11th BIU Winter School on Cryptography

References on delegated computation

Thomas Vidick, Caltech

February 15, 2021

Lecture 1: Delegation with a small quantum verifier

- A comprehensive survey on delegated quantum computation (DQC): [GKK19].
- Composable definition of delegated computation in abstract cryptography [DFPR14].
- Childs' protocol for blind DQC [Chi05].
- Impossibility results for information-theoretic blind delegation with a classical client [ACGK19]. Quantum homomorphic encryption [Mah20].
- (Non-composable) definition of authentication [BCG$^+$02] and Clifford authentication scheme [ABOEM17]. For a composable security proof, see [Por17].
- Verifiable protocols: circuit-based [ABOE08, ABOEM17, Bro18] and measurement-based [BFK09, FK17].

Lecture 2: Delegation with two quantum servers sharing entanglement

- BFLS protocol for two-server delegation of classical NP computations [BFLS91].
- For more on rigidity of the Magic Square games, and other references, see Lecture 3 in the lecture notes `http://users.cms.caltech.edu/~vidick/teaching/fsmp/fsmp.pdf`.
- The RUV delegation protocol [RUV13]. For a high-level description, see Section 10.4 in the notes `http://users.cms.caltech.edu/~vidick/notes/QCryptoX/LN_Week10.pdf`.
- QMA-completeness of local Hamiltonians with only XX or ZZ terms is shown in [CM16]. The nonlocal form given in lecture follows by a simple amplification trick (taking tensor powers).
- The Grilo delegation protocol [Gri19].
- For notes on the Pauli braiding test, see the notes `http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf`, which are based on [NV17]. The "quantum low-degree test" extension using poly-logarithmic communication appears in [JNV$^+$20, Appendix A].

Lecture 3: Delegation with a classical verifier and a single quantum prover

- The Morimae-Fitzsimons protocol appears in [MF16]; see also [FHM18].
- The Mahadev verification protocol is [Mah18].
- Trapdoor claw-free functions with the adaptive hardcore bit property are constructed in [BCM+18].
- The definition of the extracted qubit and claims around it can be found in Lecture 6 here `http://users.cms.caltech.edu/~vidick/teaching/fsmp/fsmp.pdf`.
- Non-interactive protocol in QRO model [ACGH20].
- Efficient verifier in CRS+QRO [CCY19].
- Verification of sampling problems [CLLW20].
- Proofs of knowledge [VZ20].
- Composable protocol [GV19].

References

[ABOE08] Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. *arXiv preprint arXiv:0810.5375*, 2008.

[ABOEM17] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiv preprint arXiv:1704.04487*, 2017.

[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.

[ACGK19] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. Complexity-theoretic limitations on blind delegated quantum computation. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 449–458. IEEE, 2002.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 320–331. IEEE, 2018.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009.

[BFLS91] László Babai, Lance Fortnow, Leonid A Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 21–32, 1991.

[Bro18] Anne Broadbent. How to verify a quantum computation. *Theory of Computing*, 14(1):1–37, 2018.

[CCY19] Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. Classical verification of quantum computations with efficient verifier. *arXiv preprint arXiv:1912.00990*, 2019.

[Chi05] Andrew M Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, 2005.

[CLLW20] Kai-Min Chung, Yi Lee, Han-Hsuan Lin, and Xiaodi Wu. Constant-round blind classical verification of quantum sampling. *arXiv preprint arXiv:2012.04848*, 2020.

[CM16] Toby Cubitt and Ashley Montanaro. Complexity classification of local hamiltonian problems. *SIAM Journal on Computing*, 45(2):268–316, 2016.

[DFPR14] Vedran Dunjko, Joseph F Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer, 2014.

[FHM18] Joseph F Fitzsimons, Michal Hajdušek, and Tomoyuki Morimae. Post hoc verification of quantum computation. *Physical review letters*, 120(4):040501, 2018.

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

[GKK19] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of computing systems*, 63(4):715–808, 2019.

[Gri19] Alex Bredariol Grilo. A simple protocol for verifiable delegation of quantum computation in one round. In *46th International Colloquium on Automata, Languages, and Programming,{ICALP} 2019, July 9-12, 2019, Patras, Greece*, 2019.

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033. IEEE, 2019.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*= RE. *arXiv preprint arXiv:2001.04383*, 2020.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267. IEEE, 2018.

[Mah20] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. *SIAM Journal on Computing*, (0):FOCS18–189, 2020.

[MF16] Tomoyuki Morimae and Joseph F Fitzsimons. Post hoc verification with a single prover. *arXiv preprint arXiv:1603.06046*, 2016.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015, 2017.

[Por17] Christopher Portmann. Quantum authentication with key recycling. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 339–368. Springer, 2017.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[VZ20] Thomas Vidick and Tina Zhang. Classical proofs of quantum knowledge. *arXiv preprint arXiv:2005.01691*, 2020.