Quantum Aspects of Cryptography

Assignments 8 and 9—Haar measure and Commitments from PRSGs
(topics from Lectures 17, 18, 19 and 20)
Version: $\alpha.1$—April 1, 2025

Instructions. Same as those in previous assignments (including the updates since Assignment 5) except that the *end-sem exam* 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 8*, use `Alice8.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 8—Haar Randomness

Simple assignment, mostly about writing down a bunch of results from [2] we covered in class. Should mostly require you to fill in the gaps in your class notes.

- Submission link: OneDrive link for Assignment 8.
- Due: Thursday, **April 10, 2025**

Statement numbers below are referencing the corresponding statements in [2].

Exercise 1. State and prove (when applicable) the following.

1. Definition 1 (Haar measure)
2. Proposition 2 ($\mathbb{E}[U^{\otimes k_1} \otimes U^{*\otimes k_2}] = 0$ whenever $k_1 \neq k_2$)
3. Proposition 3 ($\mathbb{E}[f(U^\dagger)] = \mathbb{E}[f(U)]$)

Exercise 2. State and prove (when applicable) the following

1. Definition 4 (kth Moment operator $\mathcal{M}^{(k)}$) and Definition 5 (Commutant).
2. Lemma 6 (numbered as follows)
   (a) $\mathcal{M}^{(k)}$ is linear, trace-preserving and self-adjoint wrt Hilbert-Schmidt inner product
   (b) $\mathcal{M}^{(k)} \in \mathrm{Comm}(\mathrm{U}(d), k)$
   (c) If $A \in \mathrm{Comm}(\mathrm{U}(d), k)$, then $\mathcal{M}^{(k)}(A) = A$
3. Theorem 7 ($\mathcal{M}^{(k)}(O) = \sum \langle P_i, O\rangle_{HS} P_i$ where $P_1 \dots P_{\dim(\mathrm{Comm})}$ is an orthonormal basis (wrt Hilbert Schmidt norm) of $\mathrm{Comm}(\mathrm{U}(d), k)$).

Exercise 3. State and prove (when applicable) the following.

1. Definition 8 (Permutation operators). Why does the paper use π^{-1} in Eq 23 (in ...) according to you?
2. Theorem 9 (Schur Weyl duality) $\mathrm{Comm}(\mathrm{U}(d), k) = \mathrm{span}(V_d(\pi) : \pi \in S_k)$
3. Theorem 10 (Computing moments) $\mathbb{E}[U^{\otimes k} O U^{\dagger \otimes k}] = \sum c_\pi(O) V_d(\pi)$ and give a system of equations using which $c_\pi(O)$ can be computed
4. Proposition 11 $\{V_d(\pi)\}_{\pi \in S_k}$ are linearly independent if $k \leq d$ and linearly dependant if $k > d$.

Exercise 4. State and prove (when applicable) the following.

1. Definition 12 (Identity and Flip operators on 2 systems). Also show that $\mathsf{tr}((A \otimes B)\mathbb{F}) = \mathsf{tr}(AB)$.
2. Corollary 13 (first and second moment) Express $\mathbb{E}(UOU^\dagger)$ and $\mathbb{E}(U^{\otimes 2} O U^{\dagger \otimes 2})$ in terms of the identity and flip operators.
3. Example 14 (establish the Schur-Weyl for the $k = 1$ and $k = 2$ case).

Exercise 5 (Symmetric subspace.)**.** State and prove (when applicable) the following.

1. Definition 15 (Defines $\mathrm{Sym}_k(\mathbb{C}^d)$) and also define $P_{\mathrm{sym}}^{(d,k)}$ as in Eq (66).
2. Theorem 16 (P_{sym} is an orthogonal projector onto Sym_k).
3. Theorem 17 (Dimension of Sym_k is $\begin{pmatrix} k+d-1 \\ k \end{pmatrix}$).

Exercise 6 (Anti-symmetric subspace (this we did not cover in class))**.** State and prove (when applicable) the following.

1. Definition 18 (Defines $\mathrm{ASym}_k(\mathbb{C}^d)$) and also define $P_{\mathrm{asym}}^{(d,k)}$.
2. Theorem 19 (P_{asym} is an orthogonal projector onto ASym_k).

3. Proposition 20 (Dimension of $\mathrm{ASym}_k$is $\begin{pmatrix} d \\ k \end{pmatrix}$).

Exercise 7. Final connections. Show the following.

1. $P_{\mathrm{asym}}^{\dagger} P_{\mathrm{sym}} = 0$ and $(\mathbb{C}^d)^{\otimes 2} = \mathrm{Sym}_2(\mathbb{C}^d) \oplus \mathrm{ASym}_2(\mathbb{C}^d)$.
2. Theorem 22 ($\left[U^{\otimes k} \left|\phi\right\rangle \left\langle\phi\right|^{\otimes k} U^{\dagger \otimes k}\right] = P_{\mathrm{sym}} / \mathsf{tr}(P_{\mathrm{sym}})$.

Assignment 9—PRSG $\implies$ Commitments

This is based on the 'pre-recorded' lecture which covers the commitment scheme in [3]. Please reach out if something is unclear in the lecture or the questions below.

- Submission link: OneDrive link for Assignment 9.
- Due: Thursday, **April 14, 2025**

Exercise 8. Informally explain Naor's classical commitment scheme and argue security. How is the construction in [3] a generalisation of Naor's classical commitment scheme?

Exercise 9 (Prior notions and Definitions)**.** State and prove (when applicable) the following.

1. State Lemma 2.1 (Quantum one-time pad) and prove it for the single qubit case, i.e. $m = 1$ by explicit calculation.
2. State Definition 2.1 (Pseudorandom quantum state generators (PRSGs))
3. Explain Remark 2.1 (about assuming PRSGs are pure without loss of generality)
4. State Definition 2.2 (Single-copy-secure PRSGs)
5. Briefly summarise Remarks 2.2, 2.3, 2.4 and 2.5 (can be long if you like but it is not needed).

Exercise 10. Write down the following definitions and briefly justify (where sensible) them.

1. Definition 3.1 (Non-interactive quantum commitments (syntax))
2. Definition 3.2 (Perfect correctness)
3. Definition 3.3 (Computational hiding)
4. Definition 3.4 (Statistical sum-binding)

Exercise 11 (Construction)**.** Answer the following.

1. Describe the construction in Section 3.2.
2. Explain Remark 3.1 (how the reveal phase can be entirely classical) and briefly state Remark 3.2 (the security proof also works for PRSGs that use auxilliary qubits)

Exercise 12 (Computational Hiding)**.** Answer the following.

1. State Theorem 3.1 (computational hiding of the construction in Section 3.2) and write out the three hybrids (i.e. Hybrid 0, 1 and 2) described in the proof.
2. State and prove Lemma 3.1 (i.e. Hybrid 0 and 1 behave essentially the same)
3. State and prove Lemma 3.2 (i.e. Hybrid 1 and 2 behave essentially the same)
4. Prove Theorem 3.1 using Lemma 3.1 and 3.2.

Exercise 13 (Statistical Binding)**.** Answer the following.

1. State Theorem 3.2 (statistical sum-binding) and write down all the properties of Fidelity that are used in the proof.
2. Write down the proof of the Theorem 3.2.

Research Areas To the best of my knowledge, while commitments to quantum states has only recently been formalised (see [1]), classical commitments to quantum states are still not fully understood. There is also the question of building such primitives from other candidate minimal assumptions.

References

[1] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. Commitments to quantum states. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1579–1588, New York, NY, USA, 2023. Association for Computing Machinery.

[2] Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner's tutorial. *Quantum*, 8:1340, May 2024.

[3] Tomoyuki Morimae and Takashi Yamakawa. *Quantum Commitments and Signatures Without One-Way Functions*, page 269–295. Springer Nature Switzerland, 2022.