Quantum Aspects of Cryptography

Assignments 10 and 11—BQP$\neq$QMA, yet PRU exist, Self-testing, QFHE and Verification
(topics from Lectures 22 to 27)
VERSION: $\alpha.1$—APRIL 25, 2025

Instructions. Same as those in previous assignments (including the updates since Assignment 5) except that *May 6, 2025* for this course is a *hard deadline* for all assignments—no unused extension can be availed to extend beyond that.

1. If your name is *Alice* and you're submitting answers to *Assignment 10*, use `Alice10.pdf` as your filename when submitting.
2. Submit your assignment using the appropriate link below and add the submission date to this Google spreadsheet.[1]

Please let me know if you spot a mistake or if something is unclear or feels suspicious.

[1] The system automatically adds a date-time stamp when you upload it to the OneDrive folder but I didn't want to spend time writing a script to fetch this data into Google sheets.

Assignment 10—BQP=QMA yet PRUs exist and QFHE

- Submission link: OneDrive link for Assignment 10.
- Due: **Tuesday, May 6, 2025** (no extensions)

A. BQP=QMA yet PURs exist

This is based on by Kretschmer (v5 on arXiv) [3]. While there seems to be a gap in one of the steps, let us review what we covered in class anyway.

Exercise 1. The following argument shows that QMA can distinguish PRS from Haar random states. What is wrong with the argument?
QMA protocol:
Arthur holds many copies of $|\psi\rangle$.
Merlin gives the circuit C that produces $|\psi\rangle$ to Arthur.
Arthur does a swap test between $|\psi\rangle$ and $C\,|0^n\rangle$.
If $|\psi\rangle$ is PRS, such a circuit C exists and Merlin can convince Arthur that the state is PRS and not Haar random.

Exercise 2. Pre-requisites. State the following.

1. From §2.2 Probability
   (a) Lemma 5 (Baye's decision rule); also briefly explain how this shows one can't do better than Baye's rule for guessing
   (b) Lemma 6 (Borel-Cantelli); also briefly explain how this result can be seen as a criterion under which at most finitely many events occur with probability 1 (taking X_i to denote whether event i occurs or not).
2. From §2.3 Quantum Information: Fact 7, Fact 8, Lemma 9
3. From §2.4 Haar measure and Concentration:
   (a) Definition of $\mathbb{U}(N)^M$, μ_N^M
   (b) Definition of L-Lipschitz
   (c) Theorem 10
4. From §2.5 Complexity theory
   (a) Definition of a language, a promise problem and the $\mathrm{Dom}(\Pi)$ notation for a promise problem Π
   (b) Definition 11 (Promise BQP) and 11 (PromiseQMA)
5. From §2.6 Quantum Oracles,
   (a) explain how controlled-$\mathcal{U}$ can be viewed as $\mathbb{I} \oplus \mathcal{U}$.
   (b) explain how the 'query cost' is defined for queries $\mathcal{U} = \{\mathcal{U}_n\}_{n\in\mathbb{N}}$.
6. From §2.7 Cryptography
   (a) Definition 16 (Pseudorandom unitary transformations)
   (b) Briefly explain why, in this work, $n(\kappa)$ the number of qubits on which the pseudorandom unitary acts, is taken to be at least $\omega(\log \kappa)$ where κ is the security parameter.

Exercise 3. (2x) This is based on §5 Pseudorandomness from a quantum oracle.

1. From §5.1, define the language $\mathcal{C}$
2. From §5.2 PromiseBQP = PromiseQMA relative to $(\mathcal{U}, \mathcal{C})$
   (a) Lemma 28 and its proof
   (b) Lemma 29 and its proof

Exercise 4. (10x) State and prove Theorem 30; identify the step that has a gap in its justification (we discussed this in class).

Exercise 5. From §5.3 Pseudorandom unitaries

1. State the construction for the PRU ensemble used by the author
2. State Lemma 31
3. (2x) Prove Lemma 31

B. QFHE

The following refers to statements in Appendix A of KLVY '22[2].

Exercise 6. Answer the following

1. Explain informally what is meant by homomorphic encryption.
2. Write down Definition A1.
3. Explain briefly the connection between your informal explanation and the formal definition.

Answer the following, semi-formally, about Mahadev's encryption scheme (as described in Appendix A of [2]).

Exercise 7. Explain the encryption procedure Mahadev uses.

Exercise 8. Explain how the Eval function is implemented for Clifford gates

Exercise 9. Explain why this strategy fails for the Toffoli gate, T, by explicitly writing down the extra factors that appear when one moves a Toffoli past the Pauli pad.

Exercise 10. Explain what additional properties of trapdoor claw-free functions are assumed by Mahadev for implementing Eval for T.

Exercise 11 (3x)**.** Explain how Eval is implemented for T gates.

Assignment 11—Self-testing and Verification

- Submission link: OneDrive link for Assignment 11.
- Due: **Tue, May 6, 2025** (no extensions)

A. Self-testing

The following refers to statements in Section 4 of the review paper by Šupić and Bowles '20 [4].

Exercise 12. Semi-formally, describe what is meant by self-testing.

Exercise 13. Setting up the general strategy

1. Explain how A_x and B_y are defined in terms of projectors and why this is without loss of generality.
2. Show Eq (20), i.e. these observables are Herimitian and unitary.

Exercise 14. Bell operator.

1. Write down the expression for β_{CHSH} and explain how $\langle A_x B_y \rangle$ are to be interpreted.
2. For what choices of $\{A_x\}_x$ and $\{B_y\}_y$ and state $|\psi\rangle$ do we get β_{CHSH} to be $2\sqrt{2}$ (don't need to prove it if you don't feel like it)

Exercise 15. SoS and anti-commutation

1. Explain how the SoS decomposition technique can be used to deduce that $P_\lambda |\psi\rangle = 0$ for all λ where $\beta_Q \mathbb{I} - \mathcal{B} = \sum_\lambda P_\lambda^\dagger P_\lambda$, $\mathcal{B}$ is a Bell operator (see Eq (26)) and β_Q is the maximum quantum value (achieved by $|\psi\rangle$).
2. Use Eq (30) and the argument above, to deduce that $\frac{(A_0 \pm A_1)}{\sqrt{2}} |\psi\rangle = B_{0/1} |\psi\rangle$.
3. Using your answer above, show that B_0 and B_1 anti-commute (simply expand $\{B_0, B_1\} |\psi\rangle$ in terms of $A_0 \pm A_1$).

Exercise 16. Swap Isometry

1. Write down the Swap Isometry Φ as shown in Figure 4 of the paper.
2. Show that this indeed acts the Swap isometry when Z_A, Z_B are taken to be the Pauli z operators and X_A, X_B are taken to be the Pauli x operators, and $|\psi\rangle_{AB}$ is a 2-qubit state.
3. Suppose $Z_A = \frac{1}{\sqrt{2}}(A_0 + A_1), Z_B = B_0, X_A = \frac{1}{\sqrt{2}}(A_0 - A_1), X_B = B_1$.
   (a) Show that $\{Z_A, X_A\} = 0$
   (b) Also show that $\{Z_B, X_B\} |\psi\rangle = 0$
   (c) $Z_A |\psi\rangle = Z_B |\psi\rangle$ and $X_A |\psi\rangle = X_B |\psi\rangle$
4. (5x) For simplicity, suppose Φ is an isometry even for the choice of Zs and Xs we made above. Now, establish that

$$\Phi[|\psi\rangle] = \sum_{i,j\in\{0,1\}} |ij\rangle_{A'B'} \otimes \underbrace{\left(\frac{1}{4} X_A^i (\mathbb{I} + (-1)^i Z_A) X_B^j (\mathbb{I} - (-1)^j Z_B)\right)}_{=:\hat{f}_{ij}} |\psi\rangle_{AB}\,.$$

5. Prove that $\hat{f}_{01} |\psi\rangle = \hat{f}_{10} |\psi\rangle = 0$.
6. Prove that $\hat{f}_{11} |\psi\rangle = \hat{f}_{00} |\psi\rangle$.
7. Explain how existence of Φ shows that one can self-test the Bell state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ (be consistent with your answer to ??).

B. Verification

This last part is based on Grilo '20 [1].

Exercise 17. Background/Self-testing. State the following.

1. Lemma 1 and also explain the magic square game
2. Pauli Braiding Test (as written in Figure 1)
3. Theorem 2

Exercise 18. Background/Local Hamiltonian problem. State the following.

1. Describe what is meant by a local hamiltonian problem
2. Definition 3 (XZ Local Hamiltonian)
3. Lemma 4 (QMA completeness of XZ local hamiltonians)
4. Lemma 5 (amplifying soundness/completeness of XZ Local Hamiltonians)
5. Definition 6 (What is meant by non-local games for Local Hamiltonians)

Exercise 19. Write down the protocol in Figure 2 and intuitively (to the extent reasonable) explain what is going on.

Exercise 20. (3x) State and prove Lemma 7 (bound on max winning probability of semi-honest strategies).

Exercise 21. (3x) State and prove Lemma 8 (bound on general strategies)

Exercise 22. (3x) State and prove Theorem 9 (uses Lemma 7 and Lemma 8 to satisfy Definition 6; then amplifies the soundness/completeness gap)

Exercise 23. State Corollary 9.

References

[1] Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round, 2020.

[2] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game, 2022.

[3] William Kretschmer. Quantum pseudorandomness and classical complexity. 2021.

[4] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020.