridge, 2017.

[CMS23] L. Colisson, G. Muguruza, and F. Speelman. Oblivious Transfer from Zero-Knowledge Proofs, or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States, March 2, 2023. To appear in ASIACRYPT 2023.

[CW05] M. Christandl and S. Wehner. Quantum Anonymous Transmissions. In B. Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, Lecture Notes in Computer Science, pages 217–235, Berlin, Heidelberg. Springer, 2005.

[DFP+14] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner. Composable security of delegated quantum computation. In P. Sarkar and T. Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, pages 406–425, Berlin, Heidelberg. Springer Berlin Heidelberg, 2014.

[DGJ+20] Y. Dulek, A. B. Grilo, S. Jeffery, C. Majenz, and C. Schaffner. Secure Multi-party Quantum Computation with a Dishonest Majority. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, Lecture Notes in Computer Science, pages 729–758, Cham. Springer International Publishing, 2020.

[DM13] G. Demay and U. Maurer. Unfair coin tossing. *2013 IEEE International Symposium on Information Theory*:1556–1560, 2013.

[DNS12] F. Dupuis, J. B. Nielsen, and L. Salvail. Actively Secure Two-Party Evaluation of Any Quantum Operation. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, Lecture Notes in Computer Science, pages 794–811, Berlin, Heidelberg. Springer, 2012.

[FK17] J. F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(1):012303, July 5, 2017.

[Gan09] M. Ganz. Quantum leader election. *Quantum Information Processing*, 16, October 2009.

[GKK19] A. Gheorghiu, T. Kapourniotis, and E. Kashefi. Verification of Quantum Computation: An Overview of Existing Approaches. *Theory of Computing Systems*, 63(4):715–808, May 1, 2019.

[GLS+21] A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan. Oblivious Transfer Is in MiniQCrypt. In A. Canteaut and F.-X. Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, Lecture Notes in Computer Science, pages 531–561, Cham. Springer International Publishing, 2021.

[GV19] A. Gheorghiu and T. Vidick. Computationally-secure and composable remote state preparation. *ArXiv*, abs/1904.06320, 2019.

[HHT+18] M. Houshmand, M. Houshmand, S.-H. Tan, and J. Fitzsimons. Composable secure multi-client delegated quantum computation. *ArXiv*, abs/1811.11929, 2018.

[HZB+06] M. Hillery, M. Ziman, V. Bužek, and M. Bieliková. Towards quantum-based privacy and voting. *Physics Letters A*, 349(1):75–81, January 9, 2006.

[JMM19] D. Jost, U. Maurer, and M. Mularczyk. A unified and composable take on ratcheting. Cryptology ePrint Archive, Report 2019/694, 2019.

[KP17] E. Kashefi and A. Pappa. Multiparty Delegated Quantum Computing. *Cryptography*, 1(2):12, July 2017.

[Mau11] U. Maurer. Constructive cryptography - a new paradigm for security definitions and proofs. *IN Theory of Security and Applications*:33–56, 2011.

[Mau12] U. Maurer. Constructive Cryptography – A New Paradigm for Security Definitions and Proofs. In S. Mödersheim and C. Palamidessi, editors, *Theory of Security and Applications*, Lecture Notes in Computer Science, pages 33–56, Berlin, Heidelberg. Springer, 2012.

[MF18] T. Morimae and J. F. Fitzsimons. Post hoc verification with a single prover. *Physical Review Letters*, 120(4):040501, January 22, 2018.

[MPB+16] W. McCutcheon, A. Pappa, B. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. Rarity, and M. Tame. Experimental verification of multipartite entanglement in quantum networks. *Nature Communications*, 7:13251, November 2016.

[MR11a] U. Maurer and R. Renner. Abstract Cryptography. In *ICS*, 2011.

[MR11b] U. Maurer and R. Renner. Abstract cryptography. *In Innovations In Computer Science*, 2011.

[MR16a] U. Maurer and J. Ribeiro. New perspectives on weak oblivious transfer. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 790–794, July 2016.

[MR16b] U. Maurer and R. Renner. From indifferentiability to constructive cryptography (and back). In *Theory of Cryptography*, pages 3–24, Berlin, Heidelberg. Springer Berlin Heidelberg, 2016.

[NC10] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information: 10th Anniversary Edition. Higher Education from Cambridge University Press. December 9, 2010.

[PCW+11] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis. Multipartite entanglement verification resistant against dishonest parties. *Physical Review Letters*, 108, December 2011.

[UM22] A. Unnikrishnan and D. Markham. Verification of graph states in an untrusted network. *Physical Review A*, 105(5):052420, May 13, 2022.

[UMY+18] A. Unnikrishnan, I. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis. Anonymity for practical quantum networks. *Physical Review Letters*, 122, November 2018.

[Unr10] D. Unruh. Universally Composable Quantum Multi-party Computation. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, Lecture Notes in Computer Science, pages 486–505, Berlin, Heidelberg. Springer, 2010.

[van20] J. van de Wetering. ZX-calculus for the working quantum computer scientist. *arXiv:2012.13966 [quant-ph]*, December 2020.

[VPdR19] V. Vilasini, C. Portmann, and L. del Rio. Composable security in relativistic quantum cryptography. *New Journal of Physics*, 21(4):043057, April 2019.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1):78–88, January 1, 1983.

[YDK21] R. Yehia, E. Diamanti, and I. Kerenidis. Composable security for multipartite entanglement verification. *Physical Review A*, 103(5):052609, May 19, 2021.