Public-key pseudoentanglement and the hardness of learning ground state entanglement structure

Adam Bouland[*1], Bill Fefferman[†2], Soumik Ghosh[‡2], Tony Metger[§3], Umesh Vazirani[¶4], Chenyi Zhang[‖1], and Zixin Zhou[**1]

[1]Stanford University
[2]University of Chicago
[3]ETH Zurich
[4]UC Berkeley

Abstract

Given a local Hamiltonian, how difficult is it to determine the entanglement structure of its ground state? We show that this problem is computationally intractable even if one is only trying to decide if the ground state is volume-law vs near area-law entangled. We prove this by constructing strong forms of pseudoentanglement in a public-key setting, where the circuits used to prepare the states are public knowledge. In particular, we construct two families of quantum circuits which produce volume-law vs near area-law entangled states, but nonetheless the classical descriptions of the circuits are indistinguishable under the Learning with Errors (LWE) assumption. Indistinguishability of the circuits then allows us to translate our construction to Hamiltonians. Our work opens new directions in Hamiltonian complexity, for example whether it is difficult to learn certain phases of matter.

[*]abouland@stanford.edu
[†]wjf@uchicago.edu
[‡]soumikghosh@uchicago.edu
[§]tmetger@ethz.ch
[¶]vazirani@eecs.berkeley.edu
[‖]chenyiz@stanford.edu
[**]jackzhou@stanford.edu

Contents

1 Introduction

The central problem in Hamiltonian complexity is to understand the structure of ground states of local Hamiltonians and the difficulty of learning properties of them, e.g. [Has07, SCV08, LVV15, ALVV17, AA23]. In this work we study the following question: given a local Hamiltonian H, how difficult is it to learn about the entanglement structure of its ground state? For example, given H, can you tell if its ground state is area-law or volume-law entangled? We call such questions about the qualitative features of the entanglement structure a *Learning Ground State Entanglement Structure* (LGSES) problem. This problem is related to both condensed matter physics – where ground state entanglement structure is a central object of study – and may also shed light on questions in quantum gravity regarding how entanglement could possibly be dual to other physical quantities [BFV19, GH20].

Whereas most effort in many-body physics has been directed towards the positive side of this question, i.e. finding conditions under which properties of the ground state can be efficiently learnt or computed (see e.g. [CPF+10, LVV15, HKT+22]), here our goal is to prove hardness results for the LGSES problem from cryptographic assumptions. This explores the limitations that any algorithm for such problems must run up against. In other words, hardness results for the LGSES problem point to qualitative features of Hamiltonian ground states that are inherently computationally intractable to compute.

To prove computational hardness results for the LGSES problem, we will relate it to a notion called *pseudoentanglement*, a term recently introduced in [ABF+23]. Informally, pseudoentangled state ensembles consist of low-entanglement states that masquerade as high-entanglement states to computationally bounded observers; in other words, a pseudoentangled state only looks like a high-entanglement state to bounded observers, whereas its actual (information-theoretic) entanglement is low. The main result of [ABF+23] is that it is possible to create pseudoentangled states which hide vast differences in entanglement. More concretely, they construct two ensembles of quantum states, Ψ^{high} and Ψ^{low}, such that any state $|\psi\rangle \in \Psi^{\text{high}}$ has high entanglement entropy across any bipartition of the qubits and states in Ψ^{low} have low entanglement, but any computationally bounded quantum algorithm that receives a state from $\Psi^{\text{high}} \cup \Psi^{\text{low}}$ cannot tell which kind of state it received.

This notion of pseudoentanglement is interesting in its own right and has been used for various applications in [ABF+23], but its relevance to Hamiltonian complexity is unclear. This is because the settings are inherently different: the notion of pseudoentanglement in [ABF+23] involves a *quantum* input, namely copies of the relevant quantum states, being given to the distinguisher. If we tried to translate this into a setting involving Hamiltonian ground states, we would end up in a model where we study the properties of Hamiltonian ground states given quantum copies of these ground states, but without knowing the actual Hamiltonian itself. In contrast, in Hamiltonian complexity we assume that we know a classical description of the Hamiltonian under consideration and would like to determine properties of its ground state.

Therefore, if we want to use some notion of pseudoentanglement to prove hardness results for the LGSES problem, we need to consider a model where the distinguisher is not just given quantum copies of the high- or low-entanglement states, but rather an efficient classical description of these states. This leads to a different kind of pseudoentanglement, which we call *public-key* pseudoentanglement since the description of the states (the "key") can be made public. This notion is already implicit in earlier work by Gheorghiu and Hoban [GH20], who gave a construction of public-key pseudoentanglement that we discuss in more detail below.

Definition 1.1 (Public-key pseudoentanglement (implicit in [GH20]))**.** Two ensembles of n-qubit $\text{poly}(n)$-gate quantum circuits $\{C_k\}$, $\{C'_k\}$ are public-key pseudoentangled with entanglement gap $f(n)$ vs $g(n)$ if they are computationally indistinguishable to poly-time quantum algorithms, and yet with high probability

over the ensembles, $C_k|0^n\rangle$ has entanglement $\geq f(n)$ and $C'_k|0^n\rangle$ has entanglement $\leq g(n)$ across one or more cuts of the system.

The key difference between this definition and the one in [ABF+23] is that here a classical description of the circuit used to prepare the states is given as input to the distinguisher, whereas in [ABF+23] the distinguisher only receives copies of the output state of the circuit. A distinguisher can therefore not only prepare copies of the output state, but also analyse the classical description of the circuits directly to gain additional information, making it harder to "hide" the entanglement of pseudoentangled states. Hence, public-key pseudoentanglement is a much stronger notion than that in [ABF+23], which we will call *private-key* pseudoentanglement as the circuits are hidden.

There are generally two features we care about in a pseudoentanglement construction: the entanglement gap, which we want to be as large as possible in order to hide as much entanglement as possible, and the set of cuts across which this entanglement gap holds. Informally, a more general set of cuts (i.e. bipartitions of the qubits) across which the entanglement gap holds corresponds to hiding more qualitative information about the entanglement structure of the state; this is what we are most interested in for the LGSES problem.

The pioneering work of Gheorghiu and Hoban gave the first pseudoentanglement construction with entanglement gap n vs $n - O(1)$ across a single cut based on the Learning With Errors (LWE) assumption [GH20]. Using this they showed that it is difficult to learn *fine-grained* properties of the ground state entanglement – namely if the ground state has entanglement n vs $n - O(1)$ across a fixed cut. The basic idea is that if one passes the circuit to prepare pseudoentangled states through a modified Kitaev clock construction [KSV02, NVY18], the ground state of the resulting Hamiltonian has the same entanglement properties as the output state of the circuit. We emphasize that the Kitaev clock Hamiltonian encodes the circuit used to prepare the state in plaintext, so this application necessarily requires a *public-key* construction.

However, Gheorghiu and Hoban's construction only suffices to prove hardness of detecting very small differences in the entanglement of the ground state across a single cut. In contrast, the LGSES problem asks about *qualitative* or *coarse-grained* features of the entanglement structure, as very fine-grained properties are usually not physically relevant. This raises the following question: is it possible to get a public-key pseudoentanglement construction that hides qualitatively different entanglement structures? This would lead to natural hardness statements for the LGSES problem.

1.1 Near area-law public-key pseudoentanglement

Our first result is to construct strong forms of public-key pseudoentanglement from LWE. In particular we show it is possible to hide 1D near area-law vs volume-law entanglement.

Theorem 1.2 (Volume vs area-law public-key pseudoentanglement (informal))**.** *Assuming subexponential-time hardness of LWE, there exist public-key pseudoentangled ensembles with volume-law vs near area-law entanglement when the qubits are arranged on a 1D line.*

That is, in one case the states have entanglement $\Omega(\min(k, n-k))$ across any division of the qubits into k vs $n-k$ qubits (volume-law), and in the other case the entanglement of any cut is $\leq |A|\text{polylog}(n)$ where $|A|$ is the area of the cut when the qubits are arranged on a 1D line (i.e. the number of times the cut crosses the 1D line). We call this *near area-law entangled*. This is optimal because if the polylog factor were changed to a log, then these states would be efficiently distinguishable from one another by standard Matrix Product State learning algorithms [CPF+10, LVV15]. Hiding such qualitatively different entanglement structures requires a completely different construction from [GH20]. We note that while in Theorem 1.2 we assume subexponential-time hardness of LWE, we also show that the standard LWE assumption implies a similar

result.[1] We will discuss the application of our result to Hamiltonian complexity shortly, after we present its proof sketch.

Proof sketch for single-cut pseudoentanglement. Let us first consider a single cut partitioning the qubits into sets A and B. In this case, the most natural states to consider are of the form $\sum_{x\in\{0,1\}^n} |x\rangle_A |h(x)\rangle_B$ for some function h. If one chooses h to be injective, then this state has entanglement entropy n across this cut; if one chooses h to be 2^k-to-1, then the entanglement is $n-k$. [GH20] used exactly these states with trapdoor claw-free functions from [BCM+18], which are functions that are either injective or 2-to-1, but the two cases are computationally hard to distinguish (given a description of the function) assuming the hardness of LWE. There are some additional subtleties arising from the fact that the trapdoor claw-free functions from [BCM+18] do not output numbers, but probability distributions, and are only approximately 2-to-1. We refer to [GH20] for a detailed analysis of this construction.

To increase the entanglement gap, we need to make the many-to-1 functions *more compressing*. The functions in [GH20, BCM+18] additionally have a trapdoor; however, we observe that for pseudoentanglement, we can dispense with the trapdoor and only need so-called *lossy functions*: these are functions that are either injective or 2^k-to-1, but again the two kinds of functions are hard to distinguish. Starting from this observation, it turns out to be possible to combine the construction from [GH20] with ideas from a recent randomness generation protocol [MVV22] to achieve an entanglement gap of n vs n^δ for any $\delta > 0$.[2]

The challenge with this approach based on [GH20] is that it appears fundamentally restricted to a single cut. However, our goal is to obtain pseudoentangled states with near area-law vs volume-law entanglement structure, which requires low entanglement across *exponentially many cuts* simultaneously. This would require controlling the entanglement not just between regions A and B, but also within these regions. With the approach of [GH20] it seems difficult to appropriately modify the state in register A without jeopardising the entanglement across the cut between A and B.

For this reason, we need a different kind of state that allows us to control the entanglement across all cuts simultaneously. It turns out that a useful class to consider are binary phase states as in [JLS18, BS19, ABF+23], i.e., states of the form $\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle$. Our approach will be as follows: we start from a phase state with high-entanglement across every cut. We will then modify this state (in a computationally undetectable way) to have low entanglement across some particular cut. This achieves the essentially same as the [GH20]-based construction above.[3] However, crucially our "modification procedure" is iterable: this means that we can perform essentially the same entanglement reduction operation across many cuts in sequence and end up with a state with low entanglement across every cut.

We first describe the construction and proof for a single cut. For simplicity, let us first consider the cut between the first and second $n/2$ qubits. One can easily compute that the reduced density matrix of the first half of the state is $\rho \propto TT^\top$ where $T_{ij} = (-1)^{f(i\|j)}$ and $i, j \in \{0,1\}^{n/2}$ are the first and second halves of the string x, i.e., T is the truth table of the function f written out in a matrix form. By a direct calculation, one can show an upper bound on the entanglement entropy of our phase state (i.e. the von Neumann entropy of ρ) in terms of the rank of T, and a lower bound on the entanglement entropy in terms of the Frobenius norm of $TT^\top$. Our strategy will therefore be to start from a "T-matrix" for a high-entanglement state, and then

[1] In particular, the polylog correction factor to the area-law scaling is replaced by an n^ϵ correction, where ϵ can be any constant > 0.

[2] We note that independently from and simultaneously to our work, Gheorghiu and Hoban updated their results to include a construction of this form, which achieves the aforementioned gap of n^δ vs n across a fixed cut with n qubits in one set and $\mathrm{poly}(n)$ in the other.

[3] One advantage of this construction even for a single cut is that it allows an entanglement gap of n vs $\mathrm{poly}\log n$ for an $O(n)$-qubit state, whereas in the [GH20]-based construction the B-register had to have $\mathrm{poly}(n)$ qubits for a comparable entanglement gap.

perform one of two modifications in a computationally indistinguishable way: either modify T to reduce its rank to get low-entanglement states, or modify T in a way that does *not* reduce $\left\|TT^\top\right\|_2$ too much so that the entanglement of the states remains high. These modified T-matrices then correspond to modified phase states, and our goal is to hide which of the two procedures we performed, even when handing out a classical description for preparing the corresponding states.

In [ABF+23] the idea is to apply a private key cryptographic hash function to repeat rows of the matrix T to reduce its rank. That is, we pick a phase function $f(x)$ which yields high entanglement [BS19], and then "whittle down" its entanglement by replacing $f(x)$ with $f(h(i)j)$ where $i,j \in \{0,1\}^{n/2}$ and $h : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is a 2^k-to-1 function. This reduces the number of distinct rows in T (each of which is now repeated many times) and correspondingly decreases the rank of T. As a result, this procedure lowers the entanglement of ρ by k. On the other hand, if we pick h to be a 1-to-1 function, we simply permute the rows of T and do not change $\left\|TT^\top\right\|_2$. To make this public-key, we need a way of applying a 2^k-to-1 or a 1-to-1 hash function to these phase states in such a way that it is hard to tell which one was applied, even when the state preparation circuit (and therefore the source code for h) is public.

At first sight, it may seem that we can use the same idea as above: take the lossy functions from [MVV22] and use them to reduce the rank of T. However, the phase state construction is much less flexible than states of the form $\sum_x |x\rangle|h(x)\rangle$: for the latter, the codomain of h does not matter and we can use the functions h from [MVV22], whose codomain are probability distributions over $\mathbb{Z}_q^m$ for $m \gg n$. In contrast, for phase states we need lossy functions $h : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, i.e. the codomain has to be the same as the domain. This is a somewhat unusual requirement from a cryptographic perspective and forces us to use a custom construction of "imperfect" lossy functions based on LWE. Concretely, we first show how to create lossy functions mapping $\{0,1\}^{n/2} \to \{0,1\}^{\mathrm{poly}(n)}$ which are *exactly* injective vs 2^k-to-1 (for sufficiently large k) with high probability. This is not yet what we need, as the codomain is exponentially larger than the domain. To fix this, we compose these functions with pairwise independent hash functions which shrink the codomain size back to $2^{n/2}$. This can only make the 2^k-to-1 functions more compressing, which is to our benefit. However, this also introduces unwanted collisions for the injective functions which might break the high-entanglement case. To deal with this, we show that the repetition pattern this produces in the matrix T is sufficiently well-behaved that the corresponding states still have high entanglement. Intuitively, this holds because even though the "injective" functions or no longer actually injective, they are still pairwise independent, which ensures enough independence in the row repetition pattern of T to give a strong lower bound on the Frobenius norm $\left\|TT^\top\right\|_2$.

From single-cut to multi-cut pseudoentanglement. As we mentioned, the advantage of the above construction is that it can be extended to pseudoentanglement across all cuts simultaneously. We now explain how this extension works at a high level. A first observation is that to achieve pseudoentangled states with 1D near area law scaling, reducing the entanglement across all $n-1$ contiguous cuts of the line to $O(\mathrm{polylog}(n))$ suffices by strong subadditivity. Therefore, a natural approach is to perform a 1D sweep of the line, reducing the entanglement of the contiguous cuts one at a time. For reasons that will become apparent below, we perform this sweep right-to-left. The final phase function is then a complicated composition of n independent lossy functions and hash functions.

To show that this construction indeed achieves pseudoentanglement across all cuts simultaneously, we need to worry about two issues: firstly, for the low entanglement states we need to ensure that performing the entanglement reduction operation for a cut towards the left of the line does not inadvertently increase the entanglement across earlier cuts to the right, so that the low entanglement across those earlier cuts is preserved. Secondly, for the high entanglement states we need to make sure that the fact that we are using

"imperfect" injective functions does not decrease the entanglement too much even after applying these functions across every cut.

The first concern is relatively easy to deal with due to the relationships between the "T-matrices" for different cuts. To see this, consider a phase state $|\psi\rangle = \sum(-1)^{f(x)}|x\rangle$ on $n+m$ qubits on a line and let $T^{n|m} \in \{\pm 1\}^{2^n \times 2^m}$ be the T-matrix for the cut between the first n and last m qubits, i.e. $T^{n|m}_{ij} = (-1)^{f(i\|j)}$ for $i \in \{0,1\}^n, j \in \{0,1\}^m$. After performing the entanglement reduction operation, this matrix will only have some smaller number R of distinct rows, each repeated many times. In the next step of the sweep (recalling that we move right to left), we consider the cut between the first $n-1$ and last $m+1$ qubits. We denote the corresponding T-matrix by $T^{n-1|m+1} \in \{\pm 1\}^{2^{n-1}\times 2^{m+1}}$. From the definition of the T-matrix, one can see that the first row of $T^{n-1|m+1}$ simply consists of the first two rows of $T^{n|m}$ stacked side by side. More generally, the i-th row of $T^{n-1|m+1}$ is simply the horizontal concatenation of rows $2i-1$ and $2i$ from $T^{n|m}$. Suppose we now reduce the rank of $T^{n-1|m+1}$ by removing some rows and duplicating others. We then need to check that if we go back to the cut $n|m$, the resulting T-matrix (denoted $\tilde{T}^{n|m}$) still has rank at most R. This is the case since the rows of $\tilde{T}^{n|m}$ consist of the first and second parts of the rows of $T^{n-1|m+1}$; since the rank reduction only repeats, but does not modify, rows in $T^{n-1|m+1}$, every row in $\tilde{T}^{n|m}$ must have already appeared in $T^{n|m}$. As a result, the subsequent rank reduction for cut $n-1|m+1$ can only decrease, not increase, the rank of the T-matrix across $n|m$. It is not too hard to see that this argument generalises to any future rank reduction operation, not just the immediately subsequent one.

The second concern is more difficult to deal with. When applying this sweep with *approximately* injective functions, the entanglement is reduced slightly each time. The rightmost (first) cut in particular has its entanglement reduced n times, so even a tiny loss could kill the entire construction. Perhaps surprisingly, we show that this is not the case, and the entanglement losses do not compound too badly. We show that different rows have different probabilities of being hashed together due to the structure of the sweep, and a careful accounting of this process reveals that not much entanglement is lost, even in the first cut. The analysis is somewhat technical and we refer to Section 3.3 for details. Finally, we note that while the construction we described here does not produce pseudorandom states ensembles (i.e. the families of pseudoentangled states, without the public key, are not necessarily pseudorandom states [JLS18]), we can make a simple modification to our construction to ensure that this is the case. Since our applications do not rely on this we only give a sketch of this in Section 3.3.3.

1.2 Hardness of learning ground state entanglement structure

Our second result is to show that this public-key, area vs volume-law pseudoentanglement construction enables new applications in quantum Hamiltonian complexity. Because our public-key pseudoentanglement construction can hide qualitative features of the entanglement structure, we can show natural results for the hardness of the Learning Ground State Entanglement Structure (LGSES) problem for broad differences in entanglement structure. As we mentioned above, the main idea for turning pseudoentanglement constructions into hard instances of LGSES is to use a circuit-to-Hamiltonian construction on the state preparation circuit for the pseudoentangled state. There are a variety of circuit-to-Hamiltonian constructions and using these on our pseudoentangled states yields a variety of hardness statements for LGSES. In this paper, we consider three different constructions: a Kitaev clock construction with a binary clock, a Kitaev clock construction with a unary clock, and a customised version of a geoemtrically local 2D construction [AVDK$^+$08]. As we discuss in Section 1.4, an interesting open problem is whether a custom circuit-to-Hamiltonian construction that is focused purely on preserving entanglement structure (rather than QMA-hardness) can produce hard instances of the LGSES problem for more physically natural Hamiltonians.

Using a Kitaev clock construction with a binary clock [KSV02], we get the following result (see Theorem 4.2 for the formal statement).

Theorem 1.3 (informal)**.** *Assuming subexponential-time hardness of LWE, LGSES is intractable when the input Hamiltonian is $O(\log n)$-local on n qubits, and the goal is to decide whether the ground state is volume-law or near area-law entangled for the qubits arranged on a 1D line.*

This result follows relatively straightforwardly from the standard Kitaev clock construction. There are only two issues that need to be addressed: firstly, the ground state of the Hamiltonian in the Kitaev clock construction is the history state of the circuit, not the output state. However, our pseudoentanglement construction only provides guarantees on the entanglement structure of the output state. This problem can be addressed using a "padding trick" [NVY18]: we can simply pad the pseudoentanglement circuit with a large (polynomial) number of identity gates at the end. This will ensure that the history state has most weight on the output state. Using continuity properties of the von Neumann entropy, this implies that the history state has the desired entanglement structure, too. The second issue is that we have no control over the entanglement within the clock register of the Hamiltonian. However, this does not matter for the coarse-grained entanglement structure of the state: since the clock register only has logarithmically many qubits, discarding it only changes the entanglement by $O(\log n)$, which is irrelevant for our $O(\mathrm{poly}\log n)$ vs $\Omega(n)$ entanglement gap.

The Hamiltonian in Theorem 1.3 does not achieve constant locality because the Hamiltonian terms acting on the binary clock register require locality $\log n$. By using a unary clock instead of a binary clock, we can make the Hamiltonians in Theorem 1.3 have constant locality [KSV02]. This is also what was used in [GH20] to study a Hamiltonian version of their entropy difference problem. However, the clock register now has $\Theta(n)$ qubits, and because it has so many qubits, the analysis from Theorem 1.3 no longer yields the desired entanglement gap. However, if we trace out the clock register and measure entanglement of the remaining mixed state by any operational mixed-state entanglement measure, we show that we still recover a maximal entanglement gap across any cut. Intuitively, this is because due to the padding trick, after tracing out the clock register the remaining mixed state is close in trace distance to the (pure) output state of the pseudoentanglement circuit. We refer to Theorem 4.4 for the formal statement.

The main downside of the Kitaev clock construction is that the resulting Hamiltonian is not *geometrically* local, i.e. even though we imagine the qubits as arranged on a 1D line in order to talk about area and volume law entanglement, the Hamiltonian itself has no inherent 1D geometrical structure. In contrast, most physical Hamiltonians are geometrically local. To obtain hard instances of the LGSES problem for geometrically local Hamiltonians we can use a more sophisticated 2D clock construction, where we account for time across one of the spatial dimensions instead of needing to add extra clock qubits to the circuit. We first state the resulting hardness statement for LGSES informally and then briefly sketch the proof. We refer to Theorem 4.19 for the formal statement and Section 4.3 for details of the construction.

Theorem 1.4. *Assuming subexponential-time hardness of LWE, LGSES is intractable when the input Hamiltonian is* geometrically local *on a 2D grid of $n \times \mathrm{poly}(n)$ qudits with constant local dimension $d = O(1)$, and the goal is to decide whether the ground state has entanglement scaling* $\mathrm{polylog}(n)$ *or n across horizontal cuts.*

At a high level, the construction of the 2D geometrically local case is similar to before: we take padded versions of our pseudoentanglement circuits and convert them to local Hamiltonians using a 2D circuit-to-Hamiltonian construction [AVDK+08]. This circuit-to-Hamiltonian construction produces a geometrically local Hamiltonian by dispensing with an explicit clock register. As a result, the ground state also does not

have a clock register and is instead of the form $\sum_t V_t|\psi_t\rangle$ (with normalization), where $|\psi_t\rangle$ is the state of the circuit after time step t and V_t are isometries such that $V_t^\dagger V_{t'} = 0$ for any $t \neq t'$. In other words, similarly to the Kitaev clock construction, the ground state of the Hamiltonian has the form of a history state, with different time steps encoded in mutually orthogonal states. Since we padded the circuit with identities, we can approximate this ground state by $\sum V_t|\psi_{\text{out}}\rangle$ with $|\psi_{\text{out}}\rangle$ the output state of our pseudoentanglement circuit.

The challenge in bounding the entropy of the reduced states of this "history state" is that the different time steps are encoded in different bases, specified by the isometries V_t. This is in contrast to the Kitaev construction, where the intermediate states are all encoded in the same basis. As a result, when we trace out part of the state $\sum V_t|\psi_{\text{out}}\rangle$, we get a state that looks very different from just the reduced state of $|\psi_{\text{out}}\rangle$. With the construction of [AVDK+08], we do not know how to bound the entanglement of these reduced states.

We therefore need to modify the construction from [AVDK+08] to gain better control over the entropy of these reduced states. We do this by increasing the local dimension of the qudits in order to better keep track of different steps of the circuit execution. With this modified construction, we can ensure that reduced states of different $V_t|\psi_{\text{out}}\rangle$ corresponding to different phases of the circuit execution are, in a certain sense, "cutwise" orthogonal (see Lemma 4.15 for details). The overall reduced state is now a sum of different "orthogonal" reduced states, each corresponding to a different phase of the circuit execution. We can compute the entropy of each of these individual reduced states relatively easily from the entanglement properties of our pseudoentangled states. Using cutwise orthogonality allows us relate the entropy of the overall state to the entropies of the individual reduced states that we sum over (Lemma 4.13). As a result, we can compute the entropy of the overall reduced state even though all the different time steps are encoded in different bases.

1.3 Related work

We have already given a detailed discussion of the work of Gheorghiu and Hoban [GH20], which introduced the idea of public key-pseudoentanglement and gave the first construction, and the work of Aaronson et al. [ABF+23], which coined the term pseudoentanglement and gave a private-key construction with maximal entanglement gap across any cut.

The main motivation in [GH20] was to provide a hardness result for the so-called (quantum) entropy difference problem: given two (quantum) circuits, decide whose output has more entropy when acting on a uniformly random input. If the circuit depth is polynomial, these problems are known to be complete for the complexity classes QSZK and SZK, respectively [GV99, BASTS08]. Gheorghiu and Hoban showed that for constant-depth circuits with unbounded fan-out or logarithmic-depth circuits with constant fan-out, both the QED and ED problems are still at least as hard as breaking LWE. In their proof, the entropy difference between the high- and low-entropy circuits was a single bit. Our improved pseudoentanglement construction implies that both ED and QED remain LWE-hard with large entropy gaps.[4] This is similar in spirit to the classical result that SZK gaps can be amplified [SV03].

Recently, independent and complementary work of Arnon-Friedman, Brakerski, and Vidick [AFBV23] gave a new definition of pseudoentanglement. Their definition is private-key and is natural in the context of operational tasks in quantum Shannon theory. Consequently, they focus on operational mixed-state en-

[4]This result only requires our single-cut pseudoentanglement construction, for which the depth can be made logarithmic as in [GH20]. In fact, as mentioned earlier, an independently updated version of [GH20] also achieves single-cut pseudoentanglement with a large gap, implying the same hardness result for the (Q)ED problem that we obtain from our construction, although their circuits have poly(n) output qubits for an entropy gap of n^δ vs n, whereas ours only have $O(n)$ output qubits, i.e. achieve a larger relative gap. We refer to [GH20] for a more detailed analysis.

tanglement measures across a single cut and require their states to be efficiently preparable under LOCC. In contrast in our work we focus on creating *public-key* pseudoentanglement with different large-scale geometrical structures, which is driven by our applications in Hamiltonian complexity.

Finally, we discuss the relationship between the LGSES problem and existing algorithms for properties of ground states. While the physics literature on computing properties of ground states is too vast to survey here, we highlight two results closer to computer science. First, in [LVV15] the authors provide a polynomial-time algorithm that, given a classical description of a one-dimensional geometrically local Hamiltonian with constant spectral gap, outputs an MPS description of the ground state. Therefore 1D constant gapped geometrically local Hamiltonians cannot "hide" anything about their ground state entanglement structure. We note that this algorithm cannot be used on the Hamiltonians we construct in this paper as they are neither 1D geometrically local nor have constant spectral gap. Therefore our results limit potential further improvements to their algorithm. Second, the recent result [HKT+22] considers the problem of distinguishing phases of matter given labelled examples of states in different phases. The authors show that if there is a constant spectral gap and the separation between the phases is sufficiently well-conditioned[5], then a classical algorithm can efficiently learn to distinguish between the phases using information from only few-body measurements. In condensed matter physics, different qualitative entanglement structures are often associated with different quantum phases of matter; therefore our result also limits potential further improvements to such algorithms, i.e. it is not possible to relax some of their assumptions e.g. to gapless phases. An interesting direction for future work is to make our pseudoentanglement Hamiltonians "more physical" to be closer to the assumptions of theses algorithmic settings. This would help to better delineate the boundary between tractability vs intractability of learning properties of ground states of local Hamiltonians.

1.4 Discussion and open questions

In this work, we have introduced and studied the Learning Ground State Entanglement Structure (LGSES) problem: given a classical description of a local Hamiltonian, determine qualitative properties of the entanglement of its ground state, e.g. whether it is area-law or volume-law entangled. To prove hardness results for this problem, we have related it to a notion that we call public-key pseudoentanglement: low-entanglement states that are computationally indistinguishable from high-entanglement states even when given the state preparation circuit. Our main technical contribution is to construct public-key pseudoentanglement with (near) area-law vs volume-law scaling assuming the hardness of LWE.

Psedoentanglement is a relatively new idea with many avenues for future work. We suggest three main directions: (i) improving pseudoentanglement constructions themselves, (ii) strengthening the link between pseudoentanglement and condensed matter physics, and (iii) applications of pseudoentanglement beyond Hamiltonian complexity. We briefly discuss each in turn.

(i) Our public-key pseudoentanglement construction achieves essentially optimal parameters, but its construction uses a fairly involved iterated entanglement reduction procedure. In contrast, the private-key construction from [ABF+23] is very simple and based on subset states. It would be desirable to have a similarly straightforward construction of public-key pseudoentanglement, too. Furthermore, as we suggested in our discussion of [AFBV23], one can extend our definition of public-key pseudoentanglement to include a trapdoor that allows for efficient distillation of the "hidden" entanglement. It is not obvious how to extend our construction to include this feature.

[5] In particular, there must be a well-behaved function of few-body observables that separates the phases.

(ii) Our hardness results for the LGSES problem use Hamiltonians that differ from the Hamiltonians typically studied in condensed matter physics. For example, while we do prove a hardness result for the LGSES problem for 2D geometrically local Hamiltonians, this only holds for a certain set of cuts across the system. We expect that these results can be improved to be closer to the settings studied in condensed matter physics, such as to geometrically local Hamiltonians with more natural entanglement structures and larger spectral gaps,[6] which would have implications for the hardness of studying quantum phases of matter. This may require developing new sorts of clock constructions where the only goal is to preserve entanglement structure of BQP computations rather than to encode more general QMA-complete problems.

(iii) While we have focused on applications in Hamiltonian complexity in this work, pseudoentanglement might be a useful tool for proving hardness results in other domains, too. For example, recent work [BEM+23, AFBV23] has analysed the computational resources required to execute certain tasks from quantum Shannon theory, e.g. entanglement distillation. As observed in [AFBV23], proving hardness results for such problems is closely related to pseudoentanglement, and we hope that our construction of public-key pseudoentanglement will lead to additional and stronger hardness results in this direction.

Furthermore, public-key pseudoentanglement might also be interesting from a quantum cryptographic point of view, in particular its trapdoor-variant we suggested above. For example, recent work has focused on finding minimal assumptions for quantum cryptography (see e.g. [Zha23] and references therein for an overview), and it would be interesting to explore how pseudoentanglement is related to these assumptions.

Finally, it is natural to ask if public-key pseudoentanglement might have applications in quantum gravity. The AdS/CFT correspondence postulates that gravitational theories are dual to quantum mechanical systems, and that the entanglement structure of the quantum system is related to the geometry of the gravitational system [RT06]. Our results show that it is difficult to estimate the entanglement of quantum states. In contrast, geometry seems to be easy to determine, which might provide an argument that this duality is exponentially hard to compute, as first suggested in [BFV19]. Indeed this was part of the motivation for prior works of pseudoentanglement [GH20, ABF+23, AFBV23]. Our public-key extension might allow one to argue about hardness of different versions of the duality, e.g. the duality remains hard to compute even if given a parent Hamiltonian for the quantum state.

Acknowledgments

We thank Rotem Arnon-Friedman, Jordan Docter, Tudor Giurgica-Tiron, Andru Gheorghiu, Hsin-Yuan Huang, Vinod Vaikuntanathan, and Thomas Vidick for helpful discussions. B.F. and S.G. acknowledge support from AFOSR (FA9550-21-1-0008). This material is based upon work partially supported by the National Science Foundation under Grant CCF-2044923 (CAREER) and by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers (Q-NEXT). This research was also supported in part by the National Science Foundation under Grant No. NSF PHY-1748958. A.B., B.F.,

[6] Of course, we cannot hope to construct hard instances of the LGSES problem where both the area and volume law Hamiltonians are geometrically local and have constant spectral gap. This is simply because the area law (proven in 1D [Has07] and in 2D under extra conditions [AAG22], but widely believed to hold generally) requires *any* such Hamiltonian to have area law entanglement. However, this does not rule out computationally indistinguishable families of Hamiltonians where the area law Hamiltonian has constant gap and the volume law Hamiltonian has inverse polynomial gap, since determining the spectral gap itself is computationally infeasible [CPGW15, BCLPG20].

C.Z., and Z.Z. were supported in part by the DOE QuantISED grant DE-SC0020360. A.B. and C.Z. were supported in part by the U.S. DOE Office of Science under Award Number DE-SC0020266. A.B. was supported in part by the AFOSR under grant FA9550-21-1-0392. C.Z. was supported in part by the Shoucheng Zhang graduate fellowship. T.M. acknowledges support from SNSF Grant No. 200021_188541 and the ETH Zurich Quantum Center. U.V. was supported in part by DOE NQISRC QSA grant FP00010905, NSF QLCI Grant No. 2016245, and MURI Grant FA9550-18-1-0161.

2 Preliminaries

2.1 Notation

We write $[n]$ for the set $\{1,\dots,n\}$. For a bitstring $x \in \{0,1\}^n$, we denote the m most and least signficant bits by $\mathrm{MSB}_m(x)$ and $\mathrm{LSB}_m(x)$, respectively. We denote the concatenation of strings by $x \parallel y$. For a set of indices $I \subset [n]$ and bitstrings $x \in \{0,1\}^{|I|}$, $y \in \{0,1\}^{n-|I|}$ we denote by $z = x \parallel_I y$ the string z that equals x in indices in I and y on indices in $[n] \setminus I$. We will occasionally think of a bitstring as a $\mathbb{Z}_2$-vector, in which case we denote it as $\vec{x}$.

For a matrix $A \in \mathbb{C}^{m\times n}$, we denote by $\|A\|_p = \mathrm{Tr}\left[(A^\dagger A)^{p/2}\right]^{1/p}$ its Schatten p-norm. The 1-norm is also called the trace norm, the 2-norm the Frobenius norm (or Hilbert-Schmidt norm), and the ∞-norm the operator norm.

Quantum systems are denoted by capital letters A, B, etc. For a pure state $|\psi\rangle_{AB}$ or a mixed state ρ_{AB} on systems A and B, we denote the reduced states on system A by ψ_A and ρ_A, respectively. We write quantum circuits as $\mathsf{C} = U_T \cdot U_{T-1} \cdots U_1$, where U_i are elementary gates. This should be thought of as a list of gates, not simply a large unitary; in particular, inserting identity gates into the circuit does change the circuit (although of course it does not change the unitary implemented by the circuit). We will use this property of circuits in Section 2.6.

2.2 Independent hash functions

Definition 2.1 (r-wise independent function family)**.** A function family $H = \{h_k : [N] \to [M]\}_{k\in\mathcal{K}}$ indexed by some set of keys $\mathcal{K}$ is r-wise independent if for all distinct $x_1,\dots,x_r \in [N]$, the random variables $h_k(x_1),\dots,h_k(x_r)$ (for $k \in \mathcal{K}$ chosen uniformly) are uniform i.i.d.

The following is a standard result (see e.g. [Vad12, Corollary 3.34]):

Lemma 2.2. *For any $n, m, r \in \mathbb{N}$, there exists an r-wise independent function family $H_n = \{h_k : \mathbb{Z}_q^n \to \mathbb{Z}_q^m\}_{k\in\mathcal{K}}$ such that each $k \in \mathcal{K}$ has length $\mathrm{poly}(n, mr, \log q)$ and given $k \in \mathcal{K}$, the function h_k can be evaluated in time $\mathrm{poly}(n, m, r, \log q)$.*

2.3 Entropies

We recall the basic definitions of quantum entropies. Throughout, we use the convention that $0 \log 0 = 0$.

Definition 2.3 (von Neumann entropy)**.** The von Neumann entropy of a quantum state ρ is defined as

$$S(\rho) = -\mathrm{Tr}[\rho \log \rho] \,.$$

Definition 2.4 (Conditional von Neumann entropy)**.** The conditional von Neumann entropy of a quantum state ρ_{AB} is defined as

$$S(\rho_{A|B}) = S(\rho_{AB}) - S(\rho_B).$$

Definition 2.5 (Binary entropy function)**.** The binary entropy function is defined as

$$h(x) = -x\log x - (1-x)\log(1-x),$$

for $x \in [0,1]$.

2.3.1 Continuity properties

Lemma 2.6 (Continuity of the von Neumann entropy [Fan73, Aud07])**.** *Let ρ_{AB} and σ_{AB} be the density matrix of two n-qubit quantum states respectively, each partitioned into subsystems A and B, and let*

$$\frac{1}{2}||\rho_{AB} - \sigma_{AB}||_1 \leq \epsilon.$$

Then,

$$|S(\rho_{AB}) - S(\sigma_{AB})| \leq \epsilon \cdot n + h(\epsilon),$$

where $h(\cdot)$ is the binary entropy function.

Lemma 2.7 (Continuity of the conditional von Neumann entropy [Win16])**.** *Let ρ_{AB} and σ_{AB} be the density matrix of two n-qubit quantum states respectively, each partitioned into subsystems A and B, and let*

$$\frac{1}{2}||\rho_{AB} - \sigma_{AB}||_1 \leq \epsilon.$$

Then,

$$|S(\rho_{A|B}) - S(\sigma_{A|B})| \leq 2\epsilon \cdot \log|A| + (1+\epsilon) \cdot h\left(\frac{\epsilon}{1+\epsilon}\right),$$

where $|A|$ is the dimension of the Hilbert space for subsystem A and $h(\cdot)$ is the binary entropy function.

2.4 Entanglement measures

2.4.1 Pure state entanglement measure

For pure states on systems AB, the entanglement between A and B is quantified using the so-called entanglement entropy, which is simply the von Neumann entropy of the reduced state on either subsystem.

Definition 2.8 (Entanglement entropy)**.** For a *pure* state $|\psi\rangle_{AB}$, the entanglement entropy between systems A and B is defined as $S(\psi_A)$. Note that this is invariant under swapping A and B since for a pure state $|\psi\rangle_{AB}$, $S(\psi_A) = S(\psi_B)$.

2.4.2 Entanglement entropy for phase states

Definition 2.9 (T-matrix associated with phase states)**.** Let $s : \{0,1\}^n \to \{0,1\}$. For an n-qubit phase state

$$|\psi\rangle = \sum_x (-1)^{s(x)}|x\rangle$$

and a subset $X \subseteq [n]$, we define the "T-matrix" with respect to the cut X as a $\{\pm 1\}^{2^{|I|} \times 2^{n-|I|}}$-matrix with entries

$$T_{ij} = (-1)^{s(i\|_X j)},$$

where $\|_X$ is the "index string concatenation" defined in Section 2.1.

Lemma 2.10. *Let $s : \{0,1\}^n \to \{0,1\}$ and $|\psi\rangle = \sum_x (-1)^{s(x)}|x\rangle$. Then for any cut $X \subseteq [n]$, the entanglement entropy of that cut is bounded by*

$$-\log\left(\left\|\frac{1}{2^n}TT^\top\right\|_2\right) \leq S(\psi_X) \leq \log \operatorname{rank}(T)\,,$$

where T is the T-matrix of $|\psi\rangle$ across cut X.

Proof. This follows from a direct computation, see [ABF+23, Equation (113)]. □

2.4.3 Mixed state entanglement measures

Quantifying the entanglement of mixed states is much more difficult than for pure states, and several measures have been proposed [HHHH09]. The two most operationally meaningful ones are the distillable entanglement, denoted $E_D(\rho_{AB})$, and the entanglement cost, denoted $E_C(\rho_{AB})$. Informally, the distillable entanglement of a state ρ_{AB} is the rate at which one can extract EPR pairs from many copies of ρ_{AB} using local operations and classical communication (LOCC) (i.e. it gives the number of extractable EPR pairs divided by the number of available copies of ρ in the limit of infinitely many copies). Conversely, the entanglement cost of a state ρ_{AB} is the rate at which one needs to consume EPR pairs to create the state ρ_{AB} using LOCC. For our purposes the precise definition of these measures does not matter and we refer to [HHHH09, Section XV.A] for details.

More importantly for our purposes, distillable entanglement and entanglement cost are extremal measures in the sense that any entanglement measure E that satisfies a number of nautral requirement is bounded as [DHR02, Chr06]

$$E_D(\rho_{AB}) \leq E(\rho_{AB}) \leq E_C(\rho_{AB})\,. \tag{2.1}$$

We will be interested in bounding these operational entanglement measures. For this we will rely on non-operational quantities that are easier to deal with mathematically. Concretely, we will use the entanglement of formation and the coherent information, both defined below.

Definition 2.11 (Entanglement of formation)**.** The entanglement of formation of a quantum state ρ_{AB} is defined as

$$E_F(\rho_{AB}) = \inf\left\{\sum_i p_i\, S(\psi_{i,A})\right\},$$

where the infimum is taken over all possible ways in which we can decompose ρ_{AB} as

$$\rho_{AB} = \sum_i p_i\, |\psi_i\rangle_{AB}\langle\psi_i|_{AB}.$$

Definition 2.12 (Coherent information)**.** The coherent information of a quantum state ρ_{AB} is defined as

$$I(\rho_{AB}) = -S(\rho_{A|B}).$$

We then get the following useful bounds.

Lemma 2.13. *Any* natural entanglement measure $E(\rho_{AB})$ *(in the sense of Equation (2.1), see [DHR02] for details) satisfies*

$$I(\rho_{AB}) \leq E_D(\rho_{AB}) \leq E(\rho_{AB}) \leq E_C(\rho_{AB}) \leq E_C(\rho_{AB})\,.$$

Proof. The lower bound in terms of coherent information was shown in [DW05] and the upper bound in terms of entanglement of formation follows from [HHT01]. □

For pure states, all of these measures coincide with the entanglement entropy:

Lemma 2.14 ([Woo01], [HH01], [SN96])**.** *Let ρ_{AB} be a pure state. Then,*

$$E_F(\rho_{AB}) = E_C(\rho_{AB}) = E_D(\rho_{AB}) = I(\rho_{AB}) = S(\rho_A).$$

Finally, we will require the following continuity property of entanglement of formation.

Lemma 2.15 (Continuity of entanglement of formation [Win16])**.** *Let ρ_{AB} and σ_{AB} be the density matrix of two n-qubit quantum states respectively, each partitioned into subsystems A and B, and let*

$$\frac{1}{2}||\rho_{AB} - \sigma_{AB}||_1 \leq \epsilon\,.$$

Additionally, let $\delta = \sqrt{\epsilon(2-\epsilon)}$ and let $h(\cdot)$ be the binary entropy function. Then,

$$|E_F(\rho_{AB}) - E_F(\sigma_{AB})| \leq \delta \cdot n + (1+\delta) \cdot h\left(\frac{\delta}{1+\delta}\right).$$

2.5 Learning with Errors

Definition 2.16 (Uniform, Gaussian, and lossy matrix distributions)**.** We denote the uniform distribution over $\mathbb{Z}_q^{m\times n}$-matrices by $U_q^{m\times n}$. We denote by $D_{q,\sigma}^{m\times n}$ the distribution over $\mathbb{Z}_q^{m\times n}$ where each element is an i.i.d. sample from the discretised Gaussian distribution with width σ (see [Pei16, Section 2.2] for a definition).

We further define the following distribution $L_{q,\ell,\sigma}^{m\times m}$ over $\mathbb{Z}_q^{m\times m}$-matrices:

(i) Sample $B, C \leftarrow U_q^{\ell\times m}$.

(ii) Sample $E \leftarrow D_{q,\sigma}^{m\times m}$.

(iii) Output $B^\top \cdot C + E$.

Definition 2.17. The $\mathrm{LWE}_{n,m,q,\sigma}$ problem is the computational problem of distinguishing the following two distributions:

(i) $(A, \vec{u}) \leftarrow U_q^{m\times n} \times U_q^m$.

(ii) $(A, A\cdot\vec{s}+\vec{e})$, where $A \leftarrow U_q^{m\times n}$, $\vec{s} \leftarrow U_q^n$, and $\vec{e} \leftarrow D_{q,\sigma}^m$.

We will rely on the following standard assumption in post-quantum cryptography [Reg09, Pei16].

Assumption 2.18 (Standard LWE assumption)**.** For every constant $\beta > 0$, every $\mathrm{poly}(m)$-time quantum algorithm has $\mathrm{negl}(m)$-advantage in solving the $\mathrm{LWE}_{n,m,q,\sigma}$ problem for $n = m^\beta$, $q = 2^{\mathrm{poly}(n)}$, and $\sigma \geq \frac{q}{\mathrm{poly}(m)} \geq 2\sqrt{m}$.

We will also make use of the following stronger assumption to achieve larger entanglement gaps in our pseudoentanglement construction [LP11, Pei16].

Assumption 2.19 (Subexponential-time LWE assumption)**.** There exist constants $\beta_1 > \beta_2 > 0$ such that every $\mathrm{poly}(m)$-time quantum algorithm has advantage at most $2^{-\Omega(\ell^{\beta_1})}$ in solving the $\mathrm{LWE}_{\ell,m,q,\sigma}$ problem for $m = 2^{O(\ell^{\beta_2})}$, $q = 2^{\mathrm{poly}(m)}$, and $\sigma \geq \frac{q}{\mathrm{poly}(m)} \geq 2\sqrt{m}$.

We will use the following immediate consequence of Assumption 2.18 [GKPV10].

Lemma 2.20.

(i) *Under Assumption 2.18 matrices sampled from $U_q^{m\times m}$ and $L_{q,\ell,\sigma}^{m\times m}$ are computationally indistinguishable for $m = \mathrm{poly}(\ell)$, $q = 2^{\mathrm{poly}(m)}$, and $\sigma \geq \frac{q}{\mathrm{poly}(m)} \geq 2\sqrt{m}$.*

(ii) *Under Assumption 2.19 there exists a constant $\beta > 0$ such that matrices sampled from $U_q^{m\times m}$ and $L_{q,\ell,\sigma}^{m\times m}$ are computationally indistinguishable for $m = 2^{\ell^\beta}$, $q = 2^{\mathrm{poly}(m)}$, and $\sigma \geq \frac{q}{\mathrm{poly}(m)} \geq 2\sqrt{m}$.*

Proof. In $A = B^\top \cdot C + E$, we can view every column $c_i \in \mathbb{Z}_q^\ell$ of C as an LWE secret of length ℓ. Then distinguishing $U_q^{m\times m}$ and $L_{q,\ell,\sigma}^{m\times m}$ is equivalent to solving at least one of m instances of $\mathrm{LWE}_{\ell,m,q,\sigma}$ decision problems. This can be bounded using a union bound for both parts of the lemma:

(i) By Assumption 2.18, the distinguishing advantage on a single instance of $\mathrm{LWE}_{\ell,m,q,\sigma}$ is $\mathrm{negl}(m)$, so the distinguishing advantage for m copies is at most $m\,\mathrm{negl}(m)$, which is still negligible in m.

(ii) By Assumption 2.19, there are constants $\beta := \beta_2 < \beta_1$ such that the distinguishing advantage on a single instance of $\mathrm{LWE}_{\ell,m,q,\sigma}$ is $2^{-\Omega(\ell^{\beta_2})}$, so the distinguishing advantage for m copies is at most $m2^{-\Omega(\ell^{\beta_2})} = 2^{O(\ell^\beta)-\Omega(\ell^{\beta_2})} = \mathrm{negl}(m)$ since $\beta_2 > \beta$.

□

Lemma 2.21. *If $q \geq 2^{\ell/2}$ and $\ell \leq m$, then*

$$\Pr_{A\leftarrow U_q^{\ell\times m}}[\mathrm{rank} A = \ell] \geq 1 - O(2^{-\ell/4}).$$

Proof. We can imagine A being sampled row-by-row. Conditioned on the first r rows being linearly independent, the probability of the first $r+1$ rows being linearly independent is $1 - q^r/q^m$, so the probability of all rows being linearly independent is

$$\prod_{r=0}^{\ell-1}\left(1 - \frac{q^r}{q^m}\right) \geq 1 - \frac{\ell}{q} \geq 1 - O(2^{-\ell/4}).$$

□

We will need the following simple fact about the number of binary vectors that get mapped to 0 under a random matrix multiplication.

Lemma 2.22. *If $q \geq 2^{m/\ell}$, then*

$$\Pr_{A\leftarrow U_q^{\ell\times m}}\left[|\{\vec{x}\in\{0,1\}^m \text{ s.t. } A\cdot\vec{x} = \vec{0}\}| \leq 2^\ell\right] \geq 1 - O(2^{-\ell}).$$

Proof. For $\vec{x} \in \{0,1\}^m$ define $\mathbf{1}_{\vec{x}}$ as the indicator random variable (over the random choice of A) that is 1 if $A \cdot \vec{x} = \vec{0}$. Then by linearity of expectation,

$$\mathbb{E}_A \left[|\{\vec{x} \in \{0,1\}^m \text{ s.t. } A \cdot \vec{x} = \vec{0}\}| \right] = \mathbb{E}_A \left[\sum_{\vec{x}} \mathbf{1}_{\vec{x}} \right] = \sum_{\vec{x}} \mathbb{E}_A [\mathbf{1}_{\vec{x}}] = 1 + \frac{2^m - 1}{q^\ell},$$

where the last equality holds because $1_{\vec{0}} = 1$ always, and for the remaining $2^m - 1$ choices of $\vec{x} \neq \vec{0}$, the vector $A \cdot \vec{x}$ is uniform in $\mathbb{Z}_q^\ell$. Therefore by Markov's inequality,

$$\Pr_{A \leftarrow U_q^{\ell \times m}} \left[|\{\vec{x} \in \{0,1\}^m \text{ s.t. } A \cdot \vec{x} = \vec{0}\}| > 2^\ell \right] \leq 2^{-\ell} + \frac{2^m - 1}{(2q)^\ell} = O(2^{-\ell})$$

for $q \geq 2^{m/\ell}$. □

2.6 Hamiltonians and Kitaev clock construction

In this section, we will introduce some notations having to do with some variants of the standard circuit-to-Hamiltonian construction by [KSV02].

Definition 2.23 (History state)**.** For a circuit $\mathsf{C} = U_K \cdot U_{T-1} \cdots U_1$, the history state $|\Psi_{\mathsf{C}}\rangle$ is defined as

$$|\Psi_{\mathsf{C}}\rangle = \frac{1}{\sqrt{K+1}} \sum_{t=0}^{T} U_t \cdot U_{t-1} \cdots U_1 |0^n\rangle \otimes |\text{clock}(t)\rangle.$$

Here, $\text{clock}(t)$ can be any encoding of the integer t, typically in binary or unary.

Definition 2.24 (Padded history state Hamiltonian)**.** For a circuit $\mathsf{C} = U_K \cdot U_{K-1} \cdots U_1$ on n qubits with $K = \text{poly}(n)$, define the M-padded circuit as $\mathsf{C}'_M = U_{K+M} \cdots U_{K+1} \cdot U_K \cdots U_1$, where $U_{K+M}, \ldots, U_{K+1}$ are identity gates. A M-padded history state Hamiltonian $H_{\mathsf{C},M}$ for circuit C is any Hamiltonian with spectral gap at least $1/\text{poly}(n)$ whose unique ground state is $|\Psi_{\mathsf{C}'_M}\rangle$.

Applying Kitaev's well-known circuit-to-Hamiltonian construction [KSV02] to a padded circuit immediately shows the existence of padded history state Hamiltonians. The requirement on the spectral gap follows e.g. from [AVDK+08].

Lemma 2.25 ([KSV02, AVDK+08])**.** *If we choose* $\text{clock}(t)$ *in Definition 2.23 to be a binary encoding, then for any* $K = \text{poly}(n)$*, a* $\text{poly}(n)$*-length circuit* C *has a* $O(\log n)$*-local* M*-padded history state Hamiltonian* $H_{\mathsf{C},M}$*.*

If we choose $\text{clock}(t)$ *in Definition 2.23 to be a unary encoding, then for any* $K = \text{poly}(n)$*, a* $\text{poly}(n)$*-length circuit* C *has a* $O(1)$*-local* M*-padded history state Hamiltonian* $H_{\mathsf{C},M}$*.*

The useful property of the padded history state Hamiltonian is that its ground state is close to the output state of the circuit C. This has already been shown and used in [NVY18, GH20], so we only sketch the proof.

Lemma 2.26. *Let* C *be a* $K = \text{poly}(n)$*-gate circuit on* n *qubits. For any* $\epsilon \geq 1/\text{poly}(n)$ *there exists a* $M = \text{poly}(n)$ *such that the ground state* $|\psi_{\text{ground}}\rangle$ *of the* M*-padded history state Hamiltonian* $H_{\mathsf{C},M}$ *satisfies*

$$\left\| |\psi_f\rangle\langle\psi_f| - |\psi_{\text{ground}}\rangle\langle\psi_{\text{ground}}| \right\|_1 \leq \epsilon,$$

where $|\psi_f\rangle = U_K \cdots U_1 |0^n\rangle \otimes \frac{1}{\sqrt{M+K+1}} \sum_{t=0}^{M+K} |\text{clock}(t)\rangle$

Proof. By construction,

$$|\psi_{\text{ground}}\rangle = \frac{1}{\sqrt{M+K+1}} \sum_{t=0}^{K} U_t \cdot U_{t-1} \cdots U_1 |0^n\rangle \otimes |\text{clock}(t)\rangle + \frac{1}{\sqrt{M+K+1}} |\psi_f\rangle \otimes \sum_{t=K+1}^{M} |\text{clock}(t)\rangle .$$

The lemma then follows by a direct calculation choosing $M = \text{poly}(n)$ sufficiently large such that $\frac{K+1}{M+K+1} = O(\epsilon)$ is sufficiently small. □

3 Public-key pseudoentanglement: definition and construction

In this section, we define and construct public-key pseudoentanglement. Our construction uses a similar idea as in [ABF+23, Appendix A], which is to consider phase states whose phases have been manipulated in a particular way to create high or low entanglement. The "manipulation" of these phases is by means of applying a one-to-one or many-to-one function (see Section 3.2 for details). We therefore need to construct such *lossy functions* with the appropriate parameters, which we do in Section 3.1 based on the LWE assumption.

In Section 3.2, we then use these lossy functions to construct indistinguishable families of quantum states where states in one family have high entanglement and states in the other family have low entanglement across a *single fixed bipartition* of the qubits. In Section 3.3, we extend this construction to states that have high or low entanglement *for (almost) every cut on a 1Dimensional line*, i.e. we imagine the qubits of the state being arranged on a line and consider all bipartitions into left and right qubits. We show that under the subexponential-time LWE assumption, it is possible to construct pseudoentangled states of this form where either all cuts a have a linear or a polylogarithmic amount of entanglement, which is the largest possible separation, as discussed in Remark 3.11. In this sense our public-key pseudoentanglement construction is optimal. We will use this multi-cut construction in Section 4 to show that learning the ground state entanglement structure of (classically described) local Hamiltonians is computationally hard (under the LWE assumption).

3.1 Construction of lossy functions

We define the following rounding function for $\mathbb{Z}_q$ elements.

Definition 3.1. For $q = cp$ with $c \in \mathbb{N}$, divide $\mathbb{Z}_q$ into p consecutive bins. We define $\lfloor x \rceil_p \in \mathbb{Z}_p$ as the index of the bin in which x lies. For a vector $x \in \mathbb{Z}_p^m$, $\lfloor \vec{x} \rceil_p \in \mathbb{Z}_p^m$ is defined as the element-wise application of $\lfloor \cdot \rceil_p$.

Definition 3.2 (Lossy function construction)**.** Choose parameters $\ell(m), r(m) \leq \text{poly}(m)$. Let $p = 2^4$, $q = 2^m$, and $\sigma = q/m^3$. Let $H_m = \{h_k : \mathbb{Z}_p^m \to \mathbb{Z}_2^m\}_{k \in \mathcal{K}_m^{\text{hash}}}$ be the $r(m)$-wise independent function family from Lemma 2.2. We define two families of functions $f : \{0,1\}^m \to \{0,1\}^m$ indexed by key sets $\mathcal{K}_m^{\text{inj}}, \mathcal{K}_m^{\text{lossy}} \subset \mathbb{Z}_q^{m \times m} \times \mathcal{K}_m^{\text{hash}}$ as follows:

- To sample a key from $\mathcal{K}_m^{\text{inj}}$, denoted $k \leftarrow \mathcal{K}_m^{\text{inj}}$, sample $A \leftarrow U_q^{m \times m}$ and $k^{\text{hash}} \in \mathcal{K}_m^{\text{hash}}$ uniformly. Set $k = (A, k^{\text{hash}})$.
- To sample a key from $\mathcal{K}_m^{\text{lossy}}$, denoted $k \leftarrow \mathcal{K}_m^{\text{lossy}}$, sample $A \leftarrow L_{q,\ell,\sigma}^{m \times m}$ and $k^{\text{hash}} \in \mathcal{K}_m^{\text{hash}}$ uniformly. Set $k = (A, k^{\text{hash}})$.

- For a key $k = (A, k^{\text{hash}}) \in \mathcal{K}_m^{\text{inj}} \cup \mathcal{K}_m^{\text{lossy}}$, the function $f_k : \{0,1\}^m \to \{0,1\}^m$ is defined as

$$f_k(\vec{x}) = h_{k^{\text{hash}}}\left(\lfloor A \cdot \vec{x} \rfloor_p\right).$$

The following theorem summarises the relevant properties of our lossy function construction.

Theorem 3.3. *The following properties hold for the function family from Definition 3.2 instantiated with any $r(m) \leq \text{poly}(m)$ and $\text{poly}\log(m) \leq \ell(m) \leq \text{poly}(m)$.*

(i) *(Almost injective functions) With overwhelming probability over the choice of $A \leftarrow U_q^{m\times m}$, the function family $\{f_{(A,k^{\text{hash}})}\}_{k^{\text{hash}} \in \mathcal{K}_m^{\text{hash}}}$ is $r(m)$-wise independent:*

$$\Pr_{A \leftarrow U_q^{m\times m}}\left[\{f_{(A,k^{\text{hash}})}\}_{k^{\text{hash}} \in \mathcal{K}_m^{\text{hash}}} \text{ is } r(m)\text{-wise independent}\right] \geq 1 - O(2^{-m}).$$

(ii) *(Highly compressing functions) For keys in $\mathcal{K}^{\text{lossy}}$, the image of f_k has size at most 2^{ℓ^2} with overwhelming probability:*

$$\Pr_{k \leftarrow \mathcal{K}_m^{\text{lossy}}}\left[|\operatorname{img} f_k| \leq 2^{\ell^2}\right] \geq 1 - 2^{-\ell/4}$$

(iii) *(Computational indistinguishability) Under Assumption 2.18, if $r(m) \leq \text{poly}(m)$ and $\ell(m) \geq \Omega(m^c)$ for any constant $c > 0$, then all efficient quantum algorithms have advantage $\text{negl}(m)$ in distinguishing keys sampled according to $\mathcal{K}_m^{\text{inj}}$ and $\mathcal{K}_m^{\text{lossy}}$.*

Similarly, under Assumption 2.19, there exists a constant $\delta > 0$ such that if $r(m) \leq \text{poly}(m)$ and $\ell(m) \geq \Omega(\log(m)^{1+\delta})$, then all efficient quantum algorithms have advantage $\text{negl}(m)$ in distinguishing keys sampled according to $\mathcal{K}_m^{\text{inj}}$ and $\mathcal{K}_m^{\text{lossy}}$.

Proof. We prove Item (i) in Corollary 3.5. Item (ii) is shown in Lemma 3.8. Item (iii) follows immediately from Lemma 2.20. □

3.1.1 Bounds for almost injective functions

Lemma 3.4. *For $m \in N$, $p = 2^4$, and $q = cp$ for some $c \in \mathbb{N}$,*

$$\Pr_{A \leftarrow U_q^{m\times m}}[\vec{x} \mapsto \lfloor A\vec{x} \rfloor_p \text{ is injective}] \geq 1 - O(2^{-m}).$$

Proof. We bound the probability that there exists a pair $\vec{x} \neq \vec{x}' \in \{0,1\}^m$ for which $\lfloor A\vec{x} \rfloor_p = \lfloor A\vec{x}' \rfloor_p$. Suppose first that $\vec{x} = 0$. Then $\vec{x}' \neq 0$, so $\lfloor A\vec{x}' \rfloor_p$ is a uniform $\mathbb{Z}_p^m$-vector over the random choice of A. Hence using $p = 2^4$ and a union bound,

$$\Pr_{A \leftarrow U_q^{m\times m}}\left[\exists \vec{x}' \text{ s.t. } \lfloor A\vec{x} \rfloor_p = \lfloor A\vec{x}' \rfloor_p\right] \leq 2^m 2^{-4m} \leq 2^{-m}.$$

If both $\vec{x}, \vec{x}'$ are non-zero, then over the random choice of A, $A\vec{x}$ and $A\vec{x}'$ are independent uniform $\mathbb{Z}_q^m$-vectors, so $\lfloor A\vec{x} \rfloor_p$ and $\lfloor A\vec{x}' \rfloor_p$ are independent uniform Z_p^m-vectors. Hence, for fixed non-zero $\vec{x}, \vec{x}'$,

$$\Pr_{A \leftarrow U_q^{m\times m}}\left[\lfloor A\vec{x} \rfloor_p = \lfloor A\vec{x}' \rfloor_p\right] \leq 2^{-4m}.$$

The lemma follows by a union bound over the (less than) 2^{2m} possible pairs $(\vec{x}, \vec{x}')$ and using $p = 2^4$. □

Corollary 3.5.

$$\Pr_{A \leftarrow U_q^{m \times m}}\left[\{f_{(A,k^{\text{hash}})}\}_{k^{\text{hash}} \in \mathcal{K}_m^{\text{hash}}} \textit{ is } r\textit{-wise independent}\right] \geq 1 - O(2^{-m}).$$

Proof. Composing an injective function with an r-wise independent hash family yields another r-wise independent hash family. Therefore, the corollary follows directly from Lemma 3.4 and the construction of $f_{(A,k^{\text{hash}})}$ in Definition 3.2. □

3.1.2 Bounds for compressing functions

Definition 3.6. For any $M \in \mathbb{Z}_q^{\ell \times m}$, let $f_M : \{0,1\}^m \to \mathbb{Z}_q^\ell$ be the associated linear map. We define $\vec{v}_j(M)$ as the j-th element of $\text{img}(f_M)$ (ordered according to the usual ordering on $\mathbb{Z}_q^\ell$). For $j \in \{1, \ldots, q^{\text{rank}M}\}$ we then define the following collection of subsets:

$$C_j(M) = f_M^{-1}(\vec{v}_j(M)) \subseteq \{0,1\}^m.$$

If $j > |\text{img}(f_M)|$, then $C_j(M) = \varnothing$.

Remark 3.7. Note that in the above definition, $j > |\text{img}(f_M)|$ can indeed occur: this is because $\text{rank}M$ is defined over $\mathbb{Z}_q$, but we have restricted the domain of f_M to bitstrings, so $\text{img}\, f_M$ only contains $\mathbb{Z}_q$ elements that have a *binary* preimage under f_M. Still, $q^{\text{rank}M}$ is an upper bound on $|\text{img}\, f_M|$, which is all that will matter for our purposes. Further, observe that the family $\{C_j(M)\}_j$ defines a partition on $\{0,1\}^m$.

Lemma 3.8.

$$\Pr_{k \leftarrow \mathcal{K}_m^{\text{lossy}}}\left[|\text{img}\, f_k| \leq 2^{\ell^2}\right] \geq 1 - 2^{-\ell}$$

Proof. First observe that for any choice of key $k = (A, k^{\text{hash}})$,

$$|\text{img}\, f_k| \leq |\text{img}\, g_A|, \tag{3.1}$$

where $g_A(\vec{x}) = \lfloor A \cdot \vec{x} \rceil_p$. We will therefore bound the latter. For this, for $A = B^\top C + E$ chosen as in Definition 3.2 we can bound

$$|\text{img}\, g_A| \leq \sum_{j=1}^{q^\ell} |\{g_A(\vec{x}) \mid \vec{x} \in C_j(C)\}|. \tag{3.2}$$

This is because $\text{rank}C \leq \ell$, so by Remark 3.7 $\{C_j(C)\}_{j=1,\ldots,q^\ell}$ forms a partition of $\{0,1\}^m$.

We now fix a C and a j such that $\vec{0} \notin C_j(C)$ and bound the expectation of $|\{g_A(x) \mid x \in C_j(C)\}|$ over $A \leftarrow L_{q,\ell}^{m \times m}$. Recall that $g_A(x)$ "rounds" each entry of $A \cdot \vec{x}$ to a $\mathbb{Z}_p$ element by dividing $\mathbb{Z}_q$ into p equally sized contiguous regions. We can therefore define $B_{q,p,\beta}$ as the set of $\mathbb{Z}_q$-elements that are within $\beta < \frac{q}{2p}$ of such a cut (where distance is in $\mathbb{Z}_q$, i.e. mod q). Since there are exactly p cuts, $|B_{q,p,\beta}| = 2p\beta$. (This is an equality because for $\beta < \frac{q}{2p}$, the β-thickenings around the cuts cannot overlap.)

For $i = 1, \ldots, m$ we define the random variable (where the randomness is only over B as we fixed a choice of C and j and $C \cdot \vec{x}$ is the same for all $\vec{x} \in C_j(C)$)

$$\mathbf{1}_i = \begin{cases} 1 & \text{if} \quad \exists \vec{x} \in C_j(C) \text{ s.t. } (B^\top C \cdot \vec{x})_i \in B_{q,p,\beta}, \\ 0 & \text{else}. \end{cases}$$

Here, $(B^\top C \cdot \vec{x})_i \in \mathbb{Z}_q$ denotes the i-th vector entry. Importantly, the different $\mathbf{1}_i$ are independent. To see this, observe that $C \cdot \vec{x}$ is a fixed non-zero vector for all $\vec{x} \in C_j(C)$. Therefore, $(B^\top C \cdot \vec{x})_i$ is the inner product between the i-th row of B and this fixed vector. Since the different rows of B are sampled independently, $(B^\top C \cdot \vec{x})_i$ are independent, too, and consequently so are $\mathbf{1}_i$. By the same reasoning, $(B^\top C \cdot \vec{x})_i$ is uniform, so

$$\Pr_B[\mathbf{1}_i = 1] = \frac{2p\beta}{q}. \tag{3.3}$$

To relate these random variables to $|\{g_A(x) \mid x \in C_j(C)\}|$, we set $\beta = 2m\sigma$ and define a set of "large" error matrices E:

$$L = \{E \in \mathbb{Z}_q^{m \times m} \mid E \text{ has a row } e_i \text{ with 1-norm } \|e_i\|_1 \geq \beta\}.$$

(i) Case $E \in L$. We will bound the probability of this happening and treat this event separately. Since each entry to E is a Gaussian with standard deviation σ, $\|e_i\|_1$ is a sum of absolute values of i.i.d. Gaussians, so by a union bound over the m rows and the 2^m possible signs for the absolute values within each row,

$$\Pr[E \in L] \leq m 2^m e^{-\frac{\beta^2}{2m\sigma^2}} \leq 2^{-m}. \tag{3.4}$$

(ii) Case $E \notin L$. In this case, in each direction i the difference between $(B^\top C \cdot \vec{x})_i$ and $(A \cdot \vec{x})_i$ is at most β. Hence, since $B^\top C \cdot \vec{x}$ is the same for all $x \in C_j(C)$, the only way that the "cloud" of points $\{A \cdot \vec{x}\}_{x \in C_j(C)}$ be split into two distinct sets along dimension i by the rounding procedure is if $\mathbf{1}_i = 1$. Therefore, for any $E \notin L$ we find that

$$|\{g_A(x) \mid x \in C_j(C)\}| \leq 2^{\Sigma_i \mathbf{1}_i}.$$

We can bound the expectation of this quantity over the random choice of B. Because the different $\mathbf{1}_i$ are independent:

$$\mathbb{E}_{B \leftarrow U_q^{\ell \times m}}\left[2^{\Sigma_i \mathbf{1}_i}\right] = \Pi_{i=1}^m \mathbb{E}_{B \leftarrow U_q^{\ell \times m}}\left[2^{\mathbf{1}_i}\right]$$

By Equation (3.3):

$$= \left(1 + \frac{2p\beta}{q}\right)^m$$

Since $q \geq 2p\beta m$ for sufficiently large m:

$$\leq e.$$

We can now combine the pieces of the proof as follows. We write $E \leftarrow L^c$ for an error matrix E sampled as in Definition 3.2 conditioned on $E \notin L$ and $C \leftarrow U_q^{\ell \times m}|_{\text{good}}$ for a uniform C conditioned on

$$|\{\vec{x} \in \{0,1\}^m \text{ s.t. } C \cdot \vec{x} = \vec{0}\}| \leq 2^\ell.$$

By Equations (3.1) and (3.4) and Lemma 2.22 and with $A = B^\top C + E$ as before:

$$\Pr_{k \leftarrow \mathcal{K}^{\text{lossy}}}\left[|\operatorname{img} f_k| > 2^{\ell^2}\right] \leq O(2^{-\ell}) + \Pr_{B \leftarrow U_q^{\ell \times m}, C \leftarrow U_q^{\ell \times m}|_{\text{full}}, E \leftarrow L^c}\left[|\operatorname{img} g_A| > 2^{\ell^2}\right]$$

By Markov's inequality:

$$\leq O(2^{-\ell}) + \frac{1}{2^{\ell^2}} \mathbb{E}_{B \leftarrow U_q^{\ell \times m}, C \leftarrow U_q^{\ell \times m}|_{\text{good}}, E \leftarrow L^c} [|\operatorname{img} g_A|]$$

By Equation (3.2)

$$\leq O(2^{-\ell}) + \frac{1}{2^{\ell^2}} \sum_{j=1}^{q^\ell} \mathbb{E}_{C \leftarrow U_q^{\ell \times m}|_{\text{good}}, E \leftarrow L^c} \left(\mathbb{E}_{B \leftarrow U_q^{\ell \times m}} [|\{g_A(\vec{x}) \mid \vec{x} \in C_j(C)\}|] \right)$$

By our analysis of the case $E \notin L$, we know that the expression in parentheses is at most e in case j is such that $\vec{0} \notin C_j(C)$. On the other hand, if $\vec{0} \in C_j(C)$ then for that value of j the expression in parentheses is trivially bounded by 2^ℓ by our definition of $U_q^{\ell \times m}|_{\text{good}}$. Therefore we can bound the whole expression by

$$\leq O(2^{-\ell}) + \frac{e(q^\ell - 1) + 2^\ell}{2^{\ell^2}} \leq O(2^{-\ell}) + O(2^{-\ell(\ell - \log q)}) \leq O(2^{-\ell})$$

since $m \geq \ell$ and $\ell - \log q \geq 1$. □

3.2 Public-key pseudoentanglement across a single cut

We will now use our lossy function construction from Section 3.1 to construct public-key pseudoentangled states for the middle cut that separates the left and right half of qubits. In Section 3.3 we will use the ideas from this section in an iterated way to construct pseudoentangled states for qubits arranged on a line that are pseudoentangled across every cut on the line. Strictly speaking, all the results in this section follow from the more general analysis in Section 3.3. We spell them out nonetheless because it may be easier for readers to first understand the single-cut construction in detail before moving on to Section 3.3.

We begin by defining single-cut public-key pseudoentanglement formally.

Definition 3.9 (Public-key pseudoentanglement across a single cut)**.** A public-key pseudoentangled state ensemble with entanglement gap $(f(n), g(n))$ across cuts $X_n \subset [n]$ consists of two sequences of families of quantum states $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k \in \mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k \in \mathcal{K}_n^{\text{high}}}$ indexed by key sets $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$ respectively with the following properties:

(i) Every $|\psi_k\rangle \in \Psi_n^{\text{low}} \cup \Psi_n^{\text{high}}$ is an n-qubit state.

(ii) Every key $k \in \mathcal{K}_n^{\text{low}} \cup \mathcal{K}_n^{\text{high}}$ has length $\text{poly}(n)$, and there exists an efficient sampling procedure that, given as input n and a label "high" or "low", outputs a key $k \in \mathcal{K}_n^{\text{low}}$ or $k \in \mathcal{K}_n^{\text{high}}$, respectively. We write $k \leftarrow \mathcal{K}_n^{\text{low}}$ and $k \leftarrow \mathcal{K}_n^{\text{high}}$ for keys sampled according to this procedure.

(iii) Given $k \in \mathcal{K}_n^{\text{low}} \cup \mathcal{K}_n^{\text{high}}$, the corresponding state $|\psi_k\rangle$ is efficiently preparable (without knowing whether $k \in \mathcal{K}^{\text{low}}$ or $k \in \mathcal{K}^{\text{high}}$). Formally, there exists a uniform polynomial-time circuit family $\{C_n\}$ such that C_n takes as input a key $k \in \mathcal{K}_n^{\text{low}} \cup \mathcal{K}_n^{\text{high}}$ and outputs a state negligibly close to $|\psi_k\rangle$.

(iv) The keys from $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$ are computationally indistinguishable. Formally, for all $\text{poly}(n)$-time quantum adversaries $\mathcal{A}$ that take as input a key $\mathcal{K}_n^{\text{low}} \cup \mathcal{K}_n^{\text{high}}$ and output a single bit:

$$\left| \Pr_{k \leftarrow \mathcal{K}_n^{\text{low}}} [\mathcal{A}(k) = 0] - \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}} [\mathcal{A}(k) = 0] \right| = \text{negl}(n).$$

(v) With overwhelming probability, across the cut X_n states in Ψ_n^{low} have entanglement entropy $\Theta(f(n))$ and states in Ψ_n^{high} have entanglement entropy $\Theta(g(n))$. Formally, there exist constants $0 < C_1 < C_2$ such that for all sufficiently large n,

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}[S((\psi_k)_{X_n}) \in [C_1 f(n), C_2 f(n)]] \geq 1 - \text{negl}(n)\,,$$
$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}[S((\psi_k)_{X_n}) \in [C_1 g(n), C_2 g(n)]] \geq 1 - \text{negl}(n)\,.$$

Here, $S((\psi_k)_{X_n})$ is the von Neumann entropy of the reduced state of $|\psi_k\rangle$ on the qubits in the set $X_n \subset [n]$.

Remark 3.10. We will frequently abuse notation and use entanglement gaps of the form $(O(f(n)), \Omega(g(n)))$. By this, we mean that (across a specified cut X_n) Ψ_n^{low} has entanglement at most $O(f(n))$ and Ψ_n^{high} has entanglement at least $\Omega(g(n))$. Formally, this means that for this case Item (v) of Definition 3.9 has to be modified as follows:

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}[S((\psi_k)_{X_n}) \leq O(f(n))] \geq 1 - \text{negl}(n)\,,$$
$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}[S((\psi_k)_{X_n}) \geq \Omega(g(n))] \geq 1 - \text{negl}(n)\,.$$

Remark 3.11. A natural question is what the optimal entanglement gap for pseudoentangled states is. Clearly, the high-entanglement states can have entanglement at most $g(n) = O(n)$ across any cut, since the entanglement entropy is upper bounded by the number of qubits. For the low-entanglement states, one can show that the entanglement entropy needs to scale faster than $\log n$, i.e. $f(n) = \omega(\log n)$. Otherwise, one could distinguish the low-entanglement states from the high-entanglement states using a variant of the SWAP test. This was proven in [JLS18] and [ABF+23, Appendix F] for private-key pseudoentangled states and the same proof applies to the public-key setting, too.

We now give a construction of single-cut pseudoentangled states based on our lossy function construction from Section 3.1. As we will show in Theorem 3.13, these states do indeed form pseudoentangled ensembles in the sense of Definition 3.9. Under the standard LWE assumption (Assumption 2.18), we can achieve an entanglement gap of $(O(n^\delta), \Omega(n))$ for any $\delta > 0$, where n is the number of qubits and the cut divides the qubits into two equal halves; under the stronger subexponential-time LWE assumption (Assumption 2.19) we can achieve an entanglement gap of $(O(\text{poly}\log n), \Omega(n))$, which is essentially optimal as noted in Remark 3.11.

For simplicity, for the rest of this subsection we always assume that n is even and write $m = n/2$. We will consider the cut that divides the qubits into two sets of size n; we could also consider more general cuts and treat them with the same technique, which we do in Section 3.3.

Overview. The intuition of the construction below is as follows: our high entanglement and low entanglement states will be phase states of the form $|\psi_k\rangle = \sum_{x\in\{0,1\}^n}(-1)^{s_k(x)}|x\rangle$, where $s_k : \{0,1\}^n \to \{0,1\}$ is a function described by some public key k. This is why we call the construction public-key: the states we are considering are fully described by the public key k, and given k one can efficiently generate $|\psi_k\rangle$. Our task then is to construct two families of functions $\{s_k\}_{k\in\mathcal{K}^{\text{high}}}$ and $\{s_k\}_{k\in\mathcal{K}^{\text{low}}}$ indexed by key sets $\mathcal{K}^{\text{high}}$ and $\mathcal{K}^{\text{low}}$, respectively, such that

(i) for $k \in \mathcal{K}^{\text{low}}$, the state $|\psi_k\rangle$ has low entanglement entropy and for $k \in \mathcal{K}^{\text{high}}$, the state $|\psi_k\rangle$ has high entanglement entropy, but

(ii) it is computationally hard to distinguish keys in $\mathcal{K}^{\text{high}}$ from those in $\mathcal{K}^{\text{low}}$.

To construct these functions, recall from Lemma 2.10 that if we define a matrix $T \in \{\pm 1\}^{2^{n/2}\times 2^{n/2}}$ by $T_{ij} = (-1)^{s_k(i\|j)}$, then

$$-\log\left(\left\|\frac{1}{2^n}TT^\top\right\|_2\right) \le S(\psi_X) \le \log \operatorname{rank}(T)\,.$$

Therefore, for the high-entanglement states we need to show that $\left\|\frac{1}{2^n}TT^\top\right\|_2$ is small, and for the low-entanglement case we need to show that $\operatorname{rank}(T)$ is small.

If one samples s_k from a 4-wise independent function family, one can show that $\left\|\frac{1}{2^n}TT^\top\right\|_2$ is indeed exponentially small. We take this as our starting point and now want to modify this s_k to "remove" entanglement to get low-entanglement states, i.e. we need to reduce the rank of the corresponding matrix T. One natural way to do this is to repeat rows of T: if we consider some many-to-one function h, then the matrix $\tilde{T}_{ij} \coloneqq T_{h(i),j}$ is the same as T, except instead of all of the rows of T, the matrix $\tilde{T}$ only contains (many copies) of those rows in T whose index is in $\operatorname{img} h$. Hence, the rank of $\tilde{T}$ is at most $\operatorname{img} h$. We can incorporate this row repetition procedure into our definition of our function s_k to get an "augmented phase function" whose states $|\psi_k\rangle$ have low entanglement. The technical term we use to describe removing entanglement by means of row repetitions is *smashing down* the entanglement.

Of course if for the high-entanglement case our s_k was simply a 4-wise independent function, but for the low-entanglement case it was augmented with this row reduction procedure, the two cases would be easily distinguishable given a description of either function. In other words, we need to smash down the entanglement in a computationally undetectable way. To solve this problem, in the high-entanglement case we will also augment s_k by a "fake" row reduction procedure that is computationally indistinguishable from the procedure in the low-entanglement case, but that does not actually meaningfully reduce the rank of the matrix T. For this, we use the lossy function construction from Section 3.1: in the low-entanglement case, the row repetition function h described above will be a compressing function and therefore reduce the rank of the matrix T; for the high-entanglement case, the function h is an almost injective function (Theorem 3.3), which we show does not reduce the Frobenius norm of $TT^\intercal$ too much. Since the compressing and almost injective functions are computationally indistinguishable (even given a public key description of them), the descriptions of the corresponding augmented phase functions s_k are also computationally indistinguishable.

We now give a formal description of this construction.

Definition 3.12. Fix a function $f(n)$. (This will be treated as a parameter of the construction.) Let $H_n = \{h_k : \{0,1\}^n \to \{0,1\}\}_{k\in\mathcal{K}_n^4}$ be a 4-wise independent family as given in Lemma 2.2. Instantiate the lossy functions from Section 3.1 with parameters $\ell(m) = \sqrt{f(2m)}$ and $r(m) = 2$. (Recall that $m \coloneqq n/2$.)

We first describe the sampling procedure for the keys $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$.

(i) To sample $k \in \mathcal{K}_n^{\text{low}}$, sample $k^{\text{rep}} \leftarrow \mathcal{K}_m^{\text{lossy}}$ and $k^{\text{fin}} \in \mathcal{K}_n^4$ uniformly. Set $k = (k^{\text{rep}}, k^{\text{fin}})$.

(ii) To sample $k \in \mathcal{K}_n^{\text{high}}$, sample $k^{\text{rep}} \leftarrow \mathcal{K}_m^{\text{inj}}$ and $k^{\text{fin}} \in \mathcal{K}_n^4$ uniformly. Set $k = (k^{\text{rep}}, k^{\text{fin}})$.

For $k = (k^{\text{rep}}, k^{\text{fin}})$, define the *labelling function* $r_k : \{0,1\}^n \to \{0,1\}^n$ by

$$r_k(x) = (f_{k^{\text{rep}}}(i) \,\|\, j) \qquad \text{with } i = \text{MSB}_m(x), j = \text{LSB}_m(x)\,.$$

We next define the function $s_k : \{0,1\}^n \to \{0,1\}$ as

$$s_k(x) = h_{k^{\text{fin}}}(r_k(x))\,.$$

The states $|\psi_k\rangle$ are then given by

$$|\psi_k\rangle = \sum_{x\in\{0,1\}^n} (-1)^{s_k(x)}|x\rangle\,.$$

Theorem 3.13.

(i) *Under the standard LWE assumption (Assumption 2.18), for any function $f(n) = n^\delta$ for $\delta > 0$, the state families $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{high}}}$ from Definition 3.12 form a pseudoentangled state ensemble with entanglement gap $(O(f(n)),\Omega(n))$ across the cuts $X_n = [n/2]$.*

(ii) *Under the subexpoential-time LWE assumption (Assumption 2.19), there exists a function $f(n) = \operatorname{poly}\log n$ such that the state families $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{high}}}$ from Definition 3.12 form a pseudoentangled state ensemble with entanglement gap $(O(f(n)),\Omega(n))$ across the cuts $X_n = [n/2]$.*

Proof. We need to check the properties required in Definition 3.9. Items (i) and (ii) are obvious. Item (iii) is also immediate because the function $s_k(x)$ is an efficiently computable classical function, so it follows from the standard phase oracle construction that $|\psi_k\rangle$ can be constructed efficiently, too. It Theorem 3.3 Item (iii) that the key families $\mathcal{K}^{\text{high}}$ and $\mathcal{K}^{\text{low}}$ are computationally indistinguishable for all choices $f(n) = n^\delta$ for $\delta > 0$ under the standard LWE assumption, and that they are indistinguishable for some (sufficiently large) $f(n) = O(\operatorname{poly}\log n)$. The proof of Item (v) is slightly more involved, so we show it separately as Lemma 3.14 below. □

Lemma 3.14. *Using the same setup as in Theorem 3.13, we have that*

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}[S((\psi_k)_{X_n}) \le f(n)] \ge 1 - \operatorname{negl}(n)\,,$$
$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}[S((\psi_k)_{X_n}) \ge n/8] \ge 1 - \operatorname{negl}(n)\,.$$

Proof. The states $|\psi_k\rangle$ in Definition 3.9 are phase states, so viewing s_k as a function $s_k : \{0,1\}^m \to \{0,1\}^m \to \{0,1\}$, we can define the matrix $T_k \in \{\pm 1\}^{2^m\times 2^m}$ as in Definition 2.9. From Lemma 2.10 we then have that

$$-\log\left(\left\|\frac{1}{2^n}T_kT_k^\top\right\|_2\right) \le S((\psi_k)_{X_n}) \le \log\operatorname{rank}(T_k)\,.$$

To prove the first statement in the lemma, we therefore need to bound the probability that T_k has large rank if $k = (k^{\text{rep}}, k^{\text{fin}}) \in \mathcal{K}_n^{\text{low}}$. For this, observe that by construction T_k has at most $|\operatorname{img} f_{k^{\text{rep}}}|$ distinct rows. Therefore, recalling that we chose $\ell(m) = \sqrt{f(n)}$ (with $n = 2m$ as before) we get from Theorem 3.3 Item (ii) that

$$\begin{aligned}\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}[S((\psi_k)_{X_n}) > f(n)] &\le \Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}[\log\operatorname{rank} T_k > f(n)]\\ &\le \Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}\left[|\operatorname{img} f_{k^{\text{rep}}}| > 2^{\ell(m)^2}\right] \le 2^{-\ell(m)} = \operatorname{negl}(n)\,.\end{aligned}$$

Here we used that $\ell(m) = \log(m)^{1+\delta}$ for some $\delta > 0$ by Theorem 3.3 Item (iii), so $2^{-\ell(m)} = \operatorname{negl}(n)$.

To prove the second statement in the lemma, we need to bound the probability that $T_kT_k^\top$ has large Frobenius norm. We will do this by computing the expectation of the Frobenius norm and then applying

Markov's inequality. We begin by expanding the Frobenius norm and using that $T_{ij} \in \{\pm 1\}$:

$$\begin{aligned}
\mathbb{E}_{k \leftarrow \mathcal{K}_n^{\text{high}}}\left[\|TT^{\mathsf{T}}\|_2^2\right] &= \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\left(\sum_{l \in \{0,1\}^m} T_{il}T_{jl}\right)^2\right] \\
&= \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\sum_{a,b \in \{0,1\}^m} T_{ia}T_{ja}T_{ib}T_{jb}\right] \\
&= \sum_{i \in \{0,1\}^m} \mathbb{E}\left[\sum_{a,b \in \{0,1\}^m} T_{ia}T_{ia}T_{ib}T_{ib}\right] + \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\sum_{a \in \{0,1\}^m} T_{ia}T_{ja}T_{ia}T_{ja}\right] \\
&\quad + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \mathbb{E}\left[\sum_{\substack{a,b \in \{0,1\}^m \\ a \neq b}} T_{ia}T_{ja}T_{ib}T_{jb}\right] \\
&= 2^{3m} + 2^{3m} + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \mathbb{E}\left[\sum_{\substack{a,b \in \{0,1\}^m \\ a \neq b}} T_{ia}T_{ja}T_{ib}T_{jb}\right] \\
&= 2^{3m+1} + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \sum_{\substack{a,b \in \{0,1\}^m \\ a \neq b}} \mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right]. \qquad (3.5)
\end{aligned}$$

Since $s_k(x) = h_{k^{\text{fin}}}(r_k(x))$, and $h_{k^{\text{fin}}}$ is drawn from a 4-wise independent function family, it is easy to see that the term $\mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right]$ is zero unless the 4 terms in the exponents pair up to cancel. In particular, this means that a necessary condition for $\mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right] \neq 0$ is that

$$r_k(i \,\|\, a) = r_k(i \,\|\, b) \qquad \text{or} \qquad r_k(i \,\|\, a) = r_k(j \,\|\, a) \qquad \text{or} \qquad r_k(i \,\|\, a) = r_k(j \,\|\, b).$$

Since $a \neq b$, from the definition of r_k we see that the first and last case never occur. The second case is equivalent to $f_{k^{\text{rep}}}(i) = f_{k^{\text{rep}}}(j)$. We can bound this using the properties of $f_{k^{\text{rep}}}$. For this, recall that $k^{\text{rep}} = (A, k^{\text{hash}})$. We call a choice of A "good" if $\{f_{(A,k^{\text{hash}})}\}_{k^{\text{hash}}}$ forms a 2-wise independent family.

$$\begin{aligned}
\Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}}[f_{k^{\text{rep}}}(i) = f_{k^{\text{rep}}}(j)] &= \Pr_{k^{\text{rep}} \leftarrow \mathcal{K}_m^{\text{inj}}}[f_{k^{\text{rep}}}(i) = f_{k^{\text{rep}}}(j)] \\
&\leq \Pr_{k^{\text{rep}}=(A,k^{\text{hash}}) \leftarrow \mathcal{K}_m^{\text{inj}}}[f_{k^{\text{rep}}}(i) = f_{k^{\text{rep}}}(j) \mid A \text{ good}] + \Pr_{k^{\text{rep}}=(A,k^{\text{hash}}) \leftarrow \mathcal{K}_m^{\text{inj}}}[A \text{ not good}] \\
&\leq O(2^{-m}).
\end{aligned}$$

The last line follows because for a good A, the probability that $f_{k^{\text{rep}}}(i) = f_{k^{\text{rep}}}(j)$ (for $i \neq j$) is 2^{-m} by 2-wise independence, and the probability that A is not good is $O(2^{-m})$ by Theorem 3.3 Item (i). Therefore,

$$\sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \sum_{\substack{a,b \in \{0,1\}^m \\ a \neq b}} \mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right] \leq 2^{4m} \cdot O(2^{-m}) = O(2^{3m}).$$

Inserting this into Equation (3.5), we get that

$$\mathbb{E}_{k \leftarrow \mathcal{K}_n^{\text{high}}}\left[\|TT^{\mathsf{T}}\|_2^2\right] \leq O(2^{3m}).$$

Therefore we get from Markov's inequality:

$$\begin{aligned}\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[-\log\left\|\frac{1}{2^n}T_{X,k}T_{X,k}^{\intercal}\right\|_2<\frac{m}{4}\right]&=\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[\left\|T_{X,k}T_{X,k}^{\intercal}\right\|_2^2>2^{2n-m/2}\right]\\&\leq\frac{1}{2^{2n-m/2}}\,\mathbb{E}_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[\left\|T_{X,k}T_{X,k}^{\intercal}\right\|_2^2\right]\\&\leq O(2^{3m-4m+m/2})=O(2^{-m/2}),\end{aligned}$$

where we inserted $n=2m$. □

3.2.1 Application: quantum entropy difference problem with maximal gap

One immediate application of our single-cut construction is that we get a maximal stretching of the entropy gap for the quantum entropy difference problem studied in [GH20]. To recap, the problem is as follows:

Definition 3.15 (Quantum entropy difference problem)**.** Given two circuits C_1 and C_2 each acting on n qubit, decide whether or not $S(\rho_A)>S(\sigma_A)$, where ρ_A and σ_A are the reduced density matrices of the states $|\psi_1\rangle=C_1|0^n\rangle$ and $|\psi_2\rangle=C_2|0^n\rangle$ with the last $n/2$ qubits traced out.

Under the subexponential-time LWE assumption (Assumption 2.19), our construction in Section 3.2 yields C_1 and C_2 such that $S(\rho_A)=\Omega(n)$ and $S(\sigma_A)=\operatorname{poly}\log n$, yet the quantum entropy difference problem still remains hard for any polynomially bounded quantum algorithm. From Remark 3.11, it can be argued that this entropy gap is maximal. Previously, the entropy gap in [GH20] was only $O(1)$. Note that by the same arguments as [GH20], our circuits can also be made shallow depth—that is, they are in NC^1.

A different version of the entropy difference problem, called the Hamiltonian quantum entropy difference problem, also appears in [GH20], where, instead of circuits, the input is the description of two Hamiltonians, and the task is to distinguish between different entanglement entropies across a fixed cut of the ground states of these Hamiltonians. [GH20] showed that this problem is LWE-hard for $O(1)$ entropy gaps. Our construction achieves hardness for a maximal entropy gap of $\operatorname{poly}\log n$ vs n for that problem, too, by running our pseudoentanglement construction through a history state Hamiltonian construction in the same manner as in [GH20].

In Section 4 we will consider a much stronger version of this problem: instead of distinguishing Hamiltonians with ground states whose entanglement differs across a single cut, we will construct indistinguishable Hamiltonians whose ground states have qualitatively different entanglement structures, e.g. near area-law vs volume-law entanglement. This will require states that are pseudoentangled across many cuts simultaneously, which we construct in the next section.

3.3 Area-law public-key pseudoentangled states on a 1D line

In this section we will give a (nearly) area-law public-key pseudoentangled states construction on a line based on the row repetition technique we introduced in Section 3.2. This means that we will construct public-key pseudoentangled states such that if we imagine the qubits arranged on a line, the entanglement gap is $\operatorname{poly}\log n$ vs n across all cuts that separate the qubits into left and right qubits on the line.

We begin by formally defining this multi-cut version of pseudoentanglement. The definition is almost identical to Definition 3.9, except that we now need to require an entanglement gap across all cuts on a line simultaneously. One slight subtlety is that if we consider cuts close to the end of the line, the entanglement will be low simply by virtue of the fact that there are only very few qubits on one side of the cut. Therefore, in

the high-entanglement case, we need to require the entanglement to be at least $g(\text{distance from end of line})$ rather than simply $g(n)$. Furthermore, very close to the boundary (namely, $O(\log n)$ close), certain properties of our construction break down. Therefore, we only consider cuts that are at least $\omega(\log n)$ far from the boundary. Since we are primarily interested in large entanglement gaps of the form $(O(\text{poly}\log n), \Omega(n))$, this small boundary region is of no particular interest to us. Nonetheless, it is possible to modify our construction to work for such small boundary regions too; we briefly sketch this in Section 3.3.3.

As in the single-cut case, we use entanglement gaps of the form $(O(f(n)), \Omega(g(n)))$ for pseudoentangled states where we only have an upper bound on the entanglement in the low-entanglement case and a lower bound in the high-entanglement case (see Remark 3.10 for details). To simplify the definition slightly, below we state the definition directly for this case; it is straightforward to adapt it to the case where one wants the exact scaling rather than one-sided bounds, but we will not need this for our results.

Definition 3.16 (Public-key pseudoentanglement across geometrically local cuts in 1D)**.** A public-key pseudoentangled state ensemble with entanglement gap $(O(f(n)), \Omega(g(n)))$ across geometrically local cuts on a 1D line consists of two sequences of families of quantum states $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{high}}}$ indexed by key sets $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$ respectively that satisfy Items (i) to (iv) from Definition 3.9 and the following modified version of Item (v) from Definition 3.9:

(v') For any function $b(n) = \omega(\log n)$, with overwhelming probability, states in Ψ_n^{low} have entanglement entropy $O(f(n))$ and states in Ψ_n^{high} have entanglement entropy $\Omega(g(\text{distance from end of line}))$ for all geometrically local cuts that are at least $b(n)$ far from the end of the line. Formally,

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}\left[\forall c \in \{b(n),\dots,n-b(n)\} :\ S((\psi_k)_{[c]}) \le O(f(n))\right] \ge 1-\text{negl}(n),$$
$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[\forall c \in \{b(n),\dots,n-b(n)\} :\ S((\psi_k)_{[c]}) \ge \Omega\big(\min(g(c), g(n-c))\big)\right] \ge 1-\text{negl}(n).$$

Here, $(\psi_k)_{[c]}$ is the reduced states of $|\psi_k\rangle$ on qubits $(1,\dots,c)$.

Overview. We first give an informal overview of our construction and proof. Recall the high-level idea for single-cut pseudoentanglement: we started from a phase-state whose phases where chosen in a 4-wise independent way and then "smashed down" the entanglement across a particular cut by repeating rows in the matrix T associated with the phase state (see Definition 2.9) associated with that cut. To generalise this to all geometrically local cuts on the 1-D line, we can sequentially apply this single cut technique. Specifically, we again begin with a phase state and consider a cut on right end of the 1D line. We can then reduce the T-matrix across that cut as in the single cut construction. The modified T-matrix corresponds to a modified phase state which is now guaranteed to have high or low entanglement across the cut we chose. We can now consider the next cut, moving right to left. Starting from the modified phase state from the first iteration of the procedure, we can again consider the associated T-matrix, but now across the second cut, and again use the row-repetition procedure as in the single cut case. Performing this procedure for all cuts, moving right to left cut-by-cut, we obtain our final states.

The key difficulty in the proof is to show that subsequent row repetition operations do not tamper with the entanglement structure across previous cuts. For the low entanglement ensemble, one might worry that future row repetition might increase the rank of the T-matrix across previous cuts. We prove that if the cuts are treated in the correct order, this does not happen, later treatments never jeopardize the low entanglement status we established for previous cuts. Combining this with the single cut analysis, we conclude that the low entanglement ensemble enjoys the same low entanglement guarantee as in the single cut analysis for each cut.

For the high entanglement ensemble, one might worry about the opposite direction, namely that treating future cuts might *reduce* the rank of the T-matrix for previous cuts. Indeed, this might happen because the functions we use for the row repetition operations in the high entanglement case are not perfectly injective, only "almost injective" as shown in Theorem 3.3. To show that nonetheless the entanglement across all cuts remains high, we prove a similar upper bound on the expectation of the Frobenius norm as the single cut version. The analysis is somewhat complicated and relies on the statistical properties of the "almost injective functions" from Theorem 3.3 and the structure of the iterated row repetition operations.

We begin by describing our construction for the multi-cut case. This is analogous to the single-cut case (Definition 3.12), except that we now need to iterate the row repetition operations, so the function r_k from Definition 3.12 needs to be modified and defined recursively.

Definition 3.17. Fix a function $f(n)$ (this will be treated as a parameter of the construction). Let $H_n = \{h_k : \{0,1\}^n \to \{0,1\}\}_{k\in\mathcal{K}_n^4}$ be a 4-wise independent family as given in Lemma 2.2. For $m \in \{f(n), f(n)+1, \ldots, n\}$, instantiate the m-bit lossy function from Section 3.1 with parameters $\ell(m) = \sqrt{f(n)}$ and $r(m) = 2$.

We first describe the sampling procedure for the keys $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$.

(i) To sample $k \in \mathcal{K}_n^{\text{low}}$, for $m \in \{f(n), f(n)+1, \ldots, n\}$, independently sample $k_m^{\text{rep}} \leftarrow \mathcal{K}_m^{\text{lossy}}$ (see Definition 3.2) and $k^{\text{fin}} \in \mathcal{K}_n^4$ uniformly. Set $k = (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \ldots, k_n^{\text{rep}}, k^{\text{fin}})$.

(ii) To sample $k \in \mathcal{K}_n^{\text{high}}$, for $m \in \{f(n), f(n)+1, \ldots, n\}$, independently sample $k_m^{\text{rep}} \leftarrow \mathcal{K}_m^{\text{inj}}$ and $k^{\text{fin}} \in \mathcal{K}_n^4$ uniformly. Set $k = (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \ldots, k_n^{\text{rep}}, k^{\text{fin}})$.

For $k = (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \ldots, k_n^{\text{rep}}, k^{\text{fin}})$, define the *labelling functions* $r_k^{f(n)}, \ldots, r_k^n : \{0,1\}^n \to \{0,1\}^n$ recursively by

$$r_k^m(x) = \begin{cases} x & m = n+1, \\ r_k^{m+1}(f_{k_m^{\text{rep}}}(i) \parallel j) & f(n) \le m \le n, \text{MSB}_m(x) = i, \text{LSB}_{n-m}(x) = j, \end{cases}$$

where $\text{MSB}_m(x)$ is the first m bits of x, $\text{LSB}_m(x)$ is the last m bits of x, and $i \parallel j$ is the concatenation of bit strings i and j. For simplicity, we define $r_k(x) = r_k^{f(n)}(x)$.

With this notation, for $k = (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \ldots, k_n^{\text{rep}}, k^{\text{fin}})$, we next define the function $s_k : \{0,1\}^n \to \{0,1\}$ as

$$s_k(x) = h_{k^{\text{fin}}}(r_k(x)),$$

The states $|\psi_k\rangle$ are then given by

$$|\psi_k\rangle = \sum_{x\in\{0,1\}^n} (-1)^{s_k(x)} |x\rangle.$$

Our main result is that this construction satisfies the requirements from Definition 3.16 as summarised by the following theorem. In particular, we show that under the subexponential-time LWE assumption, our construction achieves an entanglement gap of $\text{poly}\log n$ vs n, which is essentially optimal by Remark 3.11. On a 1D line, this entanglement scaling corresponds to area-law (up to $\text{poly}\log$ factors) vs volume law entanglement, which is why we call this result area-law pseudoentangled states.

Theorem 3.18.

(i) *Under the standard LWE assumption (Assumption 2.18), for any function $f(n) = n^\delta$ for $\delta > 0$, the state families $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{high}}}$ from Definition 3.17 form a pseudoentangled state ensemble with entanglement gap $(O(f(n)), \Omega(n))$ across geometrically local cuts in 1D (Definition 3.16).*

(ii) *Under the subexponential-time LWE assumption (Assumption 2.19), there exists a function* $f(n) = \operatorname{poly}\log n$ *such that the state families* $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{low}}}$ *and* $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k\in\mathcal{K}_n^{\text{high}}}$ *from Definition 3.17 form a pseudoentangled state ensemble with entanglement gap* $(O(f(n)), \Omega(n))$ *across geometrically local cuts in 1D (Definition 3.16).*

Proof. We need to check the properties required in Definition 3.16. Items (i) to (iv) hold by the same argument as in Theorem 3.13. The proof of Item (v') is more involved. We show the entanglement scaling for the low-entanglement states in Proposition 3.19 and for the high-entanglement states in Proposition 3.24. □

3.3.1 Low-entanglement states

Proposition 3.19. *Using the same setup as in Theorem 3.18, for any* $c \in [n]$ *we have that*

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{low}}}\left[\forall j = 1,\dots,n:\ S((\psi_k)_{[c]}) \le O(f(n))\right] \ge 1 - \operatorname{negl}(n)\,.$$

Proof. If $c < f(n)$ the statement holds trivially because then $(\psi_k)_{[c]}$ has at most $f(n)$ qubits, and therefore at most entropy $f(n)$. Hence fix any $c \in \{f(n),\dots,n\}$ and consider the cut between the first c qubits and the last $n-c$ qubits. As in Definition 2.9, we can define the matrix $T \in \{\pm 1\}^{2^c\times 2^{n-c}}$ by

$$T_{ij} = (-1)^{s_k(i\|j)} = (-1)^{h_{k^{\text{fin}}}(r_k(i\|j))}\,.$$

Then by Lemma 2.10, it suffices to show that the rank of this matrix is bounded by $2^{O(f(n))}$ with overwhelming probability.

Define the functions $\tilde{r}_k^m : \{0,1\}^c \to \{0,1\}^{2^{n-c}}$ by

$$\tilde{r}_k^m(i) = (r_k^m(i \parallel j))_{j\in\{0,1\}^{n-c}}\,.$$

In particular, $\tilde{r}_k(i) := \tilde{r}_k^{f(n)}(i)$ outputs the i-th row of T prior to applying the hash function $h_{k^{\text{fin}}}$.

From the recursive definition of r_k, it is easy to see that for $i \in \{0,1\}^c, j \in \{0,1\}^{n-c}$ we can write $r_k(i \parallel j) = \xi(r_k^c(\zeta(i)) \parallel j)$ for some functions ξ, ζ whose details do not matter here. This implies that $|\operatorname{img}\tilde{r}_k| \le |\operatorname{img}\tilde{r}_k^c|$. We then have that

$$\operatorname{rank}(T) \le |\operatorname{img}\tilde{r}_k| \le |\operatorname{img}\tilde{r}_k^c| \le |\operatorname{img} f_{k_c^{\text{rep}}}|\,,$$

where the first inequality holds because the number of distinct rows in T is at most $|\operatorname{img}\tilde{r}_k|$, the second inequality follows from the argument above, and the third inequality follow from the definition of r_k^c in Definition 3.17. Having reduced the problem to bounding the image size of $f_{k_c^{\text{rep}}}$, the lemma now follows exactly like Lemma 3.14. □

3.3.2 High-entanglement states

We will now show that despite using the imperfect injective functions from Theorem 3.3, the states in Ψ_n^{high} from our construction in Definition 3.17 have high entanglement across every geometrically local cut on a 1D line (sufficiently far from the end of the line). The keys in $\mathcal{K}_n^{\text{high}}$ are of the form $k = (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \dots, k_n^{\text{rep}}, k^{\text{fin}})$, and each k_m^{rep} has the form $k_m^{\text{rep}} = (A_m, k_m^{\text{hash}})$. By Item (i) of Theorem 3.3, we know that with overwhelming probability over the choice of the matrix A_m (as long as $m = \omega(\log n)$), the family $\{f_{(A_m,k_m^{\text{hash}})}\}_{k_m^{\text{hash}}}$ is pairwise

independent. We call a matrix A_m "good" if this is the case. We then define a "good" key $k \in \mathcal{K}_n^{\text{high}}$ as one for which all the A_m-matrices are good:

$$\mathcal{K}_n^{\text{high}}\big|_{\text{good}} = \left\{ (k_{f(n)}^{\text{rep}}, k_{f(n)+1}^{\text{rep}}, \ldots, k_n^{\text{rep}}, k^{\text{fin}}) \in \mathcal{K}_n^{\text{high}} \text{ s.t. } \forall m : k_m^{\text{rep}} = (A_m, k_m^{\text{hash}}) \text{ has a good } A_m \right\}.$$

We write $k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}$ to denote a key sampled as before, but conditioned on getting a good key.

We being by showing a few useful properties of the r_k^m-functions.

Lemma 3.20. *Instantiate the construction from Definition 3.17 with any choice of function $f(n)$. For any $x, y, x', y' \in \{0,1\}^n$ and $m \in \{f(n), f(n)+1, \ldots, n\}$ such that $x \neq y$, $x' \neq y'$, $\text{LSB}_{n-m}(x) = \text{LSB}_{n-m}(x')$, and $\text{LSB}_{n-m}(y) = \text{LSB}_{n-m}(y')$, the following two properties hold:*

$$\Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}[r_k^m(x) = r_k^m(y)] = \begin{cases} \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[r_k^{m+1}(x) = r_k^{m+1}(y)\right] & \text{if } \text{LSB}_{n-m}(x) \neq \text{LSB}_{n-m}(y) \\ \frac{1}{2^m} + \frac{2^m-1}{2^m} \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[r_k^{m+1}(x) = r_k^{m+1}(y)\right] & \text{if } \text{LSB}_{n-m}(x) = \text{LSB}_{n-m}(y), \end{cases}$$

and

$$\Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}[r_k^m(x) = r_k^m(y)] = \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[r_k^m(x') = r_k^m(y')\right].$$

Proof. For ease of exposition, let $p_{x,y}^m = \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[r_k^m(x) = r_k^m(y)\right]$. Throughout the proof all probabilities are over $k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}$. We prove the lemma by induction.

From the definition of $r^{n+1}(x)$ we have

$$\begin{aligned} p_{x,y}^n &= \sum_{x',y' \in \{0,1\}^n} \Pr[f_{k_n^{\text{rep}}}(x) = x' \wedge f_{k_n^{\text{rep}}}(y) = y'] \cdot p_{x',y'}^{n+1} \\ &= \frac{1}{2^n} \\ &= \frac{1}{2^n} + \frac{2^n-1}{2^n} \Pr_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[r_k^{n+1}(x) = r_k^{n+1}(y)\right]. \end{aligned}$$

The second line holds because $f_{k_n^{\text{rep}}}$ is pairwise independent conditioned on good k, and $p_{x',y'}^{n+1} = 0$ for any $x', y' \in \{0,1\}^n$ such that $x \neq y$. This shows the lemma for $m = n$ since trivially $\text{LSB}_0(x) = \text{LSB}_0(y)$ (so we are in the second case for the first equation in the lemma) and we have shown that $p_{x,y}^n$ is independent of x, y (so the second equation in the lemma holds).

Now assuming the claim holds for $m+1$, we will argue that it also holds for m. Let $i = \text{MSB}_m(x)$, $j = \text{MSB}_m(y)$, $a = \text{LSB}_{n-m}(x)$, $b = \text{MSB}_m(y)$. In particular, we have the following useful observation: if $\text{LSB}_{n-m}(x) = \text{LSB}_{n-m}(y)$ then $\text{LSB}_{n-m-1}(x) = \text{LSB}_{n-m-1}(y)$.

Case 1: $a \neq b$ and $i \neq j$. Since $f_{k_m^{\text{rep}}}$ is pairwise independent conditioned good k, and $\{k_m^{\text{rep}}\}$ are sampled independently for different m, we have

$$
\begin{aligned}
p^m_{x,y} &= \sum_{i',j' \in \{0,1\}^m} \Pr[f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}(i) = i' \wedge f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}(j) = j'] \cdot p^{m+1}_{i' \| a, j' \| b} \\
&= \frac{1}{2^{2m}} \sum_{i',j' \in \{0,1\}^m} p^{m+1}_{i' \| a, j' \| b} \\
&= \frac{1}{2^{2m}} \sum_{i',j' \in \{0,1\}^m} p^{m+1}_{x,y} \\
&= p^{m+1}_{x,y},
\end{aligned}
$$

where the third line uses the induction hypothesis. The second property is obvious, by induction hypothesis, $p^m_{x,y} = p^{m+1}_{x,y} = p^{m+1}_{x',y'} = p^{m+1}_{x',y'}$.

Case 2: $a \neq b$ and $i = j$. Similarly, by the fact that $f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}$ is pairwise independent conditioned good k, and $\{k^{\mathrm{rep}}_m\}$ are sampled independently for different m, we have

$$
\begin{aligned}
p^m_{x,y} &= \sum_{i' \in \{0,1\}^m} \Pr[f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}(i) = i'] \cdot p^{m+1}_{i' \| a, i' \| b} \\
&= \frac{1}{2^m} \sum_{i' \in \{0,1\}^m} p^{m+1}_{i' \| a, i' \| b} \\
&= \frac{1}{2^m} \sum_{i' \in \{0,1\}^m} p^{m+1}_{x,y} \\
&= p^{m+1}_{x,y},
\end{aligned}
$$

where the third line uses the induction hypothesis. Similarly, the second property holds for this case.

Case 3: $a = b$ and $i \neq j$. Similarly, by the fact that $f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}$ is pairwise independent conditioned good k, and $\{k^{\mathrm{rep}}_m\}$ are sampled independently for different m, we have

$$
\begin{aligned}
p^m_{x,y} &= \sum_{i',j' \in \{0,1\}^m} \Pr[f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}(i) = i' \wedge f^{\mathrm{rep}}_{k^{\mathrm{rep}}_m}(j) = j'] \cdot p^{m+1}_{i' \| a, j' \| a} \\
&= \frac{1}{2^{2m}} \sum_{i' \in \{0,1\}^n} p^{m+1}_{i' \| a, i' \| a} + \frac{1}{2^{2m}} \sum_{\substack{i',j' \in \{0,1\}^m \\ i' \neq j'}} p^{m+1}_{i' \| a, j' \| a} \\
&= \frac{1}{2^m} + \frac{1}{2^{2m}} \sum_{\substack{i',j' \in \{0,1\}^m \\ i' \neq j'}} p^{m+1}_{x,y} \\
&= \frac{1}{2^m} + \frac{2^m - 1}{2^m} p^{m+1}_{x,y},
\end{aligned}
$$

where the third line uses the induction hypothesis. Similarly, the second property holds for this case. □

Lemma 3.21. *Instantiate the construction from Definition 3.17 with any choice of function $f(n)$. For any $d \in [n]$ and $x, y \in \{0,1\}^n$ such that $\mathrm{LSB}_d(x) = \mathrm{LSB}_d(y)$ and $\mathrm{LSB}_{d+1}(x) \neq \mathrm{LSB}_{d+1}(y)$, the following holds:*

$$\Pr_{k \leftarrow \mathcal{K}_n^{\mathrm{high}}\big|_{\mathrm{good}}}[r_k(x) = r_k(y)] \leq \frac{2^{d+1}}{2^n}.$$

Proof. For ease of exposition, we again abbreviate $p_{x,y}^m = \Pr_{k \leftarrow \mathcal{K}_n^{\mathrm{high}}\big|_{\mathrm{good}}}[r_k(x) = r_k(y)]$. By Lemma 3.20 we have the following recursive relationship:

$$p_{x,y}^m = \begin{cases} \frac{1}{2^m} + \frac{2^m - 1}{2^m} p_{x,y}^{m+1} & \text{if } \mathrm{LSB}_{n-m}(x) = \mathrm{LSB}_{n-m}(y) \\ p_{x,y}^{m+1} & \text{otherwise} \end{cases},$$

with the boundary condition $p_{x,y}^{n+1} = 0$.

For $x, y \in \{0,1\}^n$ such that $\mathrm{LSB}_d(x) = \mathrm{LSB}_d(y)$ and $\mathrm{LSB}_{d+1}(x) \neq \mathrm{LSB}_{d+1}(y)$, we have

$$\begin{aligned} p_{x,y}^{f(n)} &\leq \sum_{m=f(n)}^{n} \frac{\mathbb{1}[\mathrm{LSB}_{n-m}(x) = \mathrm{LSB}_{n-m}(x)]}{2^m} \\ &\leq \sum_{m=n-d}^{n} \frac{1}{2^m} \\ &\leq \frac{2^{d+1}}{2^n}, \end{aligned}$$

as desired. □

Corollary 3.22. *Instantiate the construction from Definition 3.17 with any choice of function $f(n)$. For any $x \in \{0,1\}^n$, the following holds:*

$$\sum_{\substack{y \in \{0,1\}^n \\ x \neq y}} \Pr[r_k(x) = r_k(y)] \leq n.$$

Proof. Observe that for any given x, the number of $y \in \{0,1\}^n$ such that $\mathrm{LSB}_d(x) = \mathrm{LSB}_d(y)$ but $\mathrm{LSB}_{d+1}(x) \neq \mathrm{LSB}_{d+1}(y)$ is $\frac{2^n}{2^{d+1}}$. Therefore, splitting up the sum over y depending on the first bit on which x and y differ, we get from Lemma 3.21 that

$$\begin{aligned} \sum_{\substack{y \in \{0,1\}^n \\ x \neq y}} \Pr[r_k(x) = r_k(y)] &= \sum_{d=0}^{n-1} \sum_{\substack{y \in \{0,1\}^n \\ \mathrm{LSB}_d(x) = \mathrm{LSB}_d(y) \\ \mathrm{LSB}_{d+1}(x) \neq \mathrm{LSB}_{d+1}(y)}} \Pr[r_k(x) = r_k(y)] \\ &\leq \sum_{d=0}^{n-1} \frac{2^n}{2^{d+1}} \frac{2^{d+1}}{2^n} \\ &= n. \end{aligned}$$

□

Now we can use this lemma to upper bound the expectation of the Frobenius norm of the T-matrix (see Definition 2.9) associated *any* cut $X \subset [n]$. While Theorem 3.18 only requires us to consider geometrically local cuts, the proof works for arbitrary cuts, which we will make use of in Section 3.4. Specifically, we have the following lemma.

Lemma 3.23. *Instantiate the construction from Definition 3.17 with any choice of function $f(n)$ and consider any cut $X \subseteq [n]$ of size $m := |X| \leq n/2$. Let $T_{X,k}$ be the T-matrix (Definition 2.9) for $|\psi_k\rangle$ associated with cut X. Then we have the following bound on the expected squared Frobenius norm:*

$$\mathbb{E}_{k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}} \left[\left\| T_{X,k} T_{X,k}^{\intercal} \right\|_2^2 \right] \leq 5n \cdot 2^{2n-m}.$$

Proof. To simplify the notation, we drop the explicit dependence on X and k and simply write $T = T_{X,k}$. All expectations are taken over $k \leftarrow \mathcal{K}_n^{\text{high}}\big|_{\text{good}}$.

The first part of the proof is almost identical to the proof of Theorem 3.13, except that now we consider cuts that do not necessarily divide the qubits into two equally sized sets. We spell out the details for completeness. Expanding the Frobenius norm and using that $T_{ij} \in \{\pm 1\}$:

$$\begin{aligned}
\mathbb{E}\left[\|TT^{\intercal}\|_2^2 \right] &= \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\left(\sum_{l \in \{0,1\}^{n-m}} T_{il} T_{jl} \right)^2 \right] \\
&= \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\sum_{a,b \in \{0,1\}^{n-m}} T_{ia} T_{ja} T_{ib} T_{jb} \right] \\
&= \sum_{i \in \{0,1\}^m} \mathbb{E}\left[\sum_{a,b \in \{0,1\}^{n-m}} T_{ia} T_{ia} T_{ib} T_{ib} \right] + \sum_{i,j \in \{0,1\}^m} \mathbb{E}\left[\sum_{a \in \{0,1\}^{n-m}} T_{ia} T_{ja} T_{ia} T_{ja} \right] \\
&\quad + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \mathbb{E}\left[\sum_{\substack{a,b \in \{0,1\}^{n-m} \\ a \neq b}} T_{ia} T_{ja} T_{ib} T_{jb} \right] \\
&= 2^{2n-m} + 2^{n+m} + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \mathbb{E}\left[\sum_{\substack{a,b \in \{0,1\}^{n-m} \\ a \neq b}} T_{ia} T_{ja} T_{ib} T_{jb} \right] \\
&= 2^{2n-m} + 2^{n+m} + \sum_{\substack{i,j \in \{0,1\}^m \\ i \neq j}} \sum_{\substack{a,b \in \{0,1\}^{n-m} \\ a \neq b}} \mathbb{E}\left[(-1)^{s_k(i\|a) + s_k(i\|b) + s_k(j\|a) + s_k(j\|b)} \right]. \qquad (3.6)
\end{aligned}$$

Since $s_k(x) = h_{k^{\text{fin}}}(r_k(x))$, and $h_{k^{\text{fin}}}$ is drawn from a 4-wise independent function family, it is easy to see that the term $\mathbb{E}\left[(-1)^{s_k(i\|a) + s_k(i\|b) + s_k(j\|a) + s_k(j\|b)} \right]$ is zero unless the 4 terms in the exponents pair up to cancel. In particular, this means that a necessary condition for $\mathbb{E}\left[(-1)^{s_k(i\|a) + s_k(i\|b) + s_k(j\|a) + s_k(j\|b)} \right] \neq 0$ is that

$$r_k(i \,\|\, a) = r_k(i \,\|\, b) \qquad \text{or} \qquad r_k(i \,\|\, a) = r_k(j \,\|\, a) \qquad \text{or} \qquad r_k(i \,\|\, a) = r_k(j \,\|\, b).$$

In Theorem 3.13, the probability of this event was straightforward to bound using pairwise independence.

Here, this direct argument is replaced by using Corollary 3.22. For the first case, we can bound

$$\begin{aligned}\sum_{\substack{i,j\in\{0,1\}^m\\ i\neq j}}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\Pr[r_k(i\,\|\,a)=r_k(j\,\|\,a)] &= \sum_{i\in\{0,1\}^m}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\left(\sum_{\substack{j\in\{0,1\}^m\\ i\neq j}}\Pr[r_k(i\,\|\,a)=r_k(j\,\|\,a)]\right)\\ &\leq \sum_{i\in\{0,1\}^m}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\left(\sum_{\substack{y\in\{0,1\}^n\\ y\neq(i\|a)}}\Pr[r_k(i\,\|\,a)=r_k(y)]\right)\\ &\leq 2^{2n-m}\cdot n\,.\end{aligned}$$

For the second line we have added terms to the sum in parentheses, which can only increase its value. For the third line we have used Corollary 3.22 to deduce that the term in parentheses is at most n and then counted the number of terms in the outer sum.

By analogous derivations, we also obtain

$$\begin{aligned}\sum_{\substack{i,j\in\{0,1\}^m\\ i\neq j}}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\Pr[r_k(i\,\|\,a)=r_k(i\,\|\,b)] &\leq 2^{n+m}\cdot n\,,\\ \sum_{\substack{i,j\in\{0,1\}^m\\ i\neq j}}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\Pr[r_k(i\,\|\,a)=r_k(j\,\|\,b)] &\leq 2^{n}\cdot n\,.\end{aligned}$$

Using the trivial bound $\mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right]\leq 1$, we can therefore bound the remaining sum in Equation (3.6)

$$\begin{aligned}&\sum_{\substack{i,j\in\{0,1\}^m\\ i\neq j}}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\mathbb{E}\left[(-1)^{s_k(i\|a)+s_k(i\|b)+s_k(j\|a)+s_k(j\|b)}\right]\\ &\quad\leq \sum_{\substack{i,j\in\{0,1\}^m\\ i\neq j}}\sum_{\substack{a,b\in\{0,1\}^{n-m}\\ a\neq b}}\left(\Pr[r_k(i\,\|\,a)=r_k(j\,\|\,a)]+\Pr[r_k(i\,\|\,a)=r_k(i\,\|\,b)]+\Pr[r_k(i\,\|\,a)=r_k(j\,\|\,b)]\right)\\ &\quad\leq n\cdot 2^{2n-m}+n\cdot 2^{n+m}+n\cdot 2^n\,.\end{aligned}$$

Inserting this into Equation (3.6) we get that

$$\mathbb{E}\left[\|TT^\intercal\|_2^2\right]\leq 2^{2n-m}+2^{n+m}+n\cdot 2^{2n-m}+n\cdot 2^{n+m}+n\cdot 2^n\leq 5n\cdot 2^{2n-m}$$

since we assumed that $m\leq n/2$. □

Proposition 3.24. *Using the same setup as in Theorem 3.18, for any cut $X\subseteq[n]$ of size $m:=|X|=\omega(\log n)$ we have that*

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[\forall j=1,\ldots,n:\ S((\psi_k)_X)\geq\frac{1}{4}\min(m,n-m)\right]\geq 1-\text{negl}(n)\,.$$

Proof. Without loss of generality, we can assume that $m = |X| \leq n/2$; otherwise we can simply consider the complementary cut $[n] \setminus X$ and use the fact that $S((\psi_k)_X) = S((\psi_k)_{[n]\setminus X})$. Let $T_{X,k}$ be the T-matrix (Definition 2.9) for $|\psi_k\rangle$ associated with cut X. By Lemma 2.10 it suffices to show that

$$\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[-\log\left\|\frac{1}{2^n}T_{X,k}T_{X,k}^{\intercal}\right\|_2 < \frac{m}{4}\right] \leq \text{negl}(n)\,.$$

The event that $-\log\left\|\frac{1}{2^n}T_{X,k}T_{X,k}^{\intercal}\right\|_2 < \frac{m}{4}$ is equivalent to the event that $\left\|T_{X,k}T_{X,k}^{\intercal}\right\|_2^2 > 2^{2n-m/2}$. We can bound the probability of the latter as follows. From Item (i) in Theorem 3.3 and a union bound we know that if we sample a key $k \leftarrow \mathcal{K}_n^{\text{high}}$, the probability that this key is *not* contained in $\mathcal{K}_n^{\text{high}}\big|_{\text{good}}$ at most $n\cdot 2^{-f(n)}$, which is negligible in n since we chose $f(n) = \omega(\log n)$ in Theorem 3.18. Therefore we get that

$$\begin{aligned}
\Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}}\left[-\log\left\|\frac{1}{2^n}T_{X,k}T_{X,k}^{\intercal}\right\|_2 < \frac{m}{4}\right] &\leq \Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[-\log\left\|\frac{1}{2^n}T_{X,k}T_{X,k}^{\intercal}\right\|_2 < \frac{m}{4}\right] + \text{negl}(n)\\
&= \Pr_{k\leftarrow\mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[\left\|T_{X,k}T_{X,k}^{\intercal}\right\|_2^2 > 2^{2n-m/2}\right] + \text{negl}(n)\\
&\leq \frac{1}{2^{2n-m/2}}\,\mathbb{E}_{k\leftarrow\mathcal{K}_n^{\text{high}}\big|_{\text{good}}}\left[\left\|T_{X,k}T_{X,k}^{\intercal}\right\|_2^2\right] + \text{negl}(n)\\
&\leq 5n\cdot 2^{2n-m-2n+m/2} + \text{negl}(n)\\
&= 5n\cdot 2^{-m/2} + \text{negl}(n)\\
&= \text{negl}(n)\,.
\end{aligned}$$

Here, the third line uses Markov's inequality, the fourth line uses Lemma 3.23, and the last line holds because $m = \omega(\log n)$. □

3.3.3 Pseudorandom states and entropy lower bounds for cuts with sub-logarithmic sizes

Note that the current high entanglement construction may not always satisfy volume law entanglement for partitions where one side is extremely small (formally speaking, of size $O(\log n)$). Although this limitation does not impede the applications presented in this paper, we briefly discuss adjustments needed in our construction guaranteeing that volume law entanglement even holds for these small cuts.

Intuitively, when the size of the subsystem is at most $O(\log n)$, adversaries can approximate entanglement entropy up to an inverse polynomial error. On the other hand, a logarithmically-sized subsystem of Haar random states concentrates very strongly around the maximally mixed state. Therefore, any pseudorandom state must have volume law entanglement for cut X of size $|X| = O(\log n)$.

While the construction we have described so far is not pseudorandom,[7] a simple modification can achieve this: according to [ABF+23, Appendix A], it suffices to modify k_i^{rep} and k^{fin} such that they are pseudorandom functions (PRFs). The construction utilizes two types of functions: k-wise independent functions and LWE functions, with the latter being PRFs based on the standard LWE assumption. Consequently, the transformation involves converting k-wise independent families into families that are both k-wise independent and pseudorandom (for a specific construction, refer to [ABF+23, Appendix A]). Notably, since both our low-entanglement and high-entanglement constructions employ the same k-wise independent families, these modifications do not jeopardize the public-key indistinguishability of two constructions.

[7] By "pseudorandom" we mean that the state families *without* the public key are indistinguishable from Haar random states. Naturally, if the circuit to prepare the state is made public, it is easy to distinguish the state from Haar random states since generic Haar random states have no short state preparation circuit.

3.4 Area-law public-key pseudoentangled states on a 2D grid

We can easily generalise the 1D construction from Section 3.3 to a system of qubits arranged on a 2D grid. This is the same construction as in [ABF+23, Appendix D.5], so we only provide a short sketch. Let $|\psi_k\rangle$ be an n-qubit state from a pseudoentangled state ensemble. We can arrange the qubits of this state on an $\sqrt{n} \times \sqrt{n}$ grid as shown in Figure 1. Now consider a contiguous 2D subregion R of this $\sqrt{n} \times \sqrt{n}$ grid. Let

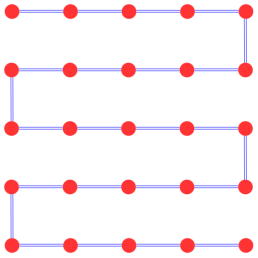


Figure 1: Arranging an n-qubit state on a $\sqrt{n} \times \sqrt{n}$ grid.

$|R|$ be the size of R (i.e. the number of qubits in R) and $|\partial R|$ the size of the boundary of R. Unfolding the "snake", this region R corresponds to a (not necessarily geometrically local) cut in 1D.

For the pseudoentangled state ensembles we constructed in Theorem 3.18, a high-entanglement state $|\psi_k\rangle$ has entanglement entropy $\Omega(|R|)$ for any (sufficiently large) cut R, even if the cut is not 1D geometrically local (Proposition 3.24). This means that arranged on a 2D grid, the high-entanglement states from Theorem 3.18 exhibit volume law entanglement scaling.

Conversely, consider a low-entanglement state $|\psi_k\rangle$ from the construction in Theorem 3.18. From the geometry of Figure 1 it is easy to see that a region R corresponds to a 1D cut that divides the qubits into at most $O(|\partial R|)$ contiguous regions; this is because the boundary of the region R can cut the "snake" at most $O(|\partial R|)$ times. For each of these $O(|\partial R|)$ cuts in 1D, we know from Theorem 3.18 that $|\psi_k\rangle$ has entanglement entropy at most $O(\operatorname{poly}\log n)$ across that cut. Using subadditivity of entanglement entropy, it then follows that the entanglement entropy of the region R is at most $O(|\partial R| \cdot \operatorname{poly}\log n)$, which corresponds to area-law scaling in two dimensions (up to polylogarithmic factors).

4 Computational hardness of learning ground state entanglement structure

Our public-key pseudoentanglement constructions can be leveraged to construct Hamiltonians such that it is hard to learn the entanglement structure of their ground state. This is what we will discuss in the next sections. Specifically, we will study variants of the following problem, which we define somewhat informally.

Definition 4.1 (Learning Ground State Entanglement Structure (LGSES) problem)**.** Given a classical description of a k-local Hamiltonian H on n qubits with spectral gap at least $\frac{1}{\operatorname{poly}(n)}$, decide whether the ground state of H has entanglement structure A or B? Here, A and B should be two qualitatively different, prespecified entanglement structures, e.g. near are-law and volume law entanglement.

We will see three different variants of this problem for three different types of local Hamiltonians and correspondingly three slightly different entanglement structures. We will progressively make our constructions more local—in some sense, more local corresponds to more physical Hamiltonians—but we will pay a slight price in terms of how straightforwardly the entanglement structures can be described.

(i) In Section 4.1, we will study the hardness of LGSES for $O(\log n)$-local Hamiltonians on n qubits arranged in a 1D line. The two entanglement structures to distinguish between will be $\operatorname{poly}\log n$ vs $\Omega(n)$ entanglement across geometrically local cuts in 1D. In other words, we are asked to distinguish 1D near area-law vs volume-law entanglement.

(ii) In Section 4.2, we will improve upon the locality of the Hamiltonian and study the hardness of LGSES for $O(1)$-local Hamiltonians on n qubits arranged in a 1D line. However, the entanglement structure will be slightly more complicated: we will consider the reduced states of ground states on a specific subsystem and ask whether this has 1D near area-law or volume-law entanglement structure for a mixed state measure of entanglement.

(iii) In Section 4.3, we will study the hardness of LGSES for 2-local Hamiltonians on a 2D grid of size $n \times \operatorname{poly}(n)$ and with constant local dimension, where all Hamiltonian terms are *geometrically local* (i.e. only nearest neighbors on the grid can interact). The two entanglement structures to distinguish will be entanglement entropy $O(\operatorname{poly}\log n)$ vs $\Omega(n)$ across horizontal cuts through the grid.

4.1 1D Hamiltonians with $\log n$-locality and pure states

In this section, we will show how to obtain two families of $\log n$-local Hamiltonians, one whose ground state has $\operatorname{poly}\log n$ entanglement scaling and the other whose ground state has $\Omega(n)$ entanglement scaling across geometrically local cuts in 1D, such that given the description of one of these Hamiltonians it is computationally hard to decide which family it belongs to.

We will start with the public-key pseudoentangled state constructions in Section 3.3, use the padded circuit-to-Hamiltonain construction of Section 2.6, and then use the trace distance closeness property of Lemma 2.26 to show that the entanglement structures of the ground states of these Hamiltonians resemble the entanglement structure of the public-key pseudoentangled states.

Theorem 4.2. *For every $n \in \mathbb{N}$, there exist two families $\mathcal{H}_n^{\text{low}}$ and $\mathcal{H}_n^{\text{high}}$ of $O(\log n)$-local Hamiltonians on $(n + O(\log n))$ qubits arranged on a 1D line with spectral gap $\Omega(1/\operatorname{poly}(n))$ and efficient procedures that sample (classical descriptions of) Hamiltonians from either family (denoted $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$) with the following properties:*

(i) *Hamiltonians sampled according to $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$ are computationally indistinguishable under Assumption 2.19.*

(ii) *With overwhelming probability, the ground states of Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have 1D near area-law entanglement and Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have 1D volume-law entanglement. Formally, this means that for geometrically local cuts in 1D of size $r = \omega(\log n)$, the ground states of the Hamiltonians have entanglement entropy $O(\operatorname{poly}\log n)$ or $\Omega(\min(r, n-r))$, respectively.*

Proof. Let $\Psi_n^{\text{low}} = \{|\psi_k\rangle\}_{k \in \mathcal{K}_n^{\text{low}}}$ and $\Psi_n^{\text{high}} = \{|\psi_k\rangle\}_{k \in \mathcal{K}_n^{\text{high}}}$ be two ensembles of public key pseudoentangled states across geometrically local cuts from Section 3.3. For a key $k \in \mathcal{K}_n^{\text{low}} \cup \mathcal{K}_n^{\text{high}}$, we denote by H_k the $O(\log n)$-local K-padded history state Hamiltonian from Lemma 2.25 with a binary clock, for $K = \operatorname{poly}(n)$ to be chosen later. We then choose $\mathcal{H}_n^{\text{low}} = \{H_k\}_{k \in \mathcal{K}_n^{\text{low}}}$ and $\mathcal{H}_n^{\text{high}} = \{H_k\}_{k \in \mathcal{K}_n^{\text{high}}}$. It follows from our pseudoentanglement construction and the padded history state Hamiltonian that these are efficiently sampleable families of $O(\log n)$-local Hamiltonians, noting that each term has a classical description (as a list of matrix entries) of size $\operatorname{poly}(n)$ and there are $\operatorname{poly}(n)$ terms, so the full Hamiltonians has an explicit classical

description of size $\text{poly}(n)$, too. The statement about the spectral gap follows from Lemma 2.25. Item (i) follows directly from the indistinguishability of $\mathcal{K}_n^{\text{low}}$ and $\mathcal{K}_n^{\text{high}}$ (Item (iv) in Definition 3.9).

To prove Item (ii), first consider a Hamiltonian $H \leftarrow \mathcal{H}_n^{\text{low}}$. Let $|\psi_{\text{ground}}\rangle$ be its ground state and define

$$|\psi_f\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\text{clock}(t)\rangle\,,$$

where $|\psi\rangle$ is the pseudoentangled state for which H is the history state Hamiltonian and T is the number of gates in the (padded) circuit (see Section 2.6). Note that from Lemma 2.26,

$$\left\| |\psi_f\rangle\langle\psi_f| - |\psi_{\text{ground}}\rangle\langle\psi_{\text{ground}}| \right\|_1 = O\left(\frac{1}{\text{poly}(n)}\right), \tag{4.1}$$

for a sufficiently large choice of padding $K = \text{poly}(n)$.

Let (A,B) be a geometrically local bipartition of the $n + O(\log n)$ with $|A|, |B| = \omega(\log n)$. Since we are considering geometrically local cuts with $|B| = \omega(\log n)$ and there are only $O(\log n)$ qubits, for a suitable choice of implicit constants in $|B| = \omega(\log n)$ all of the clock qubits are contained in B and therefore do not contribute to the entanglement across the cut. Hence,

$$S((\psi_f)_A) = O(\text{poly}\log n)\,.$$

Using the continuity property of the von Neumann entropy (Lemma 2.7) and Equation (4.1), if we choose the padding $K = \text{poly}(n)$ sufficiently large we get that

$$S((\psi_{\text{ground}})_A) \leq S((\psi_f)_A) + O\left(\frac{1}{\text{poly}(n)}\right) = O\left(\text{poly}\log n\right)$$

as desired.

By applying a similar argument, when we consider $H \leftarrow \mathcal{H}_n^{\text{high}}$ and a bipartition $(r, n-r)$,

$$S((\psi_{\text{ground}})_A) = \Omega(\min(r, n-r)).$$

This completes the proof. □

Remark 4.3. Under the standard LWE assumption (Assumption 2.18) instead of Assumption 2.19, Theorem 4.2 still holds, but with the smaller entanglement gap $O(n^\delta)$ vs $\Omega(n)$ for any $\delta > 0$. This mirrors directly the statement in Theorem 3.18.

4.2 1D Hamiltonians with constant locality and mixed states

In this section, we will modify the construction in Section 4.1 with a unary clock to get constant locality. However, because the clock register will now have $\text{poly}(n)$ qubits, we can no longer simply remove the clock qubits as we did in Theorem 4.2. Therefore, we will consider the entanglement structure of the reduced density matrices of the ground state with the clock register traced out. Using mixed state entanglement measures (Section 2.4.3), we will show that one such density matrix will have high entanglement, and the other will have low entanglement.

As discussed in Section 2.4, there are many mixed state measures of entanglement. We will show that for any "natural" mixed state entanglement measure (in the sense of Lemma 2.13), the ground state of the our Hamiltonian (with the clock register traced out) has either high or low entanglement. We achieve this by

giving an upper bound on the entanglement of formation of our low entanglement construction and a lower bound on the distillable entanglement of our high entanglement construction. Combined with Lemma 2.13, this gives an entanglement gap for any natural entanglement measure. In fact, Hamiltonians constructed from our ensembles of pseudoentangled states achieve a maximally large gap.

Theorem 4.4. *For every $n \in \mathbb{N}$, there exist two families $\mathcal{H}_n^{\text{low}}$ and $\mathcal{H}_n^{\text{high}}$ of $O(1)$-local Hamiltonians on $(n+poly(n))$ qubits arranged on a 1D line with spectral gap $\Omega(1/\text{poly}(n))$ and efficient procedures that sample (classical descriptions of) Hamiltonians from either family (denoted $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$) with the following properties:*

(i) *Hamiltonians sampled according to $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$ are computationally indistinguishable under Assumption 2.19.*

(ii) *If we trace out $poly(n)$ many qubits from the ground state of each Hamiltonian, the entanglement gap between the resultant quantum states in the high and low families is $\Omega(min(r,n-r))$ versus $\mathcal{O}(poly\log n)$, for a cut of size $(r,n-r)$, for any natural entanglement measure. With overwhelming probability, the reduced states on the first n qubits of the ground states of Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have 1D near area-law entanglement and Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have 1D volume-law entanglement with respect to any natural mixed state entanglement measure (in the sense of Lemma 2.13).*

Proof. We consider the same construction of $\mathcal{H}_n^{\text{low}}$ and $\mathcal{H}_n^{\text{high}}$ as in Theorem 4.2, except that we now use the unary clock construction from Lemma 2.25 instead of the binary one as in Theorem 4.2. With this, we only need to show Item (ii) as the other properties follow in exactly the same way as in the proof of Theorem 4.2.

First consider a Hamiltonian $H \leftarrow \mathcal{H}_n^{\text{low}}$. Let $|\psi_{\text{ground}}\rangle$ and $|\psi_f\rangle$ be as in Theorem 4.2, except with a unary clock. Let ρ_{data} be the density matrix on n qubits left when we trace out the clock qubits from $|\psi_{\text{ground}}\rangle$ and recall that the reduced state of $|\psi_f\rangle$ on the first n qubits is the pseudoentangled state $|\psi\rangle\langle\psi|$ (using the notation from Theorem 4.2). Then, using Lemma 2.26 and the fact that tracing out qubits cannot increase the trace distance between two states,

$$|| \rho_{\text{data}} - |\psi\rangle\langle\psi| ||_1 = O\left(\frac{1}{\text{poly}(n)}\right) \tag{4.2}$$

for a sufficiently large padding $K = \text{poly}(n)$. Then, using continuity properties of the conditional von Neumann entropy (Equation (4.2), Lemma 2.7), standard properties of the binary entropy function, the fact that all natural mixed state entanglement measures collapse to the von Neumann entanglement entropy for pure states (Lemma 2.14), and the fact that coherent information is just the negative of conditional von Neumann entropy (Definition 2.12) and lower bounds distilalble entanglement (Lemma 2.13),

$$E_D(\rho_{\text{data, }AB}) \geq I(\rho_{\text{data, }AB}) = \Omega\left(n - \frac{1}{\text{poly}(n)}\right).$$

By applying a similar argument, when we consider $H \leftarrow \mathcal{H}_n^{\text{high}}$ and a bipartition $(r,n-r)$, using continuity properties of the entanglement of formation (Lemma 2.15) we get that

$$E_F(\rho_{\text{data, }AB}) = O\left(\text{poly}\log n + \frac{1}{\text{poly}(n)}\right).$$

Then, with the observation that any natural entanglement measure is upper bounded by E_F and lower bounded by E_D (Lemma 2.13), the result follows. □

Remark 4.5. Just as in Remark 4.3, under the standard LWE assumption (Assumption 2.18) Theorem 4.4 still holds, but with the smaller entanglement gap $O(n^\delta)$ vs $\Omega(n)$ for any $\delta > 0$.

4.3 2D Hamiltonians with geometric locality and pure states

In this section, we will show how to obtain two families of 2D Hamiltonians on a 2D grid of $\text{poly}(n)$ qudits, one whose ground state has entanglement entropy of order n and the other whose ground state has entanglement entropy of order $\text{poly}\log n$, with respect to most horizontal cuts across the 2D grid. Thus, arguably, this gives us a relatively more complicated entanglement structure than the constructions in Theorem 4.2 and Theorem 4.4. However, we gain in geometric locality: the Hamiltonian only has nearest neighbor interactions on a 2D grid. Formally, 2D Hamiltonians are defined as follows.

Definition 4.6 (2D (local) Hamiltonian, [AGIK09])**.** Let H be a Hermitian operator (interpreted as a Hamiltonian, giving the energy of some system). We say that H is an r-state Hamiltonian if it acts on r-state qudits (i.e. $d = r$). When $r = 2$, namely, when the qudits are qubits. We say that H is k-local if it can be written as

$$H = \sum_i H_i,$$

where each H_i acts non-trivially on at most k qudits. Note that this term does not assume anything about the physical location of the qudits. We say that H is a 2D Hamiltonian if the qudits are arranged on a 2D grid and the terms H_i interact only pairs of nearest neighbor qudits. In particular, a 2D Hamiltonian is 2-local.

Overview. The main steps of our construction are as follows:

- First, we start with two n-qubit public key pseudoentangled states across multiple cuts, according to the construction in Section 3.3, and consider the circuits for preparing them. Suppose these circuits have $K = \text{poly}(n)$ gates. Without loss of generality, we assume the circuit can be decomposed into $R = \text{poly}(n)$ "rounds", each made up of exactly n nearest-neighbor interactions on qubits 1, (1,2), (2,3), etc. Any circuit can be transformed into this form by inserting a polynomial number of identity and swap gates. Hence, the circuit contains nR gates in total. As in Section 4.1, we pad the circuits with nM identity gates at the end for a sufficiently large $M = \text{poly}(n)$.

- Then, we use a modified version of the 2D clock construction [AVDK+08] to construct two families of 2D Hamiltonians such that the padded circuit is embedded into its ground state. That is, if $\mathsf{C} = U_{nT} \cdot U_{nT-1} \cdots U_1$ is the circuit with padding, where $T = M + R$ is the total number of rounds after padding, we construct a Hamiltonian H such that the ground state $|\psi_{\text{ground}}\rangle$, on an $n \times T$ grid of qudits, encodes the time evolution of the padded circuit.

- We show how, because of the padding, the entanglement structure of the 2D ground state across any horizontal cut resembles the entanglement structure of the state

$$|\psi_{\text{output}}\rangle = U_{nR} \cdot U_{nR-1} \cdots U_1 |0^n\rangle, \tag{4.3}$$

  across the same cut.

- By virtue of our pseudoentanglement construction, the state in Equation (4.3) either has high or low entanglement, whenever the cut has distance $\omega(\log n)$ to the boundary of the grid. Then, by a continuity argument, we show that the ground state $|\psi_{\text{ground}}\rangle$ also inherits the high or low entanglement property.

4.3.1 Geometrically local 2D history state Hamiltonians

Based on the framework of [AVDK+08], we begin by showing how to construct a 2D Hamiltonian whose ground state encodes the state obtained by taking our padded circuit, as defined in Equation (4.3). Without loss of generality, we assume that before padding, the circuit has initial state $|0\rangle$ and consists of R rounds, where in each rounds there are n nearest-neighbor gates, acting on qubits 1, $(1,2)$, $(2,3)$, $(3,4)$ and so on.

Legal shapes of the clock. To start, we will introduce some notation to reason about the valid clock states. Suppose we have in total $n(T+1)$ 9-state qudits arranged on a two-dimensional square lattice with n rows and $T+1$ columns. We refer to the quantum state defined on this lattice as a *clock state*. From the top to the bottom, we number the rows from 1 to n. From left to right, we number the columns from 0 to T. Intuitively, the vertical axis of the 2D grid aligns with the spatial dimension of the original circuit, while the horizontal axis of the 2D grid aligns with the temporal dimension of the original circuit. Additionally, we have the following features.

- **Possible states**: For each qudit, following the notation of [AVDK+08], we denote its 9 possible states to be

  $$|\bigcirc\rangle, |\uparrow\rangle, |\downarrow\rangle, |\Uparrow\rangle, |\Downarrow\rangle, |\otimes\rangle, |\overline{\uparrow}\rangle, |\overline{\downarrow}\rangle, |\text{M}\rangle.$$

  The former 6 states were introduced in [AVDK+08] whereas the latter three states are newly introduced in this work.

- **Phases**: These states can be categorized into six distinct *phases*: the *unborn phase* represented by $|\bigcirc\rangle$, the *first phase* containing $|\uparrow\rangle, |\downarrow\rangle$, the *second phase* containing $|\Uparrow\rangle, |\Downarrow\rangle$, the *dead phase* represented by $|\otimes\rangle$, the *flag phase* containing $|\overline{\uparrow}\rangle$, $|\overline{\downarrow}\rangle$, and the *marker phase* represented by $|\text{M}\rangle$.

- **Encoding the value**: The orientation of the state in the first phase, the second phase, and the flag phase encodes the value, i.e., $|0\rangle$ and $|1\rangle$ states of a qubit in the circuit. For example, we can map $|0\rangle$ to $|\uparrow\rangle$ ($|\Uparrow\rangle$, $|\overline{\uparrow}\rangle$) and $|1\rangle$ to $|\downarrow\rangle$ ($|\Downarrow\rangle$, $|\overline{\downarrow}\rangle$).

- **Symbols for spanned subspaces**: Denote $|\updownarrow\rangle$ as any state in the subspace spanned by $|\uparrow\rangle$ and $|\downarrow\rangle$. Similarly, denote $|\Updownarrow\rangle$ as any state in the space spanned by $|\Uparrow\rangle$ and $|\Downarrow\rangle$, and denote $|\overline{\updownarrow}\rangle$ as any state in the space spanned by $|\overline{\uparrow}\rangle$ and $|\overline{\downarrow}\rangle$.

- **Shapes**: Based on the concept of phases, we can further define the *shape* of the quantum state on this two-dimensional square lattice. A shape is defined as an allocation of one of five phases to each qudit, ignoring the orientations of the states in the first, second, or the flag phase. Intuitively, the flag phase serves as a marker for the location where the current change occurs, and plays a similar role as the flag in [AGIK09] concerning the ground state in the one-dimensional setting.

Similar to [AVDK+08], we show that we can represent the time evolution of the padded circuit using a series of $(3n-1)T+1$ clock states that are *legal shapes*, where each shape corresponds to one time step in the circuit.

Remark 4.7. Formally defined in Definition 4.8, the notion of legal shapes we consider is slightly different from the original ones in [AVDK+08] because we have the extra flag and marker states.

Definition 4.8 (Legal shapes, [AVDK+08])**.** Denote $L = (3n-1)T$. For any $t \in [0,L]$, we say a clock state is in the t-th legal shape if one of the following conditions is satisfied

(i) There exists r and $k \in [0,n]$ such that $t = (3n-1)r + k$. Moreover, the r leftmost columns of the state are in the dead phase, the top $k-1$ qudits in the $(r+1)$-th column are in their second phase, the bottom $n-k$ are in the first phase, the qudit in between is in the flag phase, and qudits in the remaining $R-r$ columns are all in the unborn phase

(ii) There exists r and $k \in [0,2n-1]$ such that $t = (3n-1)r+n+k$. Moreover, the r leftmost columns of the state are in the dead phase, the $(r+1)$-th column has its $n-k$ topmost qudits in the second phase while its remaining k qudits in the dead phase, the $(r+2)$-th column has its $n-k$ topmost qudits in the unborn phase, the bottom $k-1$ qudits in the first phase, the qudit in between is in the flag phase, and all qudits in the remaining columns are in the unborn phase.

(iii) There exists r and $k \in [0,2n-1]$ such that $t = (3n-1)r+n+k$. Moreover, the r leftmost columns of the state are in the dead phase, the $(r+1)$-th column has its $n-k$ topmost qudits in the second phase while its remaining k qudits in the dead phase, the $(r+2)$-th column has its $n-k-1$ topmost qudits in the unborn phase, the bottom k qudits in the first phase, the qudit in between is in the marker phase, and all qudits in the remaining columns are in the unborn phase.

Denote $\mathcal{S}$ to be the $(L+1)2^n$-dimensional space spanned by all states in legal shapes. Moreover, for each $0 \le t \le L$ and $0 \le j \le 2^n - 1$, define $|\gamma_t^j\rangle$ to be the state in the t-th legal shape, where the orientations of its n active qudits (i.e., qudits in the first phase, second phase, or the flag phase) correspond to the state of the circuit after applying the first t gates to an initial state that encodes the binary representation of j, or quantitatively,

$$U_t \cdot U_{t-1} \cdots U_1 |j\rangle. \tag{4.4}$$

Moreover, we denote $|\gamma(t)\rangle \equiv |\gamma_t^0\rangle$ for brevity.

The following is immediate from the construction.

Lemma 4.9. *For any $0 \le j \le 2^n - 1$ and any $t_1 \ne t_2 \in [0,L]$, $|\gamma_{t_1}^j\rangle$ and $|\gamma_{t_2}^j\rangle$ are orthogonal to each other.*

Transition rules. Based on the definition of $|\gamma_t^j\rangle$, we can further divide $\mathcal{S}$ into 2^n subspaces $\mathcal{S}_1, \ldots, \mathcal{S}_{2^n}$, where each subspace $\mathcal{S}_j$ is spanned by $\{|\gamma_0^j\rangle, \ldots, |\gamma_L^j\rangle\}$. As shown in [AVDK+08], intuitively, the transition rules between the states $|\gamma_0^j\rangle, \ldots, |\gamma_L^j\rangle$ can also be understood as follows.

- **Downward stage**: Consider a state $|\gamma_t^j\rangle$ for some $t = (3n-1)r$. In this stage, the n qudits located in the r-th column are in their initial phase, and the orientations of these active qudits (i.e., those in the first phase, second phase, and the flag phase) encode the initial state of the circuit at the beginning of the r-th round. To the left of this column, the qudits are in the dead phase, while to the right, they are in the unborn phase. The state $|\gamma_{t+1}^j\rangle$ can be obtained from $|\gamma_t^j\rangle$ by converting the uppermost qudit in the r-th column into active-phase and then applying the first gate of the r-th round (a one-qubit gate) to the state encoded in these active qudits. Subsequently, the state $|\gamma_{t+2}^j\rangle$ is derived from $|\gamma_{t+1}^j\rangle$ by converting the second qudit from the top in the r-th column into active phase, converting the frist qudit from the top in the r-th column into first phase, and applying the second gate of the r-th round (a two-qubit gate) to both this qudit and the one above it. This process continues in a similar manner until we reach the state $|\gamma_{t+n}^j\rangle$, where the entire r-th column consists of qudits in the second phase except the one at the bottom. These sequential steps are referred to as the downward stage.

- **Upward stage**: Correspondingly, there is an upward stage. In this stage, the state $|\gamma^j_{t+n+1}\rangle$ is transformed from $|\gamma^j_{t+n}\rangle$ by shifting the bottommost qudit in the r-th column one position to the right. To be more precise, the bottommost qudit shifts into the dead phase, while the qudit to the right of it shifts into the active phase. Then, $|\gamma^j_{t+n+2}\rangle$ is transformed from $|\gamma^j_{t+n+1}\rangle$ by shifting the bottommost qudit into the first phase without changing its encoding and shifting the qudit above it into the marker phase. It is worth noticing that the encoded state is not changed during this process, which corresponds to the identity gate applied in the circuit. Continuing this iterative process to go up the column, we can "copy" the encoding of the r-th column into the $(r+1)$-th column. We observe that the upward stage ends in the state $|\gamma^j_{t+n+n}\rangle = |\gamma^j_{2(r+1)n}\rangle$ which aligns with the previously described initial state of a new round.

An example of legal shapes with $n = 6$ and $T = 2$ is given in Figure 2, where the shapes correspond to $t = 0, 1, \ldots, 19$. It is worth noting that each shape has exactly n qudits in the first, second, or the flag phase. Consequently, each shape contains a subspace with a dimension of 2^n spanned by the possible states of qudits within the first or second phase.

Constructing the corresponding Hamiltonian. Based on the construction in [AVDK+08], in the remaining part of this section, we present a two dimensional Hamiltonian on the grids whose ground state is the history state of the evolution

$$|\psi_{\text{ground}}\rangle = \frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} |\gamma^0_t\rangle. \tag{4.5}$$

Following [AVDK+08], our 2D Hamiltonian H_{2D} contains three parts:

$$H_{2D} \equiv \frac{1}{2} \sum_{\ell=1}^{L} H_\ell + H_{\text{input}} + J \cdot H_{\text{clock}}, \tag{4.6}$$

where $J = \epsilon^{-2} \cdot L^6$ with $\epsilon = \frac{1}{\text{poly}\, n}$. Conceptually, each Hamiltonian term Equation (4.6) imparts an "energy penalty" upon any state that fails to meet the required properties of the ground state. In particular, H_{clock} guarantees that the ground state is a superposition over a set of clock states in legal shapes. Then, H_{input} verifies that the component in the first legal shapes encodes the input of the circuit, i.e., $|0\rangle$, in its first column of qudits. Finally, the propogation H_ℓ ensures the correctness of transitions between consecutive legal shapes, meaning that the encoded quantum state evolves in accordance with the corresponding gate applied in the circuit during that time step. Formally, as in [AVDK+08], we let

$$H_{\text{input}} \coloneqq \sum_{i=1}^{n} (|\circledcirc\rangle\langle\circledcirc|)_{i,1},$$

where the indices indicate that the corresponding term acts on the i-th row and the first column of the 2D grid. As for H_{clock}, similar to the case in [AVDK+08], it is worth noting that the legal shapes defined in Definition 4.8 can be verified in a 2-*local way*, which allows us to define a 2-local Hamiltonian such that its ground space contains only superpositions of clock states in legal shapes.

Similarly to [AVDK+08, Claim 4.2], we prove the following result.

Lemma 4.10. *A clock state is in legal shape defined in Definition 4.8 if and only if it contains none of the forbidden configurations in Table 1.*

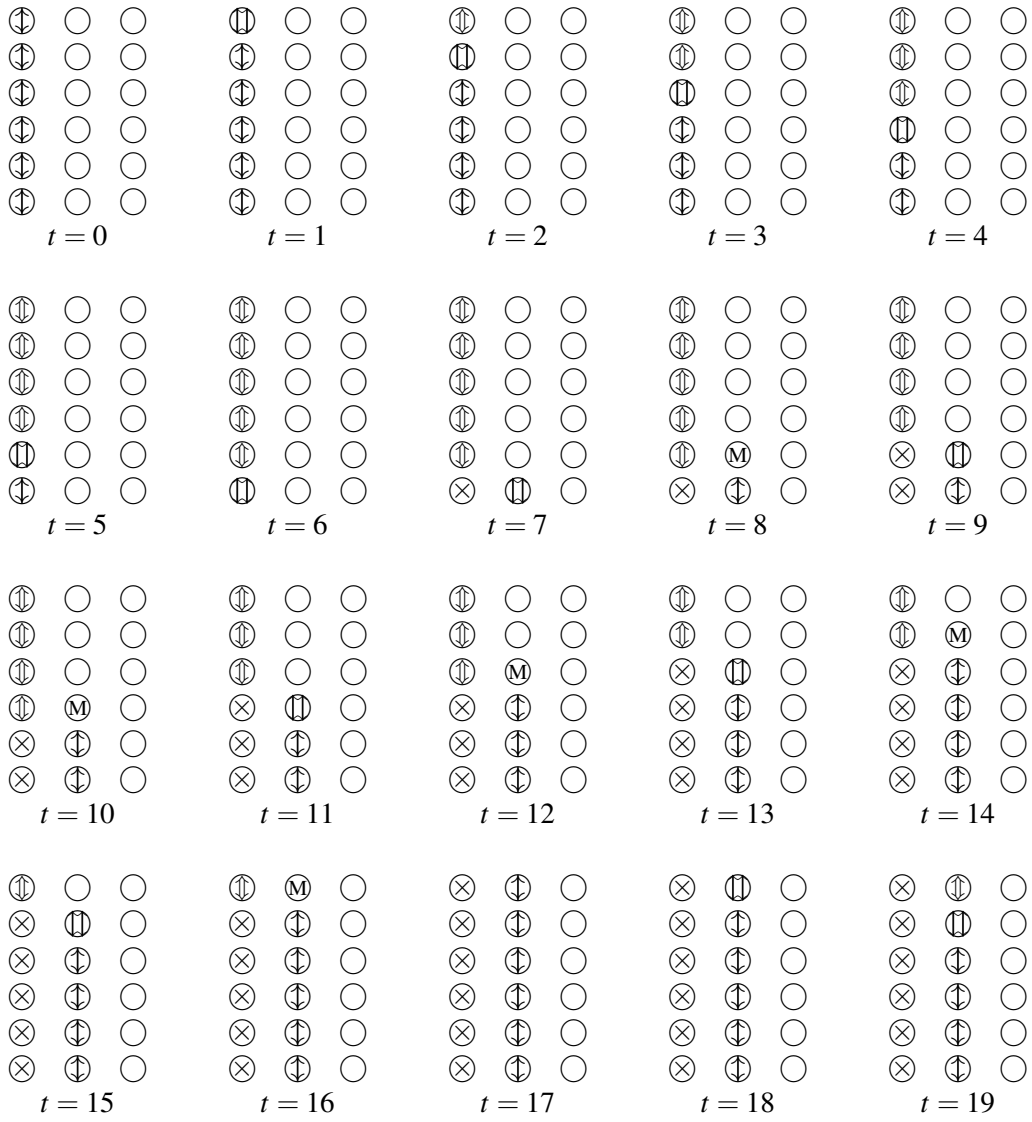


Figure 2: An example of clock states in legal shapes with $n = 6$, $T = 2$.

Proof. The proof is similar to the proof of [AVDK+08, Claim 4.2]. First, we can check that any clock state in legal shape contains none of the forbidden configurations. Conversely, for any clock state that contains none of these configurations, each of its rows admits to the pattern $\otimes^*[\updownarrow, \Updownarrow, \boxplus, \Updownarrow\text{M}]\bigcirc^*$. In other words, it starts with a sequence of zero or more $\otimes$ from the left, then incorporates either $\updownarrow$, $\Updownarrow$, $\boxplus$, or $\Updownarrow$M, and ends with a sequence of zero or more $\bigcirc$ on the right. As for the vertical direction, the columns are in one of three distinct formats when read from top to bottom: $\Updownarrow^*[\boxplus]\updownarrow^*$, $\Updownarrow^*\otimes^*$, $\bigcirc^*[\boxplus]\updownarrow^*$, or $\bigcirc^*[\text{M}]\updownarrow^*$, and such a shape must satisfy Definition 4.8. □

Based on Lemma 4.10, we can define a two-local nearest-neighbor Hamiltonian that checks whether a clock state is in legal shape or not. For example, prohibits a qudit at location (i, j) in state $\bigcirc$ to be positioned

Forbidden	Guarantees that
$\bigcirc\updownarrow, \bigcirc\Updownarrow, \bigcirc\otimes, \bigcirc\boxplus, \bigcirc\text{M}$	$\bigcirc$ is to the right of all other qubits
$\bigcirc\otimes, \updownarrow\otimes, \Updownarrow\otimes, \boxplus\otimes, \text{M}\otimes$	$\otimes$ is to the left of all other qubits
$\bigcirc\otimes, \otimes\bigcirc$	$\bigcirc$ and $\otimes$ are not horizontally adjacent
$\updownarrow\updownarrow, \updownarrow\Updownarrow, \updownarrow\boxplus$ $\Updownarrow\updownarrow, \Updownarrow\Updownarrow, \Updownarrow\boxplus$ $\boxplus\updownarrow, \boxplus\Updownarrow, \boxplus\boxplus$	only one of $\updownarrow$, $\Updownarrow$, or $\boxplus$ per row
$\bigcirc$, $\updownarrow$, $\otimes$, $\boxplus$ $\Updownarrow$, $\Updownarrow$, $\Updownarrow$, $\Updownarrow$	only $\Updownarrow$ above $\Updownarrow$
$\updownarrow$, $\updownarrow$, $\updownarrow$, $\updownarrow$ $\bigcirc$, $\Updownarrow$, $\otimes$, $\boxplus$	only $\updownarrow$ below $\updownarrow$
$\bigcirc$, $\otimes$ $\otimes$, $\bigcirc$	$\bigcirc$ and $\otimes$ are not vertically adjacent
$\Updownarrow$, $\boxplus$, $\otimes$, $\otimes$ $\bigcirc$, $\bigcirc$, $\updownarrow$, $\boxplus$	no $\bigcirc$ below $\Updownarrow$ and $\boxplus$; no $\updownarrow$ and $\boxplus$ below $\otimes$
$\bigcirc$ $\updownarrow$	no $\bigcirc$ above $\updownarrow$
$\updownarrow$, $\Updownarrow$, $\otimes$, $\boxplus$ M , M , M , M	only $\bigcirc$ above M
M , M , M , M $\bigcirc$, $\Updownarrow$, $\otimes$, $\boxplus$	only $\updownarrow$ below M
$\updownarrow\text{M}, \otimes\text{M}, \boxplus\text{M}, \text{M}\text{M}$	only $\Updownarrow$ to the left of M
$\text{M}\updownarrow, \text{M}\Updownarrow, \text{M}\boxplus$	only $\bigcirc$ to the right of M

Table 1: Local rules for basis state to be in legal shape.

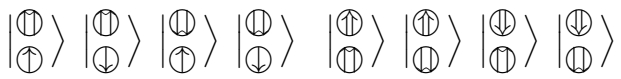
to the left of a qudit at location $(i, j+1)$ in state $\otimes$. Then, the corresponding Hamiltonian term would be $(|\bigcirc,\otimes\rangle\langle\bigcirc,\otimes|)_{(i,j),(i,j+1)}$. Summing over all the forbidden configurations of Table 1 and over all relevant pairs of particles, we have

$$H_{\text{clock}} \equiv \sum_{r\in\text{rules}} H_r. \tag{4.7}$$

Next, we turn to the propagation term H_ℓ that guarantees the correctness of transitions between clock states in consecutive legal shapes. Observe that according to Definition 4.8, consecutive legal shapes only differ in at most two adjacent locations, which makes it possible to be verified using two-local nearest-neighbour Hamiltonians. In particular, the structure of H_ℓ takes on different forms depending on whether ℓ is in the downward phase (i.e., is of the form $(3n-1)r+k$ for $1\le k\le n$) or the upward phase (i.e., is of the form $(3n-1)r+n+k$ for $1\le k<2n-1$). For the downward stage, H_ℓ checks that a gate is applied correctly. For $\ell=(3n-1)r+k$ and $2<k\le n$, as the same in [AVDK+08], we define

$$\begin{aligned} H_\ell \equiv \begin{pmatrix} 0 & -U_\ell \\ -U_\ell^\dagger & 0 \end{pmatrix} &+ \left(|\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow|\right)_{\substack{\text{k-1,r}\\ \text{k,r}}} \\ &+ \left(|\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow| + |\Updownarrow\rangle\langle\Updownarrow|\right)_{\substack{\text{k,r}\\ \text{k+1,r}}}, \end{aligned} \tag{4.8}$$

where the stacked notation $\left|\begin{smallmatrix}\cdot\\ \cdot\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\cdot\\ \cdot\end{smallmatrix}\right|$ denotes a 2-local Hamiltonian term acting on nearest neighbors as indicated by the indices outside the parentheses. Moreover, the first term in Equation (4.8) represents a Hamiltonian that acts on the two particles in positions (k,r) and $(k+1,r)$ and is restricted to the subspace spanned by



For the special cases where $k=1$ or n, we set

$$H_{(3n-1)r+1} \equiv \begin{pmatrix} 0 & -U_{(3n-1)r+1} \\ -U^{\dagger}_{(3n-1)r+1} & 0 \end{pmatrix} + \left(|\text{⊤}\rangle\langle\text{⊤}| + |\text{⊥}\rangle\langle\text{⊥}|\right)_{1,r} + \left(\left|\begin{smallmatrix}\text{⊤}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊤}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊤}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊤}\\ \text{⊥}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊥}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊥}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊥}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊥}\\ \text{⊥}\end{smallmatrix}\right|\right)_{\substack{1,r\\2,r}},$$

and

$$H_{(3n-1)r+n} \equiv \begin{pmatrix} 0 & -U_{(3n-1)r+n} \\ -U^{\dagger}_{(3n-1)r+n} & 0 \end{pmatrix} + \left(\left|\begin{smallmatrix}\text{⊤}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊤}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊤}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊤}\\ \text{⊥}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊥}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊥}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⊥}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⊥}\\ \text{⊥}\end{smallmatrix}\right|\right)_{\substack{n-1,r\\n,r}} + \left(\left|\begin{smallmatrix}\text{⇑}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⇑}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⇑}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⇑}\\ \text{⊥}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⇓}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⇓}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{⇓}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{⇓}\\ \text{⊥}\end{smallmatrix}\right|\right)_{\substack{n-1,r\\n,r}}.$$

As for the upward stage, we have $\ell=(3n-1)r+n+k$ for some $1\le k<2n-1$. If $1<k<2n-1$ and is an odd number, in this step the qudit in the marker phase $|\text{Ⓜ}\rangle$ in the i-th row with $i=n-(k-1)/2$ will acquire the value of the qudit on the left of it. Then, the corresponding Hamiltonian term H_ℓ can be written as

$$H_\ell \equiv \left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right|_{\substack{i,r+1\\ i+1,r+1}} + \left|\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} - \left(|\text{⊤},\text{Ⓜ}\rangle\langle\otimes,\text{⊤}| + |\otimes,\text{⊤}\rangle\langle\text{⊤},\text{Ⓜ}|\right)_{(i,r)(i,r+1)}$$
$$+ \left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right|_{\substack{i,r+1\\ i+1,r+1}} + \left|\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} - \left(|\text{⊥},\text{Ⓜ}\rangle\langle\otimes,\text{⊥}| + |\otimes,\text{⊥}\rangle\langle\text{⊥},\text{Ⓜ}|\right)_{(i,r)(i,r+1)},$$

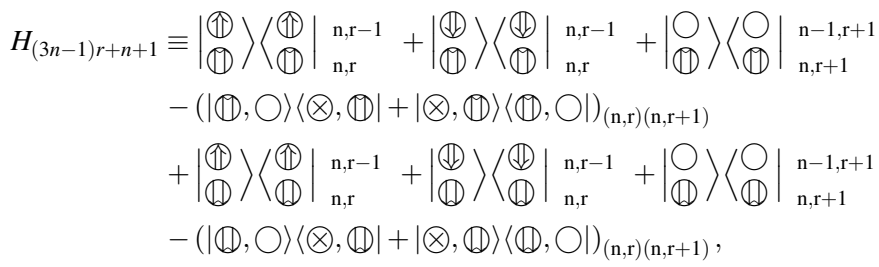
where the first line corresponds to changing the state $|\text{⊤},\text{Ⓜ}\rangle$ to $|\text{◯},\text{⊤}\rangle$, and the second line corresponds to changing the state $|\text{⊥},\text{Ⓜ}\rangle$ to $|\text{◯},\text{⊥}\rangle$.

If k is an even number, in this step the qudit in the flag phase $|\text{⊥}\rangle$ in the i-th row with $i=n+1-k/2$ will transform into the first phase ⇑, while the qudit above it will transform into the marker phase Ⓜ from the unborn phase $|\text{◯}\rangle$. Then, the corresponding Hamiltonian term H_ℓ can be written as

$$H_\ell \equiv \left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} + \left|\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} - \left(\left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{◯}\\ \text{⊤}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊤}\end{smallmatrix}\right|\right)_{\substack{i-1,r+1\\ i,r+1}}$$
$$+ \left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} + \left|\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right|_{\substack{i-1,r+1\\ i,r+1}} - \left(\left|\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right| + \left|\begin{smallmatrix}\text{◯}\\ \text{⊥}\end{smallmatrix}\right\rangle\left\langle\begin{smallmatrix}\text{Ⓜ}\\ \text{⊥}\end{smallmatrix}\right|\right)_{\substack{i-1,r+1\\ i,r+1}}.$$

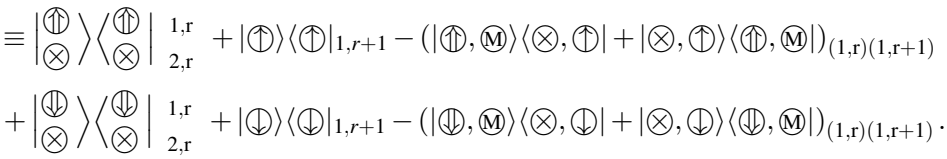
For the special case where $k = 1$ or $k = 2n-1$, we set

$$H_{(3n-1)r+n+1} \equiv$$



and

$$H_{(3n-1)(r+1)} \equiv$$



Based on the definition of H_{input}, H_{clock}, and H_{ℓ}, we present the following result, which is a variant of [AVDK+08, Lemma 4.7].

Lemma 4.11. *For any $\epsilon \geq 1/\operatorname{poly}(n)$, the Hamiltonian H_{2D} defined in Equation (4.6) on the $n \times (T+1)$ grid of qudits satisfies the following.*

- *The history state of the evolution $|\psi_{\text{ground}}\rangle$ is a ground state of H_{2D}. Moreover, any ground state of H_{2D} is ϵ-close to $|\psi_{\text{ground}}\rangle$.*
- *The spectral gap of H_{2D} is at least $\Omega((nT)^{-3}) = 1/\operatorname{poly} n$.*

The proof of Lemma 4.11 essentially follows the proof of [AVDK+08, Lemma 4.7].

4.3.2 Entanglement properties of the ground state

In this section, we analyze the entanglement properties of the state $|\psi_{\text{ground}}\rangle$ defined in Equation (4.5), which is the ground state of the 2D Hamiltonian H_{2D} defined in Equation (4.6). We begin by presenting some definitions and technical lemmas that are useful.

Definition 4.12 (Cutwise orthogonality)**.** For any $K > 0$, let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two K-qudit states, and consider any bipartite cut among these K qudits. We denote the density matrices obtained by tracing out the right parts of $|\psi_1\rangle$ and $|\psi_2\rangle$ as $\rho_1^{(A)}$ and $\rho_2^{(A)}$, respectively. Similarly, we define $\rho_1^{(B)}$ and $\rho_2^{(B)}$. We define $|\psi_1\rangle$ and $|\psi_2\rangle$ to be *cutwise orthogonal* with respect to this bipartite cut if the following condition holds:

$$\rho_1^{(A)}\rho_2^{(A)} = \rho_1^{(B)}\rho_2^{(B)} = 0.$$

The next lemma demonstrates the entanglement properties of a set of mutually cutwise orthogonal states.

Lemma 4.13. *For any $m, K > 0$, suppose there are m K-qudit states $|\psi_1\rangle, \ldots, |\psi_m\rangle$ and there is a bipartite cut among these K qudits into subsystems (A, B). Then for any $\alpha_1, \ldots, \alpha_m$ with $\sum_i \alpha_i^2 = 1$, the state*

$$|\Psi\rangle = \alpha_1|\psi_1\rangle + \cdots + \alpha_m|\psi_m\rangle$$

satisfies

$$S(\Psi_A) = \sum_{i=1}^{m} |\alpha_i|^2 S((\psi_i)_A) + \sum_{i=1}^{m} |\alpha_i|^2 \log \frac{1}{|\alpha_i|^2},$$

if $|\psi_i\rangle$ and $|\psi_j\rangle$ are cutwise orthogonal for any $i \neq j \in [m]$. Here, Ψ_A is the reduced state of $|\Psi\rangle$ on subsystem A, and likewise for the other states.

Proof. For any $i \in [m]$, we express the Schmidt decomposition of $|\psi_i\rangle$ as

$$|\psi_i\rangle = \sum_{k=1}^{K_i} \beta_{i,k} |\psi_{i,k}^{(A)}\rangle \otimes |\psi_{i,k}^{(B)}\rangle.$$

Consequently, for any $i \in [m]$ we have

$$(\psi_i)_A = \sum_{k=1}^{K_i} |\beta_{i,k}|^2 |\psi_{i,k}^{(A)}\rangle\langle\psi_{i,k}^{(A)}|, \qquad (\psi_i)_B = \sum_{k=1}^{K_i} |\beta_{i,k}|^2 |\psi_{i,k}^{(B)}\rangle\langle\psi_{i,k}^{(B)}|.$$

Given that $|\psi_i\rangle$ and $|\psi_j\rangle$ are cutwise orthogonal for any $i \neq j \in [m]$, we can then derive that

$$\left|\left\langle \psi_{i,k_i}^{(A)} | \psi_{j,k_j}^{(A)} \right\rangle\right| = \left|\left\langle \psi_{i,k_i}^{(B)} | \psi_{j,k_j}^{(B)} \right\rangle\right| = 0,$$

for any $k_i \in [K_i]$, $k_j \in [K_j]$, and any $i \neq j \in [m]$. Then, tracing out the right part of $|\Phi\rangle$, the resulting reduced state Ψ_A is given by

$$\Psi_A = \sum_{i=1}^{m} |\alpha_i|^2 \sum_{k=1}^{K_i} |\beta_{i,k}|^2 |\psi_{i,k}^{(A)}\rangle\langle\psi_{i,k}^{(A)}|,$$

where the components $\{|\psi_{i,k}^{(A)}\rangle\}$ are orthogonal to each other. Hence, we can conclude that

$$\begin{aligned} S(\Psi_A) &= \sum_{i=1}^{m} \sum_{k=1}^{K_i} |\alpha_i|^2 |\beta_{i,k}|^2 \log \frac{1}{|\alpha_i|^2 |\beta_{i,k}|^2} \\ &= \sum_{i=1}^{m} |\alpha_i|^2 \sum_{k=1}^{K_i} |\beta_{i,k}|^2 \left(\log \frac{1}{|\alpha_i|^2} + \log \frac{1}{|\beta_{i,k}|^2} \right) \\ &= \sum_{i=1}^{m} |\alpha_i|^2 S(|\psi_i\rangle) + \sum_{i=1}^{m} |\alpha_i|^2 \log \frac{1}{|\alpha_i|^2}. \end{aligned}$$

□

We consider a horizontal cut through the 2D grid of size $n \times (T+1)$ such that the cut has distance at least $\omega(\log n)$ to both the top and the bottom of the grids, and use $S(\cdot)$ to denote the entanglement entropy across this cut. Additionally, we slightly abuse notation by using $S((\psi_{\text{output}})_A)$ to denote the entanglement entropy of the reduced output state $(\psi_{\text{output}})_A$ across the corresponding cut among the n qubits. Formally, if the horizontal cut through the $n \times (T+1)$ 2D grid is positioned between the c-th line and the $(c+1)$-th line, then $S((\psi_{\text{output}})_A)$ is defined as the von Neumann entropy of $(\psi_{\text{output}})_A$, which is the reduced state of $|\psi_{\text{output}}\rangle$ across the cut between the c-th qubit and the $(c+1)$-th qubit among the n qubits. With this notation, we establish the following fact.

Lemma 4.14. *For any $t \in [(3n-1)R, L]$, the t-th legal shape $|\gamma(t)\rangle$ defined in Equation (4.4) satisfies $S(\gamma_A(t)) = S((\psi_{\text{output}})_A)$.*

Proof. For any $t \in [(3n-1)R, L]$, observe that $|\gamma(t)\rangle$ can be decomposed as follows:

$$|\gamma(t)\rangle = (\textbf{dead qudits}) \otimes (\textbf{active qudits}) \otimes (\textbf{unborn qudits}),$$

where (**dead qudits**) denotes qudits in the dead phase, (**active qudits**) denotes qudits in the first, second, or the flag phase, and (**unborn qudits**) denotes qudits in the unborn phase. Moreover, note that with respect to the cut (**dead qudits**) can be further divided into

$$(\textbf{dead qudits}) = (\textbf{dead qudits})_{\text{above}} \otimes (\textbf{dead qudits})_{\text{below}},$$

where $(\textbf{dead qudits})_{\text{above}}$ and $(\textbf{dead qudits})_{\text{below}}$ denote qubits in the dead phase that is above the cut and below the cut, respectively. Similar division can also be applied to the **unborn qudits**. Hence, we have

$$\begin{aligned}|\gamma(t)\rangle = (\textbf{dead qudits})_{\text{above}} \otimes (\textbf{unborn qudits})_{\text{above}} \otimes (\textbf{active qudits}) \\ \otimes (\textbf{dead qudits})_{\text{below}} \otimes (\textbf{unborn qudits})_{\text{below}},\end{aligned}$$

$S(\gamma_A(t))$ thus equals the von Neumann entropy of the reduced state of **active qudits**, which equals $S((\psi_{\text{output}})_A)$ given that the **active qudits** encodes $|\psi_{\text{output}}\rangle$ in their orientations when $t \geq (3n-1)R$. □

Next, we introduce a concept called "turn" to analyze the entanglement structure of the ground state $|\psi_{\text{ground}}\rangle$. Formally, we divide the $L+1$ clock states $|\gamma(0)\rangle, \ldots, |\gamma(L)\rangle$ in legal shapes into $T+1$ turns, where in each turn, the changes of the legal shapes happen on the same side of the cut. As an example, suppose n is even and the cut is between the $\frac{n}{2}$-th line and the $\left(\frac{n}{2}+1\right)$-th line. Then, the first turn consists of $\{|\gamma(0)\rangle, \ldots, |\gamma(n/2)\rangle\}$, the second turn consists of $\{|\gamma(n/2+1)\rangle, \ldots, |\gamma(3n/2)\rangle\}$, and so on. An example with $n = 6$ and $T = 2$ is given in Figure 3. It is worth pointing out that the concept of "turn" is new and is crucial to our analysis regarding the entanglement structure of the ground states.

For the p-th turn of legal shapes starting at the $t_s^{(p)}$-th legal shape and ending at the $t_e^{(p)}$-th legal shape, we define the uniform superposition state of this turn to be

$$|\zeta(p)\rangle \equiv \frac{1}{\sqrt{t_e^{(p)} - t_s^{(p)} + 1}} \sum_{\tau=t_s^{(p)}}^{t_e^{(p)}} |\gamma(\tau)\rangle. \tag{4.9}$$

Then, the ground state $|\psi_{\text{ground}}\rangle$ defined in Equation (4.5) can also be expressed as

$$|\psi_{\text{ground}}\rangle = \sum_{p=1}^{T+1} \sqrt{\frac{t_e^{(p)} - t_s^{(p)} + 1}{L+1}} |\zeta(p)\rangle.$$

Lemma 4.15. *For any $p_1 \neq p_2 \in [1, T+1]$, the uniform superposition states $|\zeta(p_1)\rangle$ and $|\zeta(p_2)\rangle$ of these two turns are cutwise orthogonal with respect to the cut per Definition 4.12.*

Proof. We prove this lemma by showing that for any two states $|\gamma(t_1)\rangle, |\gamma(t_2)\rangle$ in these two turns, respectively, are cutwise orthogonal.

If $|p_1 - p_2| > 1$, note that the number of qudits in dead phases are different on both sides of the cut for any possible $|\gamma(t_1)\rangle$ and $|\gamma(t_2)\rangle$. Hence, they are cutwise orthogonal.

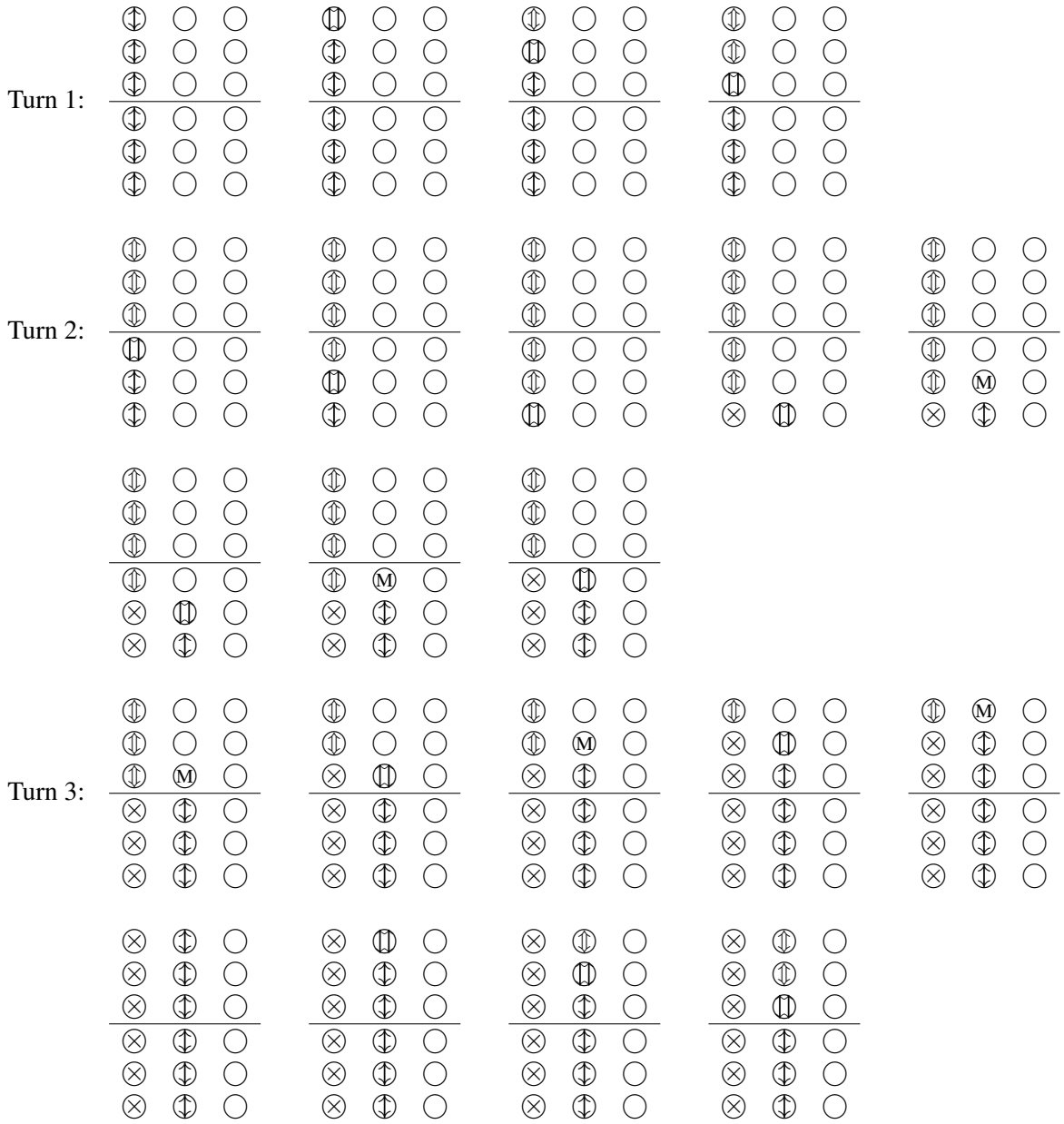


Figure 3: An example of the first three turns when $n = 6$, $T = 2$, and the cut is between the third line and the fourth line.

If $|p_1 - p_2| = 1$, i.e., p_1 and p_2 are two consecutive turns, then the changes of shapes two turns are on different sides of the cut. Without loss of generality we assume $p_2 = p_1 + 1$ and the changes in the p_2-th turn happen below the cut. Then, $|\gamma(t_2)\rangle$ contains a qudit in the flag phase $|\textcircled{\scriptsize F}\rangle$ or the marker phase $|\textcircled{\scriptsize M}\rangle$ below the cut, which is not present in $|\gamma(t_1)\rangle$. As for the part above the cut, note that $|\gamma(t_2)\rangle$ contains a column whose qudits above the cut are all in the second phase $|\textcircled{\scriptsize 2}\rangle$, which is not present in $|\gamma(t_1)\rangle$. Hence, $|\gamma(t_1)\rangle$ and $|\gamma(t_2)\rangle$ are cutwise orthogonal. □

Padding does not change entanglement structure within a turn. The next lemma can be viewed as a sanity check. Suppose we are at the time instance corresponding to $t_s = (3n-1)R$, so that $|\gamma(t_s)\rangle$ corresponds to an encoding of $|\psi_{\text{output}}\rangle$. Note that the state $|\psi_{\text{output}}\rangle$ has nice entanglement properties that we desire. For $t \geq t_s$, all we do to the circuit is pad it with unitaries. Ideally, it should not change the entanglement structure of the encoded state, but it is not immediately obvious that it is indeed the case, because of the complicated way in which we encode the clock. In the next lemma, we assuage some of that concern by showing that the entanglement structure indeed *does not* change, when we consider a superposition of temporal states, for $t > t_s$, that are all part of the same turn.

Lemma 4.16. *For any turn of states in legal shapes that starts at the t_s-th shape and ends at the t_e-th shape, denote*

$$|\zeta\rangle \equiv \frac{1}{\sqrt{t_e - t_s + 1}} \sum_{\tau=t_s}^{t_e} |\gamma(\tau)\rangle$$

to be the uniform superposition state over all the clock states in this turn as in Equation (4.9). Then, if $t_s \geq (3n-1)R$, we have

$$S(\zeta_A) = S(\gamma_A(\tau)) = S((\psi_{\text{output}})_A), \quad \forall \tau \in [t_s, t_e].$$

Otherwise, we have

$$0 \leq S(\zeta_A) \leq 2n.$$

Proof. Without loss of generality we assume the changes of the shapes in this turn happens above the cut. Observe that in all the states in this phase, their **active qudits** string encodes the same quantum state $|\psi_{\text{output}}\rangle$ in their orientations and the encodings are cut through at the same position, however in orthogonal subspaces. Hence, if $|\psi_{\text{output}}\rangle$ admits the following Schmidt decomposition

$$|\psi_{\text{output}}\rangle = \sum_i \nu_i |\psi_i^{(A)}\rangle \otimes |\psi_i^{(B)}\rangle,$$

across the cut, where A and B denote the subsystems above and below the cut, respectively, the state in the τ-th shape $|\gamma(\tau)\rangle$ admits the following decomposition

$$|\gamma(\tau)\rangle = \sum_i \nu_i |\gamma_i^{(A)}(\tau)\rangle \otimes |\gamma_i^{(B)}\rangle,$$

where $\{|\gamma_i^{(A)}(\tau_1)\rangle\}$ and $\{|\gamma_i^{(A)}(\tau_2)\rangle\}$ span orthogonal subspaces for any $\tau_1 \neq \tau_2 \in [t_s, t_e]$, and the RHS of the tensor product is identical for every $t_s \leq \tau \leq t_e$. Hence, the superposition state $|\zeta\rangle$ of this phase satisfies

$$\begin{aligned} |\zeta\rangle &= \frac{1}{\sqrt{t_e - t_s + 1}} \sum_{\tau=t_s}^{t_e} \sum_i \nu_i |\gamma_i^{(A)}(\tau)\rangle \otimes |\gamma_i^{(B)}\rangle \\ &= \sum_i \nu_i \left(\frac{1}{\sqrt{t_e - t_s + 1}} \sum_{\tau=t_s}^{t_e} |\gamma_i^{(A)}(\tau)\rangle \right) \otimes |\gamma_i^{(B)}\rangle. \end{aligned}$$

Hence, for any $t_s \leq \tau \leq t_e$, tracing out the left side of $|\gamma(\tau)\rangle$ yields the same reduced state as tracing out the left side of $|\zeta\rangle$, by which we can conclude that

$$S(\zeta_A) = S(\gamma_A(\tau)) = S((\psi_{\text{output}})_A), \quad \forall t_s \leq \tau \leq t_e.$$

where the last equation is from Lemma 4.14.

□

Remark 4.17. As for the case where $t_s < (3n-1)R$, it is possible that in this turn there exists some clock state $|\gamma(\tau)\rangle$ encoding an intermediate state of the circuit rather than $|\psi_{\text{output}}\rangle$. Nevertheless, all the clock states in this turn have their (**active qudits**) concentrated within only two columns of the 2D grid. Hence, $|\zeta\rangle$ is in a Hilbert space spanned by $2n$ basis states which has dimension at most 2^{2n}, which leads to

$$0 \le S(\zeta_A) \le 2n.$$

Showing that the ground state inherits desirable entanglement properties because of padding. In this section, we will collect all our ideas together and prove that the entanglement entropy of the ground state of our clock Hamiltonian is, more or less, the same as the entanglement entropy of $|\psi_{\text{output}}\rangle$. At a high level, this is because of padding. Since we pad with sufficiently many identities, the entanglement structure of the ground state looks fairly similar to $|\psi_{\text{output}}\rangle$, because of a preponderence of terms which encode $|\psi_{\text{output}}\rangle$ in the superposition.

Lemma 4.18. *Consider a horizontal cut through the 2D grid of size $n \times (T+1)$ such that the cut has distance at least $\omega(\log n)$ to both the top and the bottom of the grid, the entanglement entropy $S((\psi_{\text{ground}})_A)$ of the ground state $|\psi_{\text{ground}}\rangle$ defined in Equation (4.5) satisfies*

$$\left(1-\frac{1}{n}\right)\cdot S((\psi_{\text{output}})_A) \le S((\psi_{\text{ground}})_A) \le S((\psi_{\text{output}})_A) + \text{poly}\log n,$$

for any $T = \text{poly}\, n$ satisfying $T \ge 3nR$.

Proof. For any $p \in [1, T+1]$, we denote

$$\alpha_p \equiv \sqrt{\frac{t_e^{(p)} - t_s^{(p)} + 1}{L+1}},$$

where $t_s^{(p)}$ and $t_e^{(p)}$ separately denotes the number of starting shape and ending shape of the p-th turn. Then the ground state $|\psi_{\text{ground}}\rangle$ defined in Equation (4.5) satisfies

$$|\psi_{\text{ground}}\rangle = \sum_{p=1}^{T+1} \alpha_p |\zeta(p)\rangle.$$

Since the states $|\zeta(p)\rangle$ are shown to be cutwise orthogonal by Lemma 4.15, we can derive that

$$S((\psi_{\text{ground}})_A) = \sum_{p=1}^{T+1} |\alpha_p|^2 S(\zeta_A(p)) + 2\sum_{p=1}^{T+1} |\alpha_p|^2 \log(1/|\alpha_p|)$$

according to Lemma 4.13. Furthermore, by Lemma 4.16 we can establish that

$$S(\zeta_A(p)) = S((\psi_{\text{output}})_A), \quad \forall p \in (R+1, T+1],$$

which leads to

$$S((\psi_{\text{ground}})_A) = \sum_{p=R+2}^{T+1} |\alpha_p|^2 S((\psi_{\text{output}})_A) + 2\sum_{p=1}^{T+1} |\alpha_p|^2 \log(1/|\alpha_p|) + \sum_{p=1}^{R+1} |\alpha_p|^2 S(\zeta_A(p)) \tag{4.10}$$

Given that $T = \operatorname{poly} n$, we have

$$0 \leq \sum_{p=1}^{T+1} |\alpha_p|^2 \log(1/|\alpha_p|) \leq \operatorname{poly} \log n$$

for any possible values of $\alpha_1, \ldots, \alpha_{T+1}$. As for the third term in Equation (4.10), we have

$$0 \leq \sum_{p=1}^{R+1} |\alpha_p|^2 S(\zeta_A(p)) \leq 2n \cdot \sum_{p=1}^{R+1} |\alpha_p|^2,$$

given that $0 \leq S(\zeta_A(p)) \leq 2n$ by Lemma 4.16. Furthermore, we have

$$\sum_{p=1}^{R+1} |\alpha_p|^2 \leq \sum_{p=1}^{R+1} \frac{t_e^{(p)} - t_s^{(p)} + 1}{L+1} \leq \frac{3nR}{2nT+1} \leq \frac{1}{n},$$

and

$$\sum_{p=R+2}^{T+1} |\alpha_p|^2 = 1 - \sum_{p=1}^{R+1} |\alpha_p|^2 \geq 1 - \frac{1}{n}.$$

Thus, we can conclude that

$$\left(1 - \frac{1}{n}\right) \cdot S((\psi_{\text{output}})_A) \leq S((\psi_{\text{ground}})_A) \leq S((\psi_{\text{output}})_A) + \operatorname{poly} \log n.$$

□

4.3.3 Learning ground state entanglement structure for 2D geometrically local Hamiltonians

We can now use the padded circuit-to-2D-Hamiltonian construction to convert the pseudoentangled states ensembles we constructed in Section 3.3 into families of 2D Hamiltonians for which it is difficult to decide whether the ground state has low entanglement (i.e., $\operatorname{poly} \log n$) or high entanglement (i.e., $\Omega(n)$) entanglement across horizontal cuts through the $n \times \operatorname{poly}(n)$ grid. Formally, we show the following.

Theorem 4.19. *For every $n \in \mathbb{N}$, there exist two families $\mathcal{H}_n^{\text{low}}$ and $\mathcal{H}_n^{\text{high}}$ of* geometrically 2D-local *Hamiltonians on $(n \times \operatorname{poly} n)$ qudits arranged in an $n \times \operatorname{poly}(n)$ grid with spectral gap $\Omega(1/\operatorname{poly}(n))$, and there are efficient procedures that sample (classical descriptions of) Hamiltonians from either family (denoted $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$) with the following properties:*

(i) *Hamiltonians sampled according to $H \leftarrow \mathcal{H}_n^{\text{low}}$ and $H \leftarrow \mathcal{H}_n^{\text{high}}$ are computationally indistinguishable under Assumption 2.19.*

(ii) *With overwhelming probability, the ground states of Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have $\operatorname{poly} \log n$ entanglement across horizontal cuts through the grid that are at least $\omega(\log n)$ far from the boundary, and Hamiltonians $H \leftarrow \mathcal{H}_n^{\text{low}}$ have $\Omega(n)$ entanglement across the same cuts.*

Proof. We consider the same construction of $\mathcal{H}_n^{\text{low}}$ and $\mathcal{H}_n^{\text{high}}$ as in Theorem 4.2, except that we now use the 2D circuit-to-Hamiltonian construction described in Section 4.3.1. With this, we only need to show Item (ii)

as the condition on the spectral gap follows from [AVDK+08] and the other properties follow in exactly the same way as in the proof of Theorem 4.2

Consider a Hamiltonian $H \leftarrow \mathcal{H}_n^{\text{low}}$ or $H \leftarrow \mathcal{H}_n^{\text{high}}$. Let $|\psi_{\text{ground}}\rangle$ be the history state of the circuit as defined in Equation (4.5). By Lemma 4.11 any ground state of H is ϵ-close for any $\epsilon = 1/\text{poly}(n)$ that we can choose. Therefore, choosing ϵ small enough and using the continuity bound for the von Neumann entropy (Lemma 2.7), we can ensure that any ground state of H only differs in entanglement entropy from $|\psi_{\text{ground}}\rangle$ by $1/\text{poly}(n)$. It therefore suffices to show Item (ii) for $|\psi_{\text{ground}}\rangle$. This follows directly from Lemma 4.18 and the fact that the states $|\psi_{\text{output}}\rangle$ are pseudoentangled with entanglement gap $O(\text{poly}\log n)$ vs $\Omega(n)$ by our pseudoentanglement construction (Theorem 3.18). □

Remark 4.20. Just as in Remark 4.3, under the standard LWE assumption (Assumption 2.18) Theorem 4.19 still holds, but with the smaller entanglement gap $O(n^\delta)$ vs $\Omega(n)$ for any $\delta > 0$.

References

[AA23] Anurag Anshu and Srinivasan Arunachalam. A survey on the complexity of learning quantum states. *arXiv preprint arXiv:2305.20069*, 2023.

[AAG22] Anurag Anshu, Itai Arad, and David Gosset. An area law for 2d frustration-free spin systems. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 12–18, 2022.

[ABF+23] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement. *arXiv preprint arXiv:2211.00747v2*, 2023.

[AFBV23] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. Computational entanglement theory, 2023.

[AGIK09] Dorit Aharonov, Daniel Gottesman, Sandy Irani, and Julia Kempe. The power of quantum systems on a line. *Communications in mathematical physics*, 287(1):41–65, 2009.

[ALVV17] Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick. Rigorous RG algorithms and area laws for low energy eigenstates in 1D. *Communications in Mathematical Physics*, 356:65–105, 2017.

[Aud07] Koenraad M R Audenaert. A sharp continuity estimate for the von Neumann entropy. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8127–8136, June 2007.

[AVDK+08] Dorit Aharonov, Wim Van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM review*, 50(4):755–787, 2008.

[BASTS08] Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: Motivation and constructions. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 292–303. IEEE, 2008.

[BCLPG20] Johannes Bausch, Toby S Cubitt, Angelo Lucia, and David Perez-Garcia. Undecidability of the spectral gap in one dimension. *Physical Review X*, 10(3):031038, 2020.

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

[BEM+23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the uhlmann transformation problem. *arXiv preprint arXiv:2306.13073*, 2023.

[BFV19] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational pseudorandomness, the wormhole growth paradox, and constraints on the ads/cft duality. *arXiv preprint arXiv:1910.14646*, 2019.

[BS19] Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference*, pages 229–250. Springer, 2019.

[Chr06] Matthias Christandl. The structure of bipartite quantum states-insights from group theory and cryptography. *arXiv preprint quant-ph/0604183*, 2006.

[CPF+10] Marcus Cramer, Martin B Plenio, Steven T Flammia, Rolando Somma, David Gross, Stephen D Bartlett, Olivier Landon-Cardinal, David Poulin, and Yi-Kai Liu. Efficient quantum state tomography. *Nature communications*, 1(1):149, 2010.

[CPGW15] Toby S Cubitt, David Perez-Garcia, and Michael M Wolf. Undecidability of the spectral gap. *Nature*, 528(7581):207–211, 2015.

[DHR02] Matthew J. Donald, Michał Horodecki, and Oliver Rudolph. The uniqueness theorem for entanglement measures. *Journal of Mathematical Physics*, 43(9):4252–4272, August 2002.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, Jan 2005.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, December 1973.

[GH20] Alexandru Gheorghiu and Matty J Hoban. Estimating the entropy of shallow circuit outputs is hard. *arXiv preprint arXiv:2002.12814*, 2020.

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. 2010.

[GV99] Oded Goldreich and Salil Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of szk. In *Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)(Cat. No. 99CB36317)*, pages 54–73. IEEE, 1999.

[Has07] Matthew B Hastings. An area law for one-dimensional quantum systems. *Journal of statistical mechanics: theory and experiment*, 2007(08):P08024, 2007.

[HH01] Pawel Horodecki and Ryszard Horodecki. Distillation and bound entanglement. *Quantum Information & Computation*, 1:45–75, 07 2001.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[HHT01] Patrick M Hayden, Michal Horodecki, and Barbara M Terhal. The asymptotic entanglement cost of preparing a quantum state. *Journal of Physics A: Mathematical and General*, 34(35):6891, 2001.

[HKT+22] Hsin-Yuan Huang, Richard Kueng, Giacomo Torlai, Victor V Albert, and John Preskill. Provably efficient machine learning for quantum many-body problems. *Science*, 377(6613):eabk3333, 2022.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[KSV02] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, USA, 2002.

[LP11] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology–CT-RSA 2011: The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, pages 319–339. Springer, 2011.

[LVV15] Zeph Landau, Umesh Vazirani, and Thomas Vidick. A polynomial time algorithm for the ground state of one-dimensional gapped local Hamiltonians. *Nature Physics*, 11(7):566–569, 2015.

[MVV22] Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. Efficient certifiable randomness from a single quantum device, 2022.

[NVY18] Chinmay Nirkhe, Umesh Vazirani, and Henry Yuen. Approximate low-weight check codes and circuit lower bounds for noisy ground states. *arXiv preprint arXiv:1802.07419*, 2018.

[Pei16] Chris Peikert. A decade of lattice cryptography. *Foundations and trends® in theoretical computer science*, 10(4):283–424, 2016.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[RT06] Shinsei Ryu and Tadashi Takayanagi. Holographic derivation of entanglement entropy from the anti–de sitter space/conformal field theory correspondence. *Physical review letters*, 96(18):181602, 2006.

[SCV08] Norbert Schuch, Ignacio Cirac, and Frank Verstraete. Computational difficulty of finding matrix product ground states. *Physical review letters*, 100(25):250501, 2008.

[SN96] Benjamin Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, 54:2629–2635, Oct 1996.

[SV03] Amit Sahai and Salil Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM (JACM)*, 50(2):196–249, 2003.

[Vad12] Salil Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012.

[Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, Mar 2016.

[Woo01] William K. Wootters. Entanglement of formation and concurrence. *Quantum Info. Comput.*, 1(1):27–44, jan 2001.

[Zha23] Mark Zhandry. Quantum minimalism, 2023. Talk at Simons Institute, https://www.youtube.com/live/7cqnrASfjco?si=1XlLZpqfaEsBEVp8.