Post-Quantum Cryptography from Quantum Stabilizer Decoding

Jonathan Z. Lu*[1], Alexander Poremba†[2], Yihui Quek‡[3], and Akshar Ramkumar§[4]

[1] *Massachusetts Institute of Technology, Cambridge, MA*
[2] *Boston University, Boston, MA*
[3] *École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland*
[4] *California Institute of Technology, Pasadena, CA*

October 6, 2026

Abstract

Post-quantum cryptography currently rests on a small number of hardness assumptions, posing significant risks should any one of them be compromised. This vulnerability motivates the search for new and cryptographically versatile assumptions that make a convincing case for quantum hardness.

In this work, we argue that decoding random quantum stabilizer codes—a quantum analog of the well-studied LPN problem—is an excellent candidate. This task occupies a unique middle ground: it is inherently native to *quantum* computation, yet admits an equivalent formulation with purely *classical* input and output, as recently shown by Khesin *et al.* (STOC '26). We prove that the average-case hardness of quantum stabilizer decoding implies the core primitives of classical Cryptomania, including public-key encryption (PKE) and oblivious transfer (OT), as well as one-way functions. Our constructions are moreover practically efficient: our PKE scheme achieves essentially the same efficiency as state-of-the-art LPN-based PKE. We also provide substantial evidence that stabilizer decoding does not reduce to LPN, suggesting that the former problem constitutes a genuinely new post-quantum assumption.

Our primary technical contributions are twofold. First, we give a reduction from random quantum stabilizer decoding to an average-case problem closely resembling LPN, but which is equipped with additional symplectic algebraic structure. While this structure is essential to the quantum nature of the problem, it raises significant barriers to cryptographic security reductions. Second, we develop a new suite of scrambling techniques for such structured linear spaces, and use them to produce rigorous security proofs for all of our constructions.

1 Introduction

The remarkable success of modern cryptography rests on a surprisingly small number of computational hardness assumptions. Over the past four decades, these assumptions—ranging from the difficulty of factoring [RSA78] to the hardness of discrete logarithms [DH76, Mer78] and various lattice problems [HPS98, MR09]—have underpinned the construction of essentially all known cryptographic primitives. The advent of quantum computing, however, has forced a fundamental re-evaluation of this foundation. Shor's algorithm [Sho94] and its variants [Reg24] show that many of the assumptions

*lujz@mit.edu
†poremba@bu.edu
‡yihui.quek@epfl.ch
§aramkuma@caltech.edu

that underlie classical public-key cryptography are vulnerable to efficient quantum attacks, rendering large swathes of existing cryptographic infrastructure insecure in a quantum world.

In response, the cryptographic community has turned to an even smaller suite of candidate *post-quantum* assumptions [BL17, CJL+16, LM24], primarily in the world of lattices [MR09, Reg09], codes [Pie12, BCL+19], multivariate polynomial systems [CCLST22] and isogenies of elliptic curves [CLM+18]. Among these assumptions, the *Learning with Errors* (LWE) problem [Reg09] and its binary predecessor, *Learning Parity with Noise* (LPN) [BFKL94, Pie12], have emerged as a central basis of hardness. These problems enjoy worst-case to average-case reductions [Reg09, BLVW19], a rich algebraic structure, and a remarkable versatility in supporting a wide array of cryptographic constructions, including public-key encryption [Reg09, Ale03], digital signatures [Pie12], oblivious transfer [BCG+19], general secure multi-party computation [BCG+19], collision-resistant hashing [AHKI+17] and, in some cases, even homomorphic encryption [Gen09, BV14, CGHKV24].

Yet, despite their prominence, our increasing reliance on LWE and LPN as a foundation for post-quantum security is a reason for concern. The history of cryptography has taught us that even long-standing hardness assumptions can be susceptible to unexpected algorithmic breakthroughs, as in the case of factoring and discrete logarithms [Sho94]. In fact, even "quantum-safe" assumptions have recently experienced devastating classical attacks, as in the case of isogenies [Rob22] and multivariate quadratics [Beu22] that were initially believed to be secure. While LWE and LPN have so far resisted quantum attacks, there is reason to be cautious about their long-term viability: lattice problems are intimately connected to the dihedral hidden subgroup problem [Reg03], which is known to admit subexponential-time quantum algorithms [Kup04]; moreover, recent years have also seen renewed efforts targeting lattices [ES16, Che24, EH22, AJOP20, GKZ19] and codes [Eld23] via quantum attacks that, while not yet fully successful, suggest that the landscape is far from settled. This concern is further amplified by the fact that most LWE/LPN-based constructions operate under special parameter regimes that are much less understood [DP12, AHKI+17], and where worst-to-average-case reductions often do not apply [BLVW19, YZ20]. These vulnerabilities have recently motivated the search for alternative LWE/LPN-like noisy linear-algebraic assumptions which are less susceptible to attacks than existing ones, and yet still suffice for public-key encryption [GJL+25].

More broadly, many standard post-quantum assumptions are rooted in manifestly *classical* problems in mathematics—lattices, codes, or algebraic structures—whose relation to quantum computation is far from direct. Because of this disconnect, it is unlikely that even a major breakthrough undermining all of today's leading post-quantum assumptions would have a substantial impact on fundamental tasks in quantum information science. Indeed, as recent work [BEM+26, Kre21] suggests, central quantum tasks such as compressing quantum information, decoding noisy quantum channels and other local entanglement transformations lie outside of classical cryptography altogether, and may be hard even if P = NP. This disparity has led to the design of "fully quantum" cryptography, collectively known as *MicroCrypt* [Sat26, AQY22, MY24, MPSY24, BHHP25], which is inherently non-classical—typically relying on quantum communication between multiple quantum parties—and which may exist even if one-way functions do not. Even if we are willing to believe that P ≠ NP, this begs the question of whether the foundations of post-quantum cryptography, likewise, may benefit from a fundamental re-evaluation:

> *Can we also base classical cryptography on hardness assumptions which are native to quantum information processing?*

By the usual win-win premise of provable cryptography, any algorithmic advances on such an assumption would likely also have far-reaching implications for the foundations of quantum information science.

1.1 Our approach

In this work, we propose an affirmative answer to the aforementioned question by exploring the cryptographic potential of a natural quantum computational assumption: the hardness of decoding *random* quantum stabilizer codes.

Quantum stabilizer codes are among the most central objects in all of quantum information science. Not only do they form the backbone of all of quantum error correction and quantum fault-tolerance [Got24, AF24], but they are also fundamental in the theory of quantum communication [Smi06, Wil13], entanglement distillation [BDSW96, DW05, WKB10], quantum authentication [BCG+02, DS18, DGJ+20], the interactive verification of quantum computations [ABOEM17], and even in quantum gravity and black hole physics [HP07, YK17, HH13, PRV26].

From a complexity-theoretic perspective, stabilizer decoding is a natural quantum analog of classical decoding problems, such as the *nearest codeword problem* [BLVW19] or its dual *syndrome decoding problem* [BMvT78] for linear codes. In the *worst* case, the quantum decoding problem appears strictly harder than its classical counterpart: optimal quantum stabilizer decoding is #P-complete [IP15], whereas the corresponding classical decoding problem is merely NP-complete [BMvT78]. This disparity is due to quantum degeneracy: different Pauli errors can act identically on the codespace, so optimal recovery maximizes the total probability of an error class.

At first glance, therefore, it may seem counterintuitive to base classical cryptography on a quantum decoding problem. After all, stabilizer decoding appears to involve inherently quantum objects—quantum codewords and quantum noise. However, recent work [KLP+26] has revealed a surprising equivalence: average-case quantum stabilizer decoding is equivalent (under polynomial-time *quantum* reductions) to a purely *classical* average-case problem, i.e. one that involves only classical inputs and classical outputs, yet retains the essential quantum-mechanical structure and difficulty of the original problem.

This equivalence suddenly opens the door to a tantalizing possibility: *Can we base post-quantum cryptography on the hardness of decoding quantum codes?*

Cryptomania Meets Quantum Error Correction. Driven by this possibility, we show that the *average-case* hardness of quantum stabilizer decoding indeed suffices to construct core primitives of *classical* Cryptomania [Imp95], including:

- public-key encryption (PKE),
- oblivious transfer (OT), as well as
- one-way functions (OWF).

Since these primitives are known to imply symmetric encryption, asymmetric encryption, and general secure multi-party computation, this establishes stabilizer decoding as a versatile foundation for classical cryptography.

Importantly, our constructions are *efficient and near-optimal*, achieving essentially the same performance as state-of-the-art LPN-based schemes, up to small constant factors.

Learning Stabilizers with Noise. The starting point of this work is a recent characterization of average-case stabilizer decoding by the name of *Learning Stabilizers with Noise* (LSN) [PQS26, KLP+26]—the natural quantum analog of LPN [BFKL94], which is illustrated in Figure 1. The LSN problem was first introduced by Poremba, Quek and Shor [PQS26] who gave an initial assessment of the problem in terms of algorithms and complexity. In subsequent work, Khesin, Lu, Poremba, Ramkumar and Vaikuntanathan [KLP+26] showed that LSN (in most parameter regimes) is *at least*

	Learning Stabilizers with Noise	Learning Parity with Noise
Input:	$(\mathbf{C} \sim \mathcal{C}_n,\ \mathbf{E}\,\mathbf{C}\,\lvert 0^{n-k}, \psi\rangle\,)$	$(\mathbf{A} \sim \mathbb{Z}_2^{n\times k},\ \mathbf{A}\mathbf{x} + \mathbf{e} \pmod 2)$
Noise:	Depolarizing noise $\mathbf{E} \sim \mathcal{D}_p^{\otimes n}$	Bernoulli noise $\mathbf{e} \sim \mathsf{Ber}_p^{\otimes n}$
Task:	Recover k-qubit Haar state $\lvert\psi\rangle$	Recover the string $\mathbf{x} \sim \mathbb{Z}_2^k$

Figure 1: Comparison between (the *state* variant of) LSN [KLP+26, PQS26] and LPN [BFKL94]. In both cases, the input features a classical description of a *random* code; in the case of LSN, it is a random *Clifford* encoding $\mathbf{C} \sim \mathcal{C}_n$ of an $[[n, k]]$ quantum stabilizer code, whereas in the case of LPN it is given by a random *generator matrix* $\mathbf{A} \sim \mathbb{Z}_2^{n\times k}$ of a classical $[n, k]$ linear code. The input further consists of a noisy codeword; in the case of LSN, it is in the form of a random quantum codeword, whereas for LPN it consists of a random classical codeword. The parameters are characterized by the logical (qu)bits k, physical (qu)bits n, and the error probability per physical (qu)bit p.

as hard as LPN, providing a much more solid foundation for the average-case hardness of quantum stabilizer decoding.

Here we make the case that LSN is a compelling post-quantum assumption. First, LSN is *genuinely quantum in origin*. Unlike leading post-quantum assumptions, such as LWE or LPN, which are classical in nature but believed to resist quantum attacks, LSN arises naturally within fundamental quantum information processing itself. Second, LSN appears to be *incomparable* to LPN in cryptographically relevant parameter regimes (as we explain in Section 2), thus making it likely to constitute a genuinely new and distinct hardness assumption.

Basing cryptography off of LSN thus creates a "win-win-win" scenario:

- If LSN is secure, we obtain a new basis for post-quantum cryptography, grounded in a central problem in quantum information processing.
- If LSN is broken, this would represent a major breakthrough in our current understanding of quantum stabilizer codes, with profound downstream implications for many areas of quantum information science.
- If LSN turns out to be equivalent to LPN, this would reveal deep and unexpected connections between classical and quantum error correction.

1.2 Our results

We now briefly summarize our main contributions. At a high level, we show that the average-case hardness of decoding random quantum stabilizer codes—captured by (the state variant of) LSN—is sufficient to instantiate all of the core primitives of classical Cryptomania [Imp95].

Below, we use $n \in \mathbb{N}$ to denote the security parameter and block length of the stabilizer code, and we let $p \in (0, 1)$ denote the noise rate, as in Figure 1. For an in-depth discussion of our assumption and its parameters, we refer to the technical overview in Section 2.

Public-key encryption. In Section 5, we construct a PKE scheme from the hardness of LSN in the low-noise regime with $p = \Theta(1/\sqrt{n})$. The basic scheme matches the parameter regime and efficiency of state-of-the-art Alekhnovich-style LPN-based encryption [Ale03, DP12], with $O(n^2)$ encryption time and $O(n)$ decryption time. One important distinction is that our scheme is based on LSN with $k = \log(n)$, logarithmically many logical qubits. Meanwhile, Alekhnovich-style LPN-based encryption relies on the hardness of LPN with $k = O(n)$ logical bits. However, while the complexity

of LPN depends heavily on the number of logical bits, this dependence is not known to hold for LSN, which is not known to rely in any way on the number of logical qubits. In fact, the known LPN-based hardness bounds at constant noise rates are completely uniform in k, holding even with a single logical qubit [KLP+26]. We prove the following theorem.

> **Theorem (informal).** Assuming (the state variant of) LSN is hard in the low-noise regime, there exists an efficient post-quantum PKE scheme.

Our PKE scheme is formally described in Construction 5.1, and we prove its security in Theorem 5.4. We note that our security reduction is highly non-trivial and requires many new technical insights into LSN and its related variants; these form the main technical contributions of the paper.

Oblivious transfer. In Section 6, we strengthen our scheme to obtain a strongly uniform public-key encryption scheme, which once again rests on the low-noise regime with $p = \Theta(1/\sqrt{n})$. Using known black-box transformations, this implies malicious-secure oblivious transfer:

> **Theorem (informal).** Assuming (the state variant of) LSN is hard in the low-noise regime, there exist efficient post-quantum malicious-secure OT protocols with constant rounds and ε-simulation, or polynomial rounds and full simulation.

Since oblivious transfer implies general secure multi-party computation, this establishes that LSN suffices for the full power of Cryptomania.

One-way functions. In Appendix B, we construct a one-way function (OWF) from stateLSN in the constant-noise regime $p = \Omega(1)$. This gives symmetric cryptography directly from the hardest possible parameter setting of the problem.

> **Theorem (informal).** Assuming (the state variant of) LSN is hard in the constant noise regime, there exists a post-quantum OWF.

Importantly, this variant of LSN is known to be at least as hard as LPN in most regimes [KLP+26].

Taken together, these results show that the hardness of decoding random quantum stabilizer codes suffices to realize symmetric encryption, public-key encryption, and malicious-secure multi-party computation. Our constructions match the efficiency of the best known LPN-based schemes [Pie12] while resting on an assumption that is quantum-native and, as we argue in Appendix D, plausibly incomparable to existing post-quantum assumptions.

1.3 Related work

The hardness of decoding random classical linear codes and the closely related LPN (Learning Parity with Noise) problem has been studied extensively in coding theory and cryptography; see e.g. [ACPS09, GRS08, JW05, FGKP06, AG11, Ale03, Pie12, HB01, Lyu05, YZW+19, BFKL94]. A common formulation of LPN presents the adversary with a sequence of n noisy linear samples $\{(\mathbf{a}_i,\ \langle \mathbf{a}_i, \mathbf{x}\rangle + e_i)\}_{i=1}^n$ (where $\mathbf{x} \in \mathbb{Z}_2^k$), and hence a significant body of work has been focused on the fine-grained regimes where the number of samples n (equivalently, the block length of the code) is significantly larger than the message length. From a coding-theoretic perspective, this corresponds to decoding a random linear code with vanishing rate $R = k/n$. For example, BKW-style techniques yield $2^{O(k/\log k)}$-time algorithms when n is superpolynomial in k [BKW03], and refinements give $2^{O(k/\log\log k)}$-time algorithms when n is slightly superlinear in k [Lyu05]. Despite decades of work,

however, no subexponential-time algorithm is known in the constant-rate, constant-noise regime $n = \Theta(k)$, which is the regime underlying many important LPN-based cryptographic constructions. In the constant-rate, constant-noise regime, the best known algorithms for LPN tend to involve variants of *information set decoding* (ISD) attacks [Pra62, Ste88] which run in exponential time [CDMT24].

The study of quantum stabilizer decoding has historically followed a different direction. Most prior work has focused on *worst-case* formulations of the problem, often in the form of maximum-likelihood decoding, and established classical hardness results and complexity-theoretic barriers for these variants [HLG11, IP15, KL20]. Only recently the attention shifted to *average-case* formulations that are more suitable for cryptographic applications. In particular, Poremba, Quek, and Shor introduced the *Learning Stabilizers with Noise* (LSN) problem and provided an initial analysis of its algorithmic and complexity-theoretic properties [PQS26]. They also constructed a quantum bit commitment scheme from the hardness of the LSN problem. Subsequent work of Khesin, Lu, Poremba, Ramkumar and Vaikuntanathan further clarified the landscape by relating average-case stabilizer decoding to classical noisy linear problems like LPN in many parameter regimes [KLP+26]. This work shows that the problem admits a purely classical description while retaining the symplectic algebraic structure intrinsic to stabilizer codes, thereby providing initial evidence that decoding random stabilizer codes may serve as a meaningful cryptographic hardness assumption.

Outside of quantum error correction, there have been a number of recent attempts at building *quantum* rather than *classical* cryptography from other natural average-case hard computational tasks [BHHP25, KT25, FGSY25, HHM25, HM25, CGGH24, MX24]. However, unlike in our work, these constructions are inherently quantum (typically requiring quantum communication between multiple quantum parties) and do not give rise to classical cryptographic primitives as in our work.

2 Technical overview

The three primitives on which this paper focuses are one-way functions (OWF), public-key encryption (PKE), and oblivious transfer (OT). All have been constructed—with a high degree of practical efficiency—from the LPN assumption [Ale03, DP12, DGH+20, DDN14, FMV19].

Our main goal is to construct each of these primitives in such a way that

(a) breaking each primitive is at least as hard as decoding a random quantum stabilizer code, and

(b) each primitive's efficiency is as good as the state-of-the-art corresponding LPN-based construction, up to small constant factors.

This overview sketches the key technical ingredients for our constructions. Our general recipe proceeds as follows. First, we reduce the task of decoding a random quantum stabilizer code to the task of decoding a random *classical* linear code drawn from an ensemble of codes satisfying a certain algebraic structure. This problem is known as *symplectic* LPN (sympLPN), and was introduced recently as a technical tool to reduce LPN to average-case quantum stabilizer decoding in the high-noise regime [KLP+26]. Because sympLPN and LPN appear similar conceptually, one could hope that LPN-based cryptographic constructions would be readily amenable to adaptation into a sympLPN-based protocol, thereby achieving constructions secured by the hardness of quantum error correction. In reality, this intuition only holds reasonably well for OWFs, wherein inverting the OWF is essentially always equivalent to solving the underlying computational problem anyway. Asymmetric cryptographic protocols based on LPN, on the other hand, rely critically on the fact that the encoding matrix of the LPN instance features uniformly random, independent entries as part of the security proofs, and thus break down when this assumption is relaxed. *This breakdown poses a serious technical barrier when proving the security of* sympLPN*-based schemes.*

The second component of our recipe involves overcoming these barriers by introducing an entirely new suite of techniques for scrambling and unscrambling information in linear subspaces, with the algebraic conditions specified by sympLPN. This approach enables us to rigorously prove the security of our constructions under the hardness of stateLSN, at the cost of significantly increasing the technicality of the proofs relative to those of LPN-based schemes.

2.1 Reduction to an LPN-like Classical Problem

Informally, $\mathsf{stateLSN}(k, n, p)$ is the task of decoding a random quantum stabilizer code with k logical qubits, n physical qubits, and noise rate $p \in (0, 1)$. Specifically, we draw a Haar-random (i.e. uniformly random) logical state $|\psi\rangle$ as well as a random n-qubit Clifford operator $\mathbf{C}$. We also draw a random error operator $\mathbf{E}$ from the *depolarizing* distribution $\mathcal{D}_p^{\otimes n}$—the natural quantum analog of Bernoulli error (i.e. binary symmetric channel) in classical error correction.

The task of stateLSN is to approximately recover the logical state $|\psi\rangle$, given a classical description of the code $\mathbf{C}$ and the noisy code state $\mathbf{EC}(|0^{n-k}\rangle \otimes |\psi\rangle)$. Being a problem with manifestly quantum inputs and outputs, stateLSN as stated cannot be used directly for classical cryptography. However, if we can produce a *quantum reduction* from stateLSN to a problem with manifestly classical inputs and outputs, then we can at once use this classical problem directly to construct cryptography and be sure that such protocols are secured directly by the hardness of stateLSN. As a first step, consider a variant of stateLSN wherein the logical state $|\psi\rangle$ is a uniformly random *bitstring* $|\mathbf{x}\rangle$ for $\mathbf{x} \sim \mathbb{Z}_2^k$, rather than a Haar-random state; thus the output of LSN is classical though the input remains quantum. This variant is known as LSN [PQS26], and when $k = O(\log n)$ there is a known quantum reduction from stateLSN to LSN [KLP+26]. Importantly, while the hardness of LPN is characterized by the logical dimension k—there is a brute-force guess-and-check $\mathrm{poly}(2^k, n)$-time algorithm to solve it—the hardness of LSN does not appear to depend on k. At first glance, this may seem counterintuitive. The reason is that, unlike for LPN, there is no known efficient method of verifying proposed LSN solutions. Indeed, at constant noise rates, stateLSN is known to be as hard as constant-rate LPN *even for a single logical qubit* [KLP+26]. Hence, the restriction to $k = O(\log n)$ does not necessarily come at the cost of hardness.

Moreover, LSN is equivalent (via efficient quantum reductions) to a completely classical problem, which we henceforth also refer to as LSN. Defining this classical problem requires a symplectic form on the even-dimensional ambient space $\mathbb{Z}_2^{2n}$. Given bitstrings $(\mathbf{a}, \mathbf{b}), (\mathbf{a}', \mathbf{b}') \in \mathbb{Z}_2^{2n}$, the *symplectic inner product* is given by

$$(\mathbf{a}, \mathbf{b}) \odot (\mathbf{a}', \mathbf{b}') := \mathbf{a} \cdot \mathbf{b}' + \mathbf{a}' \cdot \mathbf{b} \pmod 2. \tag{1}$$

Then, the classical equivalent of $\mathsf{LSN}(k, n, p)$ is the task of recovering a bitstring $\mathbf{y} \sim \mathbb{Z}_2^k$, given $([\mathbf{A} \,|\, \mathbf{B}], \mathbf{Ax} + \mathbf{By} + \mathbf{e})$, where $\mathbf{x} \sim \mathbb{Z}_2^n, \mathbf{A} \in \mathbb{Z}_2^{2n \times n}, \mathbf{B} \in \mathbb{Z}_2^{2n \times k}, \mathbf{e} \in \mathbb{Z}_2^{2n}$; $\mathbf{A}$ and $\mathbf{B}$ are sampled jointly and uniformly subject to each having symplectically orthogonal columns and $[\mathbf{A} \,|\, \mathbf{B}]$ having full column rank, while $\mathbf{e}$ is drawn from a symplectic representation of the depolarizing distribution $\mathcal{D}_p^{\otimes n}$. Concretely, each pair (e_j, e_{n+j}) is i.i.d., being $(0, 0)$ with probability $1 - p$ and $(0, 1), (1, 0), (1, 1)$ each with probability $p/3$.

While completely classical, $\mathsf{LSN}(k, n, p)$ still differs structurally from $\mathsf{LPN}(k, n, p)$ in that only a small part of the effective logical state $[\mathbf{x} \,|\, \mathbf{y}]$ needs to be recovered.[1] In LPN, the entire logical state must be recovered.

Surprisingly, however, we are able to reduce LSN to a much more LPN-like problem, known as $\mathsf{sympLPN}(k, n, p)$. This is the same task as $\mathsf{LPN}(k, 2n, p)$, except the encoding matrix $\mathbf{A} \in \mathbb{Z}_2^{2n \times k}$ is

[1] This is due to a uniquely quantum phenomenon called *stabilizer degeneracy* [IP15, Got24]; roughly speaking, two distinct errors can have the same effect on a codeword.

uniformly random *subject to* having symplectically orthogonal columns, and the error is drawn from the depolarizing distribution's symplectic representation. Thus, $\mathsf{sympLPN}(k, n, p)$ and $\mathsf{LPN}(k, 2n, p)$ describe essentially the same objects, but draw them from different distributions. Note that formally, the sympLPN and LPN variants we consider are the *decision* variants, wherein one is given $(\mathbf{A}, \mathbf{z})$ and must decide if $\mathbf{z} = \mathbf{A}\mathbf{x} + \mathbf{e}$ ("`structured`") or $\mathbf{z}$ is uniformly random ("`unstructured`"). The *decision* variant of LPN is the standard cryptographic variant, and is essentially equivalent to the *search* variant [FS96, KSS10] (up to small factors). Importantly, we only consider the *search* variant of LSN, as their *search* and *decision* variants appear inequivalent in general [KLP+26] and the *search* variant is natural for quantum information processing. *Search* and *decision* variants of sympLPN are not known to be equivalent.

To achieve the first component in our recipe, we show in Theorem 4.1 that, perhaps surprisingly, there is a simple classical reduction from $\mathsf{LSN}(k, n, p)$ to $\mathsf{sympLPN}(n, n, p)$ for any $k = O(\log n)$. Intuitively, sympLPN appears to be "embedded" in LSN as the $\mathbf{A}$-part of the LSN matrix: sympLPN is of the form $(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{e})$ while LSN takes the form $([\mathbf{A} \,|\, \mathbf{B}], \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y} + \mathbf{e})$. Our reduction relies on the simple observation that the noisy codeword part of LSN is *identical* to that of sympLPN when $\mathbf{y} = \mathbf{0}$. If that is the case, then dropping the $\mathbf{B}$ part of the LSN matrix yields $(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{e})$, precisely the form of Decision sympLPN with a `structured` input. If $\mathbf{y} \neq \mathbf{0}$, then again dropping the $\mathbf{B}$ part of the LSN matrix yields $(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y} + \mathbf{e})$. In fact, we show that $\mathbf{B}\mathbf{y}$ is marginally negligibly close (in total variation distance) to a uniformly random vector, and thus this instance is negligibly close to an `unstructured` sympLPN task. Therefore, a sympLPN solver can decide whether or not $\mathbf{y} = \mathbf{0}$ in the LSN problem. If $\mathbf{y} = \mathbf{0}$ we are done; if $\mathbf{y} \neq \mathbf{0}$, we guess a random $\hat{\mathbf{y}} \in \mathbb{Z}_2^k \setminus \{\mathbf{0}\}$. The sympLPN solver hence gives us a minuscule advantage in solving LSN by providing a larger signal only when $\mathbf{y} = \mathbf{0}$. However, since $k = O(\log n)$, even such a small signal gives a solver with a non-negligible overall advantage over completely random guessing for LSN, which turns out to be sufficient to complete the reduction. Overall, our chain of reductions proceeds as, for $k = O(\log n)$,

$$\mathsf{stateLSN}(k, n, p) \leq_Q \mathsf{LSN}(k, n, p) \leq_C \mathsf{sympLPN}(n, n, p)\,, \tag{2}$$

where $\leq_Q, \leq_C$ respectively denote quantum and classical reductions. Crucially, this reduction works *only* for sympLPN with exactly n logical bits (i.e. rate 1/2). With even *one* less logical bit, it is no longer clear as to how much easier the sympLPN instance becomes.

2.2 Cryptographic Constructions with sympLPN

Having established that (*decision*) sympLPN is at least as hard as stateLSN, we next outline our cryptographic constructions and the technical barriers to a security proof relative to their LPN-based counterparts. Our OWF construction is the most straightforward, and unlike the public-key protocols is based directly on $\mathsf{stateLSN}(k, n, p)$, and in the hardest regime wherein $p = \Omega(1)$ and $k = \Omega(n)$. For simplicity, we here discuss it starting from LSN. The function is indexed by $[\mathbf{A} \,|\, \mathbf{B}]$, and maps on input $(\mathbf{x}, \mathbf{y}, \mathbf{e})$ to $\mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y} + \mathbf{e}$. Inverting this function is equivalent to finding $\mathbf{x}, \mathbf{y}, \mathbf{e}$ from $([\mathbf{A} \,|\, \mathbf{B}], \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y} + \mathbf{e})$, modulo stabilizer equivalence. This is at least as hard as solving $\mathsf{LSN}(k, n, p)$, which only requires finding $\mathbf{y}$. Since the break also recovers $\mathbf{e}$ (up to stabilizer equivalence), we can also use it to solve even harder decoding problems, namely stateLSN. Moreover, in the regime of $p = \Omega(1)$, $\mathsf{LPN}(pn, 2n, p)$ is known to reduce to $\mathsf{stateLSN}(k = O(\log n), n, \Theta(p))$ [KLP+26], and thus our OWF is provably at least as secure as a conventional LPN-based OWF. We defer the full construction and security proof to Appendix B.

On the other hand, the PKE and OT constructions in this work are built upon sympLPN. Our starting point is the LPN-based PKE scheme in [DP12] which is rooted in the seminal scheme of Alekhnovich [Ale03], and which remains the state-of-the-art LPN-based construction in terms of

security and efficiency. This particular scheme uses $p = \Theta(1/\sqrt{n})$, because the correctness of the scheme relies heavily on the inner product of two independently sampled noise vectors being 0 with high probability; this occurs precisely when $p = O(1/\sqrt{n})$. For constant code rate $k/n = R \in (0, 1)$, information-set decoding gives a classical attack with running time $\mathrm{poly}(n)2^{O(pn)}$ in this low-noise regime [Pra62]. For $p = \Theta(1/\sqrt{n})$, this gives an attack running in time $2^{O(\sqrt{n})}$.[2] Much of this construction is readily adaptable to sympLPN in place of LPN, with one very significant barrier. More precisely, in the process of proving the security of our sympLPN-based scheme (formally described in Construction 5.1), we find in Section 5 that the protocol's security reduces to the hardness of both $\mathsf{sympLPN}(n, n, p)$ *and* $\mathsf{sympLPN}(n-1, n, p)$. If this were LPN, this subtlety would be essentially irrelevant—the hardness of LPN provably does not depend on small changes in k. In particular, there is a simple self-reduction from $\mathsf{LPN}(k, n, p)$ to $\mathsf{LPN}(k-1, n, p)$. For sympLPN, however, this subtlety becomes a significant technical barrier. In our case, the security of our adapted PKE scheme would rely on both $\mathsf{sympLPN}(n, n, p)$ and $\mathsf{sympLPN}(n-1, n, p)$. But, as discussed above, a reduction from stateLSN is only known for $\mathsf{sympLPN}(k, n, p)$ with $k = n$ logical bits, exactly half the number of physical bits $2n$. In addition, the naïve self-reduction in which we drop one logical bit, which succeeds on LPN, fails completely on sympLPN because the entries are jointly nearly maximally far from uniformly random. Despite this failure, we find an alternative and substantially more involved approach which successfully reduces $\mathsf{sympLPN}(n, n, p)$ to $\mathsf{sympLPN}(n-1, n, p)$ by introducing new techniques for scrambling isotropic subspaces in a carefully controlled manner. We outline the key idea for these techniques below, but with this reduction complete we prove the (IND-CPA) security of our PKE. Notably, our basic scheme has the same runtime up to small constant factors as state-of-the-art Alekhnovich-type LPN-based PKE, which are quite efficient with $O(n^2)$ time encryption, $O(n)$ time decryption.

Finally, we construct malicious-secure (i.e. even if one party deviates arbitrarily from protocol, the other party's security is still guaranteed) OT from the hardness of $\mathsf{sympLPN}(n, p)$.

We use post-quantum transformations that give constant-round ε-simulation or polynomial-round full simulation. These transformations apply to a particularly structured PKE scheme known as a *strongly uniform* PKE scheme (SU-PKE), via its dense-cryptosystem property [CLPY25, Theorems 12, 13, and 20]. Informally, SU-PKE is the same as PKE with the added property that the public key in the scheme is computationally indistinguishable from a uniformly random bitstring. Since Alekhnovich-type PKE based on $\mathsf{LPN}(k, n, p)$ has public key $(\mathbf{A} \sim \mathbb{Z}_2^{n\times k}, \mathbf{Ax} + \mathbf{e})$ which is by assumption computationally indistinguishable from the uniformly random bitstring $(\mathbf{A} \sim \mathbb{Z}_2^{n\times k}, \mathbf{u} \sim \mathbb{Z}_2^n)$, they yield these OT guarantees under post-quantum hardness. However, our sympLPN-based PKE scheme has a public key which is easily distinguishable from uniformly random because the key takes the form $(\mathbf{A}, \mathbf{Ax} + \mathbf{e})$, where $\mathbf{A} \in \mathbb{Z}_2^{2n\times k}$ is a uniformly random full-rank matrix subject to having symplectically orthogonal columns. As a result, the key technical barrier to the construction of malicious-secure OT via these transformations from sympLPN is the modification of the PKE scheme to have a public key computationally indistinguishable from random. We achieve this modification in Section 6. Our modification begins with a well-known idea that a randomized algorithm sampling from some not-necessarily-uniform distribution can be replaced with a deterministic algorithm which accepts an additional input—a sufficiently long "seed" string $\mathbf{s}$ which is genuinely uniformly random. In our case, the generation of $\mathbf{A}$ can be executed by a deterministic algorithm $\mathcal{A}$ which iteratively builds a basis of the subspace symplectically orthogonal from the columns already sampled, and then picking a random linear combination of these basis vectors to be the next column of $\mathbf{A}$. This linear combination can be chosen with access to $O(n)$ random bits.

[2] The constant-noise LPN construction of [YZ16] admits a $2^{O(\log^2 n)}$ exhaustive-search attack, compared with the $2^{O(\sqrt{n})}$ information-set-decoding bound for Alekhnovich-type schemes.

Thus, we would hope to replace the public key $(\mathbf{A}, \mathbf{Ax}+\mathbf{e})$ with $(\mathbf{s}, \mathbf{Ax}+\mathbf{e})$, where $\mathbf{A}$ is computed from $\mathbf{s}$. This replacement has no impact on correctness, as the encrypting party simply first computes $\mathbf{A}$ from $\mathbf{s}$ using $\mathcal{A}$. However, while this form appears very much hard to distinguish from uniformly random bits ($\mathbf{s}, \mathbf{u} \sim \mathbb{Z}_2^{2n}$), we formally know only that $(\mathbf{A}, \mathbf{Ax}+\mathbf{e})$ is indistinguishable from $(\mathbf{A}, \mathbf{u} \sim \mathbb{Z}_2^{2n})$. Thus, to complete the proof, we must show that given $\mathbf{A}$ we can distributionally "invert" the $\mathbf{s} \mapsto \mathbf{A}$ algorithm to produce a marginally uniformly random $\hat{\mathbf{s}}$ such that $\mathcal{A}(\hat{\mathbf{s}}) = \mathbf{A}$. We give such an inversion algorithm and prove its correctness in Section 6. Thus, $\mathbf{Ax}+\mathbf{e}$ is indistinguishable from random given either $\mathbf{A}$ or $\mathbf{s}$, so $(\mathbf{s}, \mathbf{Ax}+\mathbf{e})$ is indeed computationally indistinguishable from uniformly random bits. We therefore achieve malicious-secure OT and general secure multi-party computation from the hardness of $\mathsf{sympLPN}$, with constant-round ε-simulation or polynomial-round full simulation.

2.3 Removing one logical bit in sympLPN via symplectic scrambling

We here outline our solution to the primary technical barrier to the security proof of $\mathsf{sympLPN}$-based PKE, namely reducing $\mathsf{sympLPN}(n, n, p)$ to $\mathsf{sympLPN}(n-1, n, p)$. If we wished to reduce one logical qubit for $\mathsf{LPN}(k, n, p)$, it would be straightforward: given $(\mathbf{A} \sim \mathbb{Z}_2^{n\times k}, \mathbf{Ax}+\mathbf{e})$, let $\mathbf{A'} \in \mathbb{Z}_2^{n\times(k-1)}$ be $\mathbf{A}$ with the last column removed, and run a $\mathsf{LPN}(k-1, n, p)$ decider on $(\mathbf{A'}, \mathbf{Ax}+\mathbf{e})$. If $x_k = 0$, then $\mathbf{Ax}+\mathbf{e} = \mathbf{A'x'}+\mathbf{e}$, where $\mathbf{x} = [\mathbf{x'} \,|\, x_k]$. Otherwise, $\mathbf{Ax}+\mathbf{e} = \mathbf{A'x'}+\mathbf{e}+\mathbf{a}$, where $\mathbf{a} \sim \mathbb{Z}_2^n$ is the last column of $\mathbf{A}$—so $\mathbf{Ax}+\mathbf{e}$ is uniformly random given $\mathbf{A'}$. Hence, a $\mathsf{LPN}(k-1, n, p)$ decider will output `structured` only when the input is structured with $x_k = 0$, which occurs with large enough probability to obtain a solver for $\mathsf{LPN}(k, n, p)$.

In the case of $\mathsf{sympLPN}(n, n, p)$, however, an analogous technique fails completely. Given $(\mathbf{A} \in \mathbb{Z}_2^{2n\times n}, \mathbf{Ax}+\mathbf{e})$, we might again try to remove the last column of $\mathbf{A}$ to obtain $\mathbf{A'}$. If $x_n = 0$, then indeed $\mathbf{Ax}+\mathbf{e} = \mathbf{A'x'}+\mathbf{e}$ is a $\mathsf{sympLPN}(n-1, n, p)$ structured instance. However, if $x_n = 1$, then $\mathbf{Ax}+\mathbf{e} = \mathbf{A'x'}+\mathbf{e}+\mathbf{a}$, but this time the last column $\mathbf{a} \in \mathbb{Z}_2^{2n}$ of $\mathbf{A}$ has a complicated distribution which depends sensitively on the rest of $\mathbf{A}$. In other words, $\mathbf{a}$ is nearly maximally far from uniformly random given $\mathbf{A'}$, so the instance is not at all close to unstructured. Consequently, we have no guarantees on the accuracy of a $\mathsf{sympLPN}(n-1, n, p)$ decider on this input.

To overcome this barrier, we introduce four techniques which approach the reduction in a completely different way and thereby bypass the above obstruction. Our first technique arises from the observation that the maximal dimension of a subspace of $\mathbb{Z}_2^{2n}$ in which all vectors are symplectically orthogonal is n. Thus, a useful geometric interpretation of a $(n-1)$-dimensional symplectically orthogonal subspace—the image of the matrix $\mathbf{A'} \in \mathbb{Z}_2^{2n\times(n-1)}$ in a $\mathsf{sympLPN}(n-1, n, p)$ instance—is as a hyperplane of codimension 1 within some maximal n-dimensional symplectically orthogonal subspace, symplectically orthogonal to some random vector $\mathbf{v} \in \mathbb{Z}_2^{2n}$. (Technically, there are many possible maximal subspaces which contain this hyperplane, but we ignore this subtlety in this overview.) Given a $2n \times n$ matrix $\mathbf{A}$ in a $\mathsf{sympLPN}(n, n, p)$ instance, our first step is to reduce the dimensionality by 1 by forcing all vectors in the code to be symplectically orthogonal to some fixed $\mathbf{v}$—this step effectively removes a logical bit. This is easy to do if the first entry of the error $\mathbf{e}$ is 0: we can then easily transform the code space to always have first entry 0. Equivalently, the code is symplectically orthogonal to the vector $(0^n, 1, 0^{n-1})$. However, a $\mathsf{sympLPN}(n-1, n, p)$ instance has a code orthogonal to a *random* vector $\mathbf{v}$, not a fixed one. Thus, our next step is to design a very sparse random operator $\mathbf{C} \in \mathbb{Z}_2^{2n\times 2n}$ which "rotates" this orthogonal vector to a random vector, taking its normal hyperplane along with it. We multiply to produce $(\mathbf{CA}, \mathbf{CAx}+\mathbf{Ce})$. Since $\mathbf{C}$ is very sparse, the new error $\mathbf{Ce}$ is not irrecoverably blown up, but does have a complicated distribution far from depolarizing. Hence, our third technique is to apply a "noise symmetrization" operation which, using a combination of noise flooding, starting on a fixed set of pairs, and permutations,

maps $\mathbf{Ce}$ to a depolarizing error with only slightly larger noise rate p' than p, while not affecting the distribution of the other objects. This technique turns out, however, to only work when the $(n+1)$th component of $\mathbf{e}$ is 0.

In summary, our approach only works when entries 1 and $n+1$ of $\mathbf{e}$ are 0, which does not occur with overwhelming probability. So, to complete the reduction, our final technique is an "interpolation trick". This trick arises from the observation that we are free to add extra noise prior to the start of the reduction if we wish, which will change the probabilities of the reduction's success. A simple analysis of these probabilities reveals that the two reductions—one with and one without the preliminary noise flooding—cannot both fail, and thus there must exist a successful reduction from $\mathsf{sympLPN}(n, n, p)$ to $\mathsf{sympLPN}(n-1, n, p')$ for p' only slightly larger than p.

This reduction completes the security proof of our sympLPN-based PKE scheme. Given the many technical obstructions which arise in performing even the simplest sympLPN self-reduction, it is somewhat surprising that a rigorous security proof of sympLPN-based PKE scheme is possible at all.

2.4 Comparative Hardness of LPN and sympLPN

The fact that sympLPN readily implies all of the core primitives of Cryptomania with LPN-level efficiency gives a compelling reason to consider sympLPN as an independent post-quantum assumption, provided that sympLPN *is not already equivalent or reducible to* LPN.

Prior work has shown a reduction from $\mathsf{LPN}(pn, 2n, p)$ to $\mathsf{sympLPN}(n, n, 6p)$ [KLP+26]. With $p = O(1/\sqrt{n})$, however, this reduction becomes vacuous, as $\mathsf{LPN}(\sqrt{n}, 2n, 1/\sqrt{n})$ can be solved in polynomial time by restricting to the first $\sqrt{n} \times \sqrt{n}$ minor of $\mathbf{A}$ (where an error rate of $1/\sqrt{n}$ implies that there typically only $O(1)$ errors on this block) and brute-force enumerating constant-weight errors. It is therefore not known if LPN reduces to sympLPN in this low-noise regime, or if in fact sympLPN reduces to LPN. The former reduction would establish sympLPN as being at least as good as LPN for cryptography in light of this work, while the latter reduction would prove that sympLPN adds no value for post-quantum security. While we leave the former open, we prove in Appendix D a strong barrier against the existence of a sympLPN-to-LPN reduction, suggesting that the assumptions are *inequivalent*.

The most natural approach to a reduction would be to, given $(\mathbf{A} \in \mathbb{Z}_2^{2n \times n}, \mathbf{Ax} + \mathbf{e})$, simply remove around $n/2$ rows of $\mathbf{A}$. After all, $\mathbf{A}$ has $2n^2$ entries but only has entropy $\sim \frac{3}{2}n^2$ since there are $\binom{n}{2} \sim \frac{1}{2}n^2$ constraints. More generally, we may wish to multiply $\mathbf{A}$ and $\mathbf{Ax}+\mathbf{e}$ by some $\mathbf{B} \in \mathbb{Z}_2^{m \times 2n}$, producing $(\mathbf{BA}, (\mathbf{BA})\mathbf{x} + \mathbf{Be})$, and hope that this instance is close to a $\mathsf{LPN}(n, m, p')$ instance for some p'. It is not at all clear as to why such a strategy would not work, especially because intuition from the leftover hash lemma [ILL89] suggests that it in fact may succeed. Moreover, such a "linear reduction" was used, for example, to successfully produce the first non-trivial random self-reduction for LPN from polylog-weight errors in the worst case to error rate $1/2 - 1/\operatorname{poly}(n)$ in the average case [BLVW19]. We prove, however, that linear reductions *cannot* reduce sympLPN to LPN. While the proof is quite technical, the central idea is simple. We show that for any *fixed* $\mathbf{B} \in \mathbb{Z}_2^{m \times 2n}$, the random matrix $\mathbf{BA} \in \mathbb{Z}_2^{m \times n}$ is severely deficient in entropy. That is, while $\mathbf{BA}$ must have entropy about mn to be uniformly random (and thus a LPN matrix), it actually only has entropy at most $(1-d)mn$ for some constant d. To compensate this deficiency, we must choose $\mathbf{B}$ from a sufficiently high-entropy distribution. Using this result, we then prove that any distribution over $\mathbf{B}$ which adds enough entropy so as to randomize $\mathbf{BA}$ also irrecoverably blows up the error. More precisely, in the codeword $(\mathbf{BA})\mathbf{x} + \mathbf{Be}$ part of the input, the error $\mathbf{Be}$ has expected weight at least $\frac{(1-r-\delta)}{2}m$ for any $\delta > 0$ with overwhelming probability over $\mathbf{B}$, where r is the rate $r = \frac{n}{m}$. At constant rate, adding fresh noise to make the errors independent leaves their rate above Shannon's decoding threshold.

Our barrier does not imply that no reduction exists, but it shows that the most clearly motivated

approach faces a noise barrier. A reduction following this approach would have to overcome this barrier, and it is possible that if such a reduction exists, it could also improve the random self-reductions achievable for LPN. (The current linear reduction—from worst case with polylog-weight to average case with noise rate $1/2 - 1/\operatorname{poly}(n)$—has very weak parameters, with the primary barrier to improvement being the same issue that we rigorously derive here.)

2.5 Cryptanalysis

Given the close relationship between sympLPN and LPN, a natural question is how the security of our sympLPN-based schemes compares to that of standard LPN-based schemes in practice. We focus on our PKE scheme in Construction 5.1, as our OWF construction may assume the hardest variant of LSN, which is already known to be at least as hard as LPN in most relevant parameter regimes [KLP+26].

As pointed out in [CDMT24], the dominant class of attacks against LPN are information-set decoding (ISD) algorithms, originating in the work of Prange and Stern [Pra62, Ste88]. These attacks are combinatorial: they exploit the sparsity of the error vector and are largely agnostic to the algebraic structure of the underlying code. Their running time scales exponentially in the block length, with the exponent governed by the particular noise rate. Because of this structural insensitivity, we expect ISD-type attacks to serve as the primary *generic* benchmark for sympLPN-based PKE.

To enable a meaningful comparison, it is important to place the two schemes on equal footing; for example, standard practice [DP12] suggests matching parameters by fixing the decryption success probability to be 0.75. Since sympLPN employs depolarizing noise whereas LPN uses Bernoulli noise, we can compare our decryption analysis with that of LPN-based schemes [DP12] and equate the corresponding decryption success probabilities: if p and q denote the noise rates in $\mathsf{sympLPN}(n, p)$ and $\mathsf{LPN}(n, 2n, q)$, respectively, this matching yields

$$1 - \frac{4}{3}p^2 = (1 - 2q^2)^2, \qquad \text{and hence} \qquad p = \sqrt{3(q^2 - q^4)} = \sqrt{3}\, q - O(q^2). \tag{3}$$

In particular, for the same decryption probability, say 0.75, the sympLPN distribution produces errors of slightly larger expected weight (by a constant factor) than the corresponding LPN instance.

From the perspective of ISD, this has two competing effects. On the one hand, since ISD algorithms are driven primarily by the sparsity of the error vector, the increased error weight suggests that *naïve* ISD attacks should perform somewhat worse against sympLPN than against LPN. On the other hand, the depolarizing noise in sympLPN exhibits a mild pairwise correlation structure, which induces a small entropy loss relative to fully independent noise. Naturally, this structure can be exploited by a simple *pair-aware* variant of ISD—e.g., modifications of Prange's original algorithm [Pra62]—in which coordinates are processed in pairs $(j, n + j)$ rather than independently. Taken together, these considerations suggest that while off-the-shelf ISD attacks may underestimate the vulnerability of sympLPN, tailored ISD variants should provide an accurate point of comparison, and are expected to achieve performance comparable to that observed for LPN-based PKE. This heuristic is consistent with our preliminary numerical investigations.

Our results so far suggest a qualitative message: sympLPN-based PKE schemes are likely to be similarly susceptible to brute-force ISD-attacks as comparable LPN-based schemes—even if the security of sympLPN may ultimately hinge on the symplectic structure of the underlying code and its interaction with the noise model. This is because ISD's brute-force approach has little dependence on the actual code distribution itself, and therefore does not distinguish between the random matrices in LPN and the random symplectically orthogonal matrices in sympLPN. Rather, as discussed above, ISD depends more sensitively on the noise distribution. We thus believe that, for practical purposes,

alternative noise distributions (possibly deviating from our quantum-inspired depolarizing model) could further amplify the security of the scheme. Exploring such directions, as well as refining the analysis of tailored attacks, remains an interesting avenue for future work.

2.6 Outlook

This paper shows that private-key encryption, public-key encryption, and secure multi-party computation can be constructed entirely from the average-case hardness of decoding quantum stabilizer codes, $\mathsf{stateLSN}(k, n, p)$. In the private-key regime, we construct one-way functions from high-rate ($\Omega(1)$), high-noise ($\Omega(1)$) $\mathsf{stateLSN}$. In the public-key regime, we construct PKE and malicious-secure OT (which then implies malicious-secure multi-party computation) from low-rate ($O(\frac{\log n}{n})$), low-noise ($\Theta(1/\sqrt{n})$) $\mathsf{stateLSN}$, for which known generic decoding algorithms run in time $2^{\widetilde{O}(\sqrt{n})}$. The security of $\mathsf{stateLSN}$ does not appear to depend on the rate of the code at all [KLP+26], and the known generic decoding bounds in the low-noise regime have the same $2^{\widetilde{O}(\sqrt{n})}$ form as those for low-noise LPN-based PKE schemes.

From the construction point of view, a pertinent question is whether public-key encryption can be built directly out of high-rate, low-noise $\mathsf{stateLSN}$. Our approach has been to first quantumly reduce $\mathsf{stateLSN}(k, n, p)$ with $k = O(\log n)$ logical qubits to a classical problem, $\mathsf{sympLPN}(n, n, p)$, and then construct public-key cryptography from $\mathsf{sympLPN}(n, n, p)$. Whether or not either an improved reduction with larger k, or a more direct construction from $\mathsf{stateLSN}$, remains open. A further open constructive avenue is security in different models. For example, OT secure in the *universal composability* model can be constructed from the hardness of LPN [DDN14]; can an analogous construction be made from the hardness of $\mathsf{sympLPN}$?

A second question concerns improving our understanding of the comparative security between $\mathsf{sympLPN}(n, n, p)$ and $\mathsf{LPN}(k, n', p')$, when $p = O(1/\sqrt{n})$, and thereby understanding how $\mathsf{sympLPN}$ stands as a post-quantum security assumption relative to LPN. Is there a reduction from LPN to $\mathsf{sympLPN}$ in this regime, and is there *no* reduction in the opposite direction? In this work, we have shown significant barriers towards the possibility of a converse reduction—from $\mathsf{sympLPN}$ to LPN (which would nullify the motivation to build cryptography from $\mathsf{sympLPN}$)—but a more rigorous proof that no reduction exists would substantially strengthen our hope that $\mathsf{sympLPN}$ may remain secure even in a world where LPN is broken. More generally, understanding precisely how symplectic structure affects the complexity of decoding remains a key open question.

3 Preliminaries

A comprehensive introduction to quantum computation can be found in [NC10]. For a detailed introduction to quantum error correction, we refer to [Got24].

Computational model. Unless stated otherwise, hardness and computational security are defined against non-uniform quantum polynomial-time (QPT) adversaries. Such an adversary is a family of quantum circuits of size $\mathrm{poly}(n)$ supplied with an advice state on $\mathrm{poly}(n)$ qubits; the circuit and advice may depend on n but not on the freshly sampled problem instance. Computational indistinguishability is understood against the same class of distinguishers.

Pauli matrices. The four 2×2 *Pauli matrices* are denoted as

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4}$$

The phase-free Pauli group $\mathcal{P}_n$ is the group of n-qubit Pauli operators $\{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}^{\otimes n}$ which multiply modulo phase. Any such n-qubit Pauli can be represented in so-called *symplectic form*, via a map

$$\mathrm{Symp} : \mathcal{P}_n \to \mathbb{Z}_2^{2n}. \tag{5}$$

Here, bits j and $j+n$ in $\mathrm{Symp}(\mathbf{P})$ indicate which Pauli is on the jth qubit of $\mathbf{P} \in \mathcal{P}_n$. The two bits are $(0,1)$ if $\mathbf{X}$, $(1,0)$ if $\mathbf{Z}$, $(1,1)$ if $\mathbf{Y}$, and $(0,0)$ if $\mathbf{I}$. Since $\mathbf{XY} = i\mathbf{Z}$, $\mathbf{YZ} = i\mathbf{X}$, and $\mathbf{ZX} = i\mathbf{Y}$, this representation shows that

$$\mathrm{Symp}(\mathbf{P}_1\mathbf{P}_2) = \mathrm{Symp}(\mathbf{P}_1) + \mathrm{Symp}(\mathbf{P}_2) \tag{6}$$

and thus that Symp is an isomorphism (with arithmetic mod 2). The symplectic representation is equipped with a natural inner product given by

$$(\mathbf{a}_1, \mathbf{b}_1) \odot (\mathbf{a}_2, \mathbf{b}_2) := \mathbf{a}_1 \cdot \mathbf{b}_2 + \mathbf{a}_2 \cdot \mathbf{b}_1 \pmod 2, \tag{7}$$

where $\cdot$ denotes the standard dot product. Two phase-free Paulis commute if and only if their symplectic representations have zero symplectic inner product. We say that such vectors are symplectically orthogonal. The standard symplectic basis is given by $\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{f}_1, \ldots, \mathbf{f}_n$, where $\mathbf{e}_i$ is 1 on the ith entry and 0 elsewhere, and $\mathbf{f}_i$ is 1 on the $(i+n)$th entry and zero elsewhere. Note that

$$\mathbf{e}_i \odot \mathbf{e}_j = \mathbf{f}_i \odot \mathbf{f}_j = 0, \quad \mathbf{e}_i \odot \mathbf{f}_j = \delta_{ij}. \tag{8}$$

Quantum stabilizer codes. Letting $\mathrm{U}(2^n)$ denote the unitary group on n qubits, we define the Clifford group $\mathcal{C}_n$ as the set of unitaries which leave the Pauli group invariant under conjugation:

$$\mathcal{C}_n := \{\, \mathbf{C} \in \mathrm{U}(2^n) \mid \mathbf{CPC}^\dagger \in \mathcal{P}_n, \forall\, \mathbf{P} \in \mathcal{P}_n \,\}. \tag{9}$$

An $[\![n, k]\!]$ quantum stabilizer code is the simultaneous $+1$ eigenspace of $n-k$ independent commuting n-qubit Pauli operators. Such a code can be succinctly specified by a Clifford operator $\mathbf{C}$ (e.g., in the form of a quantum circuit) as well as a choice of logical dimension k. In this case, the code space is given by $\mathbf{C}(|0^{n-k}\rangle \otimes |\psi\rangle)$, where $|\psi\rangle \in (\mathbb{C}^2)^{\otimes k}$ is any k-qubit logical state. The stabilizers of the subspace of states $|0^{n-k}\rangle \otimes |\psi\rangle$ are $\mathbf{Z}_1, \ldots, \mathbf{Z}_{n-k}$—hence, $\mathbf{CZ}_1\mathbf{C}^\dagger, \ldots \mathbf{CZ}_{n-k}\mathbf{C}^\dagger$ are stabilizers for code-vectors $\mathbf{C}(|0^{n-k}\rangle \otimes |\psi\rangle)$. A random quantum stabilizer code can be generated by using a uniformly random Clifford operator $\mathbf{C} \sim \mathcal{C}_n$ as the encoding map [PQS26, vdB21].

If we ignore phases, a Clifford is defined entirely on how it acts (via conjugation) on the $2n$ Paulis $\mathbf{X}_1, \ldots, \mathbf{X}_n, \mathbf{Z}_1, \ldots, \mathbf{Z}_n$. Thus, a Clifford modulo phases on Paulis can be represented as a matrix in $\mathbb{Z}_2^{2n\times 2n}$. Since conjugation by a Clifford does not affect the commutation relation of two Pauli operators, the symplectic representation of Cliffords preserves the symplectic inner product. That is, $(\mathbf{Cv}) \odot (\mathbf{Cw}) = \mathbf{v} \odot \mathbf{w}$ for all $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^{2n}$ if and only if $\mathbf{C} \in \mathbb{Z}_2^{2n\times 2n}$ represents a Clifford operation. These matrices are referred to as symplectic matrices. For a Clifford $\mathbf{C}$, we often abuse notation by referring to its matrix representation as $\mathbf{C}$ as well, instead of $\mathrm{Symp}(\mathbf{C})$.

Symplectic linear algebra. Given a subspace $S \subseteq \mathbb{Z}_2^{2n}$, we denote its *symplectic dual* or *symplectic orthogonal complement* by

$$S^\perp := \{\, \mathbf{v} \in \mathbb{Z}_2^{2n} \mid \mathbf{v} \odot \mathbf{w} = 0, \ \forall \mathbf{w} \in S \,\}. \tag{10}$$

Note that $\dim S + \dim S^\perp = 2n$ even though $S^\perp \cap S$ is not necessarily trivial.

Definition 3.1 (Isotropic subspaces and matrices)**.** We say that a subspace S of $\mathbb{Z}_2^{2n}$ is *isotropic* if every pair of points in S is symplectically orthogonal, i.e., $S \subseteq S^\perp$. Note that the maximum dimension of an isotropic subspace is n. A matrix is isotropic if its image is an isotropic subspace. Equivalently, a matrix is isotropic if its columns are pairwise symplectically orthogonal.

We remark that an equivalent characterization of an isotropic matrix $\mathbf{M} = \begin{bmatrix}\mathbf{M}_1 \\ \mathbf{M}_2\end{bmatrix}$ is that $\mathbf{M}_2^\intercal \mathbf{M}_1 + \mathbf{M}_1^\intercal \mathbf{M}_2 = 0$. In other words, $\mathbf{M}$ is isotropic if and only if $\mathbf{M}_1^\intercal \mathbf{M}_2$ is symmetric.

Quantum and classical noise models. The n-qubit depolarizing noise distribution with error parameter $p \in (0,1)$ is denoted as $\mathcal{D}_p^{\otimes n}$. This distribution independently draws a Pauli error on each qubit according to a distribution $\mathcal{D}_p$; namely, with probability $1-p$, no error occurs, otherwise, with probability p, a uniformly random Pauli $\{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$ is drawn and applied. Note that $\mathcal{D}_{3/4}$ coincides with a uniformly random pair of bits. In slight abuse of notation, we frequently use the same notation in the symplectic representation: we use $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$ as shorthand notation for first sampling a Pauli operator $\mathbf{E} \sim \mathcal{D}_p^{\otimes n}$ and letting $\mathbf{e} = \mathrm{Symp}(\mathbf{E})$. The resulting error vector $\mathbf{e}$ has length $2n$, with each pair (e_i, e_{i+n}) drawn independently; Each such pair is $(0,0)$ with probability $1-p$, and the other 3 possibilities each with probability $p/3$. By contrast, a vector $\mathbf{e} \sim \mathsf{Ber}_p^{\otimes n}$ has length n, with each bit being 1 independently with probability p, and 0 otherwise. For a bitstring $\mathbf{v} \in \mathbb{Z}_2^d$, let $w_H(\mathbf{v}) := |\{i \in [d] : v_i \neq 0\}|$ be its Hamming weight. For $\mathbf{e} \in \mathbb{Z}_2^{2n}$, let $w_P(\mathbf{e}) := |\{i \in [n] : (e_i, e_{i+n}) \neq (0,0)\}|$ be its Pauli weight. Then $w_P(\mathbf{e}) \leq w_H(\mathbf{e}) \leq 2w_P(\mathbf{e})$. We write $|\mathbf{v}| = w_H(\mathbf{v})$ for bitstrings.

Haar measure over states. To generate a random logical state $\mathbf{x} \in \mathbb{Z}_2^k$, say of a classical linear code, it suffices to choose $\mathbf{x}$ uniformly at random. Quantumly, one way to analogously generate a random logical state is to choose a uniformly random k-qubit state. The notion of a uniformly random state is given by the Haar measure (see [Mel24]), formally defined for the unitary group.

Definition 3.2 (Haar measure)**.** The Haar measure μ over the group of $d \times d$ unitary matrices $\mathrm{U}(d)$ is the unique probability measure which is invariant under translation. That is, for all $\mathbf{V} \in \mathrm{U}(d)$ and integrable functions f,

$$\int f(\mathbf{VU})\, d\mu(\mathbf{U}) = \int f(\mathbf{U})\, d\mu(\mathbf{U}) = \int f(\mathbf{UV})\, d\mu(\mathbf{U}). \tag{11}$$

We refer to a *Haar-random state* $|\psi\rangle \sim \mu_k$ to be a state constructed by sampling $\mathbf{U} \sim \mu$ a unitary drawn from the Haar measure over $\mathrm{U}(2^k)$ and then letting $|\psi\rangle = \mathbf{U}|0^k\rangle$.

3.1 Learning Stabilizers with Noise

The problem of decoding a random quantum error-correcting code, is known as *Learning Stabilizers with Noise* [PQS26]—the quantum analog of *Learning Parity with Noise* (LPN) which we stated in its *decision* variant: decide whether its input is a true noisy codeword or simply a uniformly random bitstring, as opposed to decoding a given noisy codeword (for a formal definition, see Appendix A).

For *Learning Stabilizers with Noise*, there are two variants which we will discuss, termed stateLSN and LSN. Both computational problems characterize the hardness of decoding an encoded quantum state, where the stabilizer code is sampled uniformly at random, the starting logical state is sampled from a specified distribution, and a random depolarizing error is applied to the state. In stateLSN, the logical state is a Haar-random pure state: the problem serves as a natural model for average-case quantum stabilizer decoding. Meanwhile, for LSN, the logical state is chosen as a uniformly random

computational basis state. Because LSN restricts itself to encoding simpler states, it is easier to characterize. In particular, it is shown in [KLP+26] that LSN is (quantumly) equivalent to a classical computational task. Below, we define stateLSN, and then LSN in its equivalent classical form. We note that in [KLP+26], various forms of these two problems are discussed, including a Decision version and a variant with more than one sample. The definitions provided here coincide with Search stateLSN and Search LSN with just one sample.

Definition 3.3 (Learning Stabilizers with Noise, state variant stateLSN)**.** The state variant of the Learning Stabilizers with Noise problem, denoted by $\mathsf{stateLSN}(k, n, p)$, is characterized by integers $k, n \in \mathbb{N}$ with $1 \leq k \leq n$ and $p \in (0, 1)$. Both p and k can vary with n. Given as input a sample of the form

$$(\mathbf{C},\ \mathbf{EC}\,|0^{n-k}, \psi\rangle), \tag{12}$$

where $\mathbf{C} \sim \mathcal{C}_n$ is a uniformly random n-qubit Clifford operator (admitting a classical description via, e.g., a circuit), $\mathbf{E} \sim \mathcal{D}_p^{\otimes n}$ is an n-qubit Pauli sampled from a depolarizing distribution with parameter p, and $|\psi\rangle \sim \mu_k$ is a Haar random k-qubit state, the task is to output a quantum state ρ_ψ within average fidelity at least $\frac{1}{2^k} + \frac{1}{\mathrm{poly}(n)}$ of $|\psi\rangle$ over the choice of $|\psi\rangle \sim \mu_k$; that is,

$$\mathop{\mathbb{E}}_{|\psi\rangle\sim\mu_k} [\langle\psi|\rho_\psi|\psi\rangle] \geq \frac{1}{2^k} + \frac{1}{\mathrm{poly}(n)}. \tag{13}$$

Here ρ_ψ denotes the decoder's output state, averaged over $\mathbf{C}$, $\mathbf{E}$, and the decoder's internal randomness and measurement outcomes for fixed $|\psi\rangle$.

Next, we formally define the classical formulation of the LSN problem.

Definition 3.4 (Learning Stabilizers with Noise, classical representation)**.** $\mathsf{LSN}(k, n, p)$, is characterized by integers $k, n \in \mathbb{N}$ with $1 \leq k \leq n$ and $p \in (0, 1)$. Here, the input is

$$\left(\left[\mathbf{A}\,|\,\mathbf{B}\right],\ \left[\mathbf{A}\,|\,\mathbf{B}\right] \cdot \begin{bmatrix} \mathbf{r} \\ \mathbf{y} \end{bmatrix} + \mathbf{e} \right) \tag{14}$$

where $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$ and $\mathbf{B} \in \mathbb{Z}_2^{2n\times k}$ are sampled jointly and uniformly subject to the constraint that $\mathbf{A}$ and $\mathbf{B}$ are isotropic and that $\left[\mathbf{A}\,|\,\mathbf{B}\right]$ is full-rank; where $\mathbf{r} \sim \mathbb{Z}_2^n$ and $\mathbf{y} \sim \mathbb{Z}_2^k$ are uniformly random, and where $\mathbf{e} \in \mathbb{Z}_2^{2n}$ is a depolarizing error with parameter p, i.e. $\mathrm{Symp}^{-1}(\mathbf{e}) \sim \mathcal{D}_p^{\otimes n}$ (for brevity, we sometimes write $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$ instead). The task is to output $\mathbf{y}$ with probability at least $1/2^k + 1/\mathrm{poly}(n)$.

$\mathsf{stateLSN}(k, n, p)$ is always at least as hard as $\mathsf{LSN}(k, n, p)$, and in fact the two problems are equivalent when $k = O(\log n)$. These reductions are necessarily quantum, as the input and output of stateLSN include quantum states.

Theorem 3.5 (stateLSN versus LSN, [KLP+26])**.** *Let $k, n, \in \mathbb{N}$ and $p \in (0, 1)$ such that $k = O(\log n)$. Then there exist efficient quantum reductions from $\mathsf{LSN}(k, n, p)$ to $\mathsf{stateLSN}(k, n, p)$ and from $\mathsf{stateLSN}(k, n, p)$ to $\mathsf{LSN}(k, n, p)$.*

The problem of $\mathsf{stateLSN}(k, n, p)$ (or, equivalently, $\mathsf{LSN}(k, n, p)$) with $k = O(\log n)$ will be the basis for the hardness of the encryption and oblivious transfer schemes that we present. However, it is challenging to work directly with these problems because of their complicated setup. As a result, we will instead define a simpler problem which bears a closer resemblance to LPN. In the

next section, we will prove that in fact LSN with $k = O(\log n)$ logical qubits reduces to this simpler problem, so that in combination with Theorem 3.5, our schemes are secured solely by the hardness of $\mathsf{stateLSN}(k = O(\log n), n, p)$. For binary distinguishing tasks, advantage means $|\Pr[\hat{b} = b] - 1/2|$, where b is a uniform bit selecting the input distribution and $\hat{b}$ is the distinguisher's guess.

Definition 3.6 (Decision $\mathsf{sympLPN}$)**.** Let $n, k \in \mathbb{N}$ with $1 \leq k \leq n$ and $p \in (0, 1)$ be parameters. Then, $\mathsf{sympLPN}(k, n, p)$ is the task of distinguishing with advantage at least $1/\operatorname{poly}(n)$ between

$$(\mathbf{A},\ \mathbf{A}\mathbf{x} + \mathbf{e}) \quad \text{or} \quad (\mathbf{A},\ \mathbf{u} \sim \mathbb{Z}_2^{2n}) \tag{15}$$

where $\mathbf{A} \in \mathbb{Z}_2^{2n \times k}$ is a uniformly random full-rank isotropic matrix, and where $\mathbf{e}$ is a depolarizing error with probability parameter p, i.e. $\mathrm{Symp}^{-1}(\mathbf{e}) \sim \mathcal{D}_p^{\otimes n}$ (for brevity, we often write $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$). Here $\mathbf{x} \sim \mathbb{Z}_2^k$ is uniformly random. The former case is called *structured* and the latter called *unstructured*. For convenience, we denote $\mathsf{sympLPN}(n, n, p)$, a parameter regime of particular relevance, as $\mathsf{sympLPN}(n, p)$.

If $\mathbf{A}$ was instead chosen to be a uniformly random matrix, then the above problem would resemble Decision LPN. A random $2n \times k$ matrix is full-rank with at least constant probability, so the isotropy condition is the fundamental difference between LPN and $\mathsf{sympLPN}$. $\mathsf{sympLPN}$ was first defined in [KLP+26] as a tool for reducing LPN to LSN—[KLP+26] demonstrates that for any regime of k, $\mathsf{sympLPN}(n, p)$ reduces to $\mathsf{LSN}(k, n, p)$, and moreover that there is a reduction from LPN to $\mathsf{sympLPN}$ for certain choices of p, namely $p = \omega(n^{-1/2})$.

4 Hardness of sympLPN

We will construct our public-key cryptographic protocols directly from $\mathsf{sympLPN}(n, p)$ for certain p. As a consequence, our first result is a reduction from $\mathsf{stateLSN}$ with very few logical qubits to $\mathsf{sympLPN}$. Therefore, cryptography built on the hardness of $\mathsf{sympLPN}$ source their security from the hardness of decoding random quantum stabilizer codes with Haar-random logical states with logarithmically many qubits. Classically, there is a polynomial time algorithm which solves $\mathsf{LPN}(k, n, p)$ when $k = O(\log n)$ by brute force. However, quantumly, there is substantial evidence that $\mathsf{LSN}(k, n, p)$ is exponentially hard (in n) at constant noise rates *for any* $k \geq 1$ [KLP+26], intuitively because there is no known efficient way to verify proposed solutions for any k so a natural brute-force approach is to enumerate possible errors rather than logical states. Therefore, the fact that $k = O(\log n)$ in our codes does not imply that security is lost.

Our public-key encryption will, however, rely on the hardness of both $\mathsf{sympLPN}(n, n, p) = \mathsf{sympLPN}(n, p)$ and $\mathsf{sympLPN}(n - 1, n, p)$. A reduction from $\mathsf{LPN}(k, n, p)$ to $\mathsf{LPN}(k - 1, n, p)$ is trivial for LPN, but is surprisingly challenging for $\mathsf{sympLPN}$. Nonetheless, we will then show how to give such a reduction by introducing some new analytical techniques for isotropic subspaces. As a consequence, the public-key encryption scheme will only rely on the hardness of $\mathsf{sympLPN}(n, p)$, as desired.

4.1 Reducing LSN for very few logical qubits to sympLPN

Since $\mathsf{stateLSN}$ and LSN are equivalent for $k = O(\log n)$ (see Theorem 3.5), we here reduce $\mathsf{LSN}(k, n, p)$ to $\mathsf{sympLPN}(n, p)$.

Theorem 4.1 (LSN reduces to $\mathsf{sympLPN}$)**.** *Let $k, n \in \mathbb{N}$ such that $k = O(\log n)$ and let $p \in (0, 1)$. Suppose $\mathcal{O}$ is an oracle which solves $\mathsf{sympLPN}(n, p)$. Then there exists a polynomial time algorithm which solves $\mathsf{LSN}(k, n, p)$, using a single call to $\mathcal{O}$.*

Proof. Let $(\mathbf{A}, \mathbf{B}, \mathbf{z})$ be an instance of LSN, where $\mathbf{z} = \mathbf{A}\mathbf{r} + \mathbf{B}\mathbf{y} + \mathbf{e}$. The algorithm queries the oracle $\mathcal{O}$ with input $(\mathbf{A}, \mathbf{z})$. If the oracle outputs `structured`, then return $\mathbf{y} = \mathbf{0}$, while if the oracle outputs `unstructured`, return a uniformly random value of $\mathbf{y} \in \{0,1\}^k \backslash \{\mathbf{0}\}$.

We analyze this algorithm in two cases: either $\mathbf{y} = \mathbf{0}$ or $\mathbf{y} \neq \mathbf{0}$. If $\mathbf{y} = \mathbf{0}$, then $(\mathbf{A}, \mathbf{z}) = (\mathbf{A}, \mathbf{A}\mathbf{r} + \mathbf{e})$ is precisely a structured instance of $\mathsf{sympLPN}$, since marginally $\mathbf{A}$ is a uniformly random full-rank isotropic matrix. Now, say that $\mathbf{y} \neq 0$. We can assume without loss of generality that $\mathbf{y} = (1, 0, \ldots, 0)^\intercal$. Indeed, for any given $W = \operatorname{im} \mathbf{B}$, each nonzero vector in W is equally likely to be the first column of $\mathbf{B}$, $\mathbf{B}\mathbf{y}$. The distribution of $\mathbf{B}\mathbf{y}$ for $\mathbf{y} = (1, 0, \ldots, 0)^\intercal$ and $\mathbf{B}\mathbf{y}$ for uniformly random nonzero $\mathbf{y}$ are both just a uniformly random nonzero vector in W.

Now, observe that the first column of $\mathbf{B}$ is equally likely to be any vector in $\mathbb{Z}_2^{2n} \backslash V$, where $V = \operatorname{im} \mathbf{A}$. For example, $\mathbf{B}$ may be sampled column by column by sampling a new vector linearly independent from $\mathbf{A}$ and symplectically orthogonal to the previous columns of $\mathbf{B}$, giving the first column this simple form. Thus in the $\mathbf{y} \neq \mathbf{0}$ case, $\mathbf{z} \sim (\mathbf{A}\mathbf{r} + \mathbf{e}) + \mathbf{b}_1$, where $\mathbf{b}_1$ is the first column of $\mathbf{B}$, uniformly random over $\mathbb{Z}_2^{2n} \setminus V$, and $\frac{|V|}{2^{2n}} = 2^{-n}$. Consequently, $\mathbf{b}_1$ has total variation distance 2^{-n} from that of uniformly random, using the fact that the TV distance between uniform distributions over sets S and $T \subseteq S$ is $1 - \frac{|T|}{|S|}$. Hence, the total variation distance between $(\mathbf{A}, \mathbf{z})$ and $(\mathbf{A}, \mathbf{u})$, where $\mathbf{u}$ is uniformly random, is also $O(2^{-n}) = \operatorname{negl}(n)$. In summary, therefore, if $\mathbf{y} = \mathbf{0}$, then the oracle $\mathcal{O}$ is given a sample from the `structured` distribution of $\mathsf{sympLPN}(n, p)$; if $\mathbf{y} \neq \mathbf{0}$, then $\mathcal{O}$ is given a sample drawn from a distribution within $\operatorname{negl}(n)$ TV distance from the `unstructured` distribution of $\mathsf{sympLPN}(n, p)$.

To complete the reduction, we calculate the success probability of our algorithm for $\mathsf{LSN}(k, n, p)$. Let $a := \Pr[\mathcal{O}(S) = \texttt{structured}]$ and $b := \Pr[\mathcal{O}(U) = \texttt{structured}]$, where S and U denote the structured and unstructured challenge distributions. By complementing the oracle output if necessary, assume $a - b = 2\epsilon$ for some $\epsilon \geq 1/\operatorname{poly}(n)$. If $\mathbf{y} = \mathbf{0}$, the algorithm succeeds with probability a. If $\mathbf{y} \neq \mathbf{0}$, it succeeds with probability at least $\frac{1-b-\operatorname{negl}(n)}{2^k-1}$. The probability of correctness over random $\mathbf{y}$ is therefore at least

$$\frac{a}{2^k} + \frac{2^k - 1}{2^k} \frac{1 - b - \operatorname{negl}(n)}{2^k - 1} = \frac{1}{2^k} + \frac{2\epsilon}{2^k} - \operatorname{negl}(n), \tag{16}$$

which exceeds 2^{-k} by an inverse-polynomial amount because $k = O(\log n)$ and $\epsilon \geq 1/\operatorname{poly}(n)$. □

4.2 Reducing logical bits in sympLPN without reducing hardness

In this section, we tighten the hardness of $\mathsf{sympLPN}$ by reducing $\mathsf{sympLPN}(n, p) = \mathsf{sympLPN}(n, n, p)$ to $\mathsf{sympLPN}(n-1, n, p')$ for slightly larger p'. In particular, this reduction barely changes the parameters, simply reducing the number of logical bits by 1. However, it is surprisingly technical and essential for our cryptographic constructions. To give a baseline intuition for this reduction, we show in Appendix A a simple analogous reduction for LPN, which proceeds by simply removing the last column of the code matrix. Unfortunately, as discussed in Section 2, this proof technique does not extend to $\mathsf{sympLPN}$ because the last column of the $\mathsf{sympLPN}$ code matrix depends heavily on the rest of the matrix. Thus, our reduction technique proceeds via a completely different approach.

Our proof will proceed in three steps. We begin with a sample of $\mathsf{sympLPN}(n, p)$, $(\mathbf{A}, \mathbf{u})$, where $\mathbf{u}$ is either structured (i.e. of the form $\mathbf{A}\mathbf{x} + \mathbf{e}$) or uniformly random. Letting $V = \operatorname{im}(\mathbf{A})$, we consider the subspace $W := \operatorname{span}(\mathbf{f}_1)^\perp \cap V$, i.e. the hyperplane in V of vectors symplectically orthogonal to $\mathbf{f}_1$, the $(n+1)$st standard basis vector in $\mathbb{Z}_2^{2n}$. W has dimension $n-1$ with overwhelming probability (so we will assume it does), and it contains precisely the vectors in V whose first coordinate is zero.

Suppose $\mathbf{u}$ is structured. If the first physical bit has no error, i.e. $e_1 = 0$, then $\mathbf{Ax} \in W$ if and only if the first bit of $\mathbf{Ax} + \mathbf{e}$ is 0. We wish to transform $\mathbf{u}$ to some $\mathbf{u}'$ such that $\mathbf{u}'$ is of the form $\mathbf{Ax}' + \mathbf{e}$ but $\mathbf{Ax}' \in W$. If $\mathbf{Ax} \in W$, then no further action is required, and we set $\mathbf{u}' = \mathbf{u}$. If $\mathbf{Ax}$ is *not* in W, by adding some $\mathbf{v} \in V \backslash W$ we can obtain $\mathbf{u}' := (\mathbf{Ax} + \mathbf{v}) + \mathbf{e} = \mathbf{Ax}' + \mathbf{e}$ such that $\mathbf{Ax}' \in W$. Note that if instead $\mathbf{u}$ were unstructured, this transformation would make $\mathbf{u}'$ uniformly random on $\mathbf{f}_1^\perp$, the hyperplane of vectors with first coordinate zero.

After this step, under the assumption that $e_1 = 0$, we have almost prepared a sample of $\mathsf{sympLPN}$ with $n-1$ logical qubits. Indeed, letting $\mathbf{B}$ be a code with W as its codespace, we can prepare $\mathbf{u}'$ so that:

1. If $\mathbf{u}$ is uniformly random, then $\mathbf{u}'$ is uniformly random on $\mathbf{f}_1^\perp$.
2. If $\mathbf{u} = \mathbf{Ax} + \mathbf{e}$, then $\mathbf{u}' = \mathbf{By} + \mathbf{e}$ for uniformly random $\mathbf{y}$.

However, W is *not* a uniformly random $(n-1)$-dimensional isotropic vector space, because it is always symplectically orthogonal to a known vector, namely $\mathbf{f}_1$. Therefore, $\mathbf{B}$ is not a uniformly random matrix with symplectically orthogonal columns. In the second step of the reduction, we design a sparse Clifford operator $\mathbf{C}$ which randomly rotates the normal vector $\mathbf{f}_1$ (the hyperplane then follows along). This operation fully scrambles the code, so that $\mathbf{CB} \in \mathbb{Z}_2^{2n \times (n-1)}$ is statistically indistinguishable from a uniformly random matrix with symplectically orthogonal columns.

This second step converts a structured sample $\mathbf{u}'$ to $\mathbf{Cu}' = \mathbf{CBy} + \mathbf{Ce}$, however, which damages the distribution of the noise $\mathbf{e}$. However, since $\mathbf{C}$ is sparse, as long as $e_{n+1} = 0$, i.e. no error occurs on the $(n+1)$st physical bit, $\mathbf{Ce}$ is low-weight. In this case, we are able to re-randomize to transform $\mathbf{Ce}$ back into depolarizing noise, at the cost of a slightly larger noise parameter p'. Now, we may query the $\mathsf{sympLPN}(n-1, n, p')$ oracle, which will output `structured` or `unstructured`, and the reduction can output the same for the sample $(\mathbf{A}, \mathbf{u})$.

This completes the reduction, but only under the assumption that a good event occurs, namely that $e_1 = e_{n+1} = 0$. However, interestingly, this assumption can be completely circumvented. In the original sample, (e_1, e_{n+1}) follows a 1-qubit depolarizing distribution with parameter p. We are, however, free to increase this noise parameter to any $q > p$ by adding additional error ourselves. For example, we could create an alternate reduction by first adding completely random bits to increase the noise on (e_1, e_{n+1}) to that of $\mathcal{D}_{3/4}$, before executing the reduction outlined above. We show that at least one of these two reductions must succeed, or else the reduction could not possibly succeed when the good event *does* occur. This is a contradiction, and thus either the original reduction or the alternate one with extra noise added must reduce $\mathsf{sympLPN}(n, p)$ to $\mathsf{sympLPN}(n-1, n, p')$.

To establish the above argument rigorously, we begin by constructing the sparse, randomizing distribution of Cliffords. Recall that $\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{f}_1, \ldots, \mathbf{f}_n$ denotes the standard symplectic basis on $\mathbb{Z}_2^{2n}$.

Definition 4.2 (Symplectic hyperplane rotation)**.** For $n \geq 2$, a *random symplectic hyperplane rotation* is an efficiently sampleable ensemble of matrices $\mathcal{R}_n$ in $\mathbb{Z}_2^{2n \times 2n}$ constructed as follows. Sample a uniformly random $\mathbf{r} \sim \mathbb{Z}_2^{2n}$. Let k be the first (positive) index for which $r_{n+k} = 1$ (if there is no such index, output $\mathbf{C} := \mathbf{I}$). Let $\mathbf{r}'$ be the same as $\mathbf{r}$, except entries 1 and k are swapped, and entries $n+1$ and $n+k$ are swapped. Let the map $\mathbf{C}_0$ execute the following map on standard basis vectors, where $\mathbf{e}_i, \mathbf{f}_i$ are respectively the ith and $(n+i)$th standard basis vectors.

$$\mathbf{e}_1 \longmapsto \mathbf{e}_1, \tag{17}$$

$$\mathbf{f}_1 \longmapsto \mathbf{r}', \tag{18}$$

$$\mathbf{e}_j \longmapsto \mathbf{e}_j + (\mathbf{r}' \odot \mathbf{e}_j)\mathbf{e}_1 \quad \text{for } j \text{ from 2 to } n, \tag{19}$$

$$\mathbf{f}_j \longmapsto \mathbf{f}_j + (\mathbf{r}' \odot \mathbf{f}_j)\mathbf{e}_1 \quad \text{for } j \text{ from 2 to } n \tag{20}$$

Define a matrix $\mathbf{\Pi}$ which swaps $(\mathbf{e}_1, \mathbf{f}_1)$ and $(\mathbf{e}_k, \mathbf{f}_k)$, and otherwise for each $j \neq 1, k$ acts as identity on $\mathbf{e}_j, \mathbf{f}_j$. Then, output $\mathbf{C} := \mathbf{\Pi}\mathbf{C}_\mathbf{0}$. Note that $\mathbf{C}\mathbf{f}_1 = \mathbf{r}$ whenever such an index k exists.

This rotation, by randomizing $\mathbf{f}_1$ up to negligible total variation distance, also randomizes the hyperplane that is symplectically orthogonal to it. The remaining relations serve only to ensure that the map is a sparse symplectic matrix (i.e., that it preserves the symplectic inner product). We claim that $\mathbf{C}$ is a valid symplectic matrix which maps the hyperplane orthogonal to $\mathbf{f}_1$ to a hyperplane whose distribution is within negligible total variation distance of uniform.

Lemma 4.3 (Randomizing symplectic hyperplanes)**.** *Denote by $\mathcal{R}_n$ the ensemble of random symplectic hyperplane rotations from Definition 4.2. Sample $\mathbf{C} \sim \mathcal{R}_n$. Then the following properties hold.*

(1) $\mathbf{C}$ *is a symplectic matrix.*

(2) For $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \in \mathbb{Z}_2^{2n}$ a uniformly random basis of an $(n-1)$-dimensional isotropic subspace V (see Definition 3.1) which is uniformly random subject to $\mathbf{f}_1 \in V^\perp \setminus V$, let $\mathbf{w}_i := \mathbf{C}\mathbf{v}_i$. Then the distribution of $(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1})$ is within total variation distance $\mathrm{negl}(n)$ to a uniformly random basis of a random $(n-1)$-dimensional isotropic subspace.

The proof is deferred to Appendix C. Before we proceed to the reduction, we also require a lemma that total depolarizing noise, applied to only certain qubits, can be scrambled into completely symmetric depolarizing noise on all qubits. A similar technique was used in [KLP+26] to reduce from LPN to sympLPN.

Lemma 4.4 (Noise symmetrization)**.** *Let $\mathbf{e} \in \mathbb{Z}_2^{2n}$, and let $\pi \sim S^n$ be a random permutation on n elements. We define π to act on elements of $\mathbb{Z}_2^{2n}$ by executing the same permutation on the first and last set of n indices. Suppose that $(e_j, e_{n+j}) = (0,0)$ for all j except in a known set M of size $m = \omega(\log n)$ with $m \leq 3n/4$; for $j \in M$, $(e_j, e_{n+j}) \sim \mathcal{D}_{3/4}$ independently (i.e., random bits). Then, for any $q \in [\frac{m}{n}, \frac{3}{4}]$, there exists a distribution μ_n over $\mathbb{Z}_2^{2n}$, sampleable in time $\mathrm{poly}(n)$, such that $\pi(\mathbf{e} + \mathbf{e}')$ for $\mathbf{e}' \sim \mu_n$ is within total variation distance $\mathrm{negl}(n)$ from $\mathcal{D}_q^{\otimes n}$.*

The proof is deferred as well to Appendix C. We also record a relevant lemma about the product of depolarizing distributions.

Lemma 4.5 (Depolarizing convolution, [KLP+26])**.** *Let $\mathbf{P}_1, \mathbf{P}_2 \in \mathcal{P}_1$ be single-qubit phase-free Paulis such that $\mathbf{P}_1 \sim \mathcal{D}_p$ and, independently, $\mathbf{P}_2 \sim \mathcal{D}_u$ where $u = \frac{q-p}{1-\frac{4}{3}p}$ for any $p \in [0, \frac{3}{4})$ and $q \in [p, \frac{3}{4}]$. Then $\mathbf{P}_1\mathbf{P}_2 \sim \mathcal{D}_q$.*

Theorem 4.6 (Reducing by one logical bit in sympLPN)**.** *Let $p \in (0,1)$ be such that $\frac{3}{4} - p = \Omega(1)$, and let $n \in \mathbb{N}$ be sufficiently large. Suppose $\mathcal{O}$ is an oracle which solves Decision $\mathsf{sympLPN}(n-1, n, p + \log^2 n/n)$. Then there exists an algorithm running in time $\mathrm{poly}(n)$, which solves Decision $\mathsf{sympLPN}(n,p)$, using a single call to $\mathcal{O}$.*

Proof. Suppose first that the input is structured. That is, we are given $(\mathbf{A}, \mathbf{u} := \mathbf{A}\mathbf{x} + \mathbf{e})$, where $\mathbf{A} \in \mathbb{Z}_2^{2n \times n}$ is a uniformly random basis of a uniformly random isotropic subspace, $\mathbf{x} \sim \mathbb{Z}_2^n$, and $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$. Define $V := \mathrm{im}(\mathbf{A})$. Since $V = V^\perp$ is uniformly random, $\Pr[\mathbf{f}_1 \in V] = (2^n - 1)/(2^{2n} - 1) = 1/(2^n + 1)$. We condition on $\mathbf{f}_1 \notin V$, equivalently on at least one column of $\mathbf{A}$ having first entry 1. Define $V_0 \subseteq \mathrm{im}(\mathbf{A})$ to be the subspace of $\mathrm{im}(\mathbf{A})$ with vectors whose first entry is 0. Having first entry 0 is equivalent to being symplectically orthogonal to $\mathbf{f}_1$. Conditioning on this event, this is one extra nontrivial constraint, so $\dim(V_0) = n - 1$ and $\mathbf{f}_1 \in V_0^\perp \setminus V_0$. Moreover, V_0 is uniformly

random subject to these conditions: each such V_0 has three Lagrangian extensions, corresponding to the three lines in the two-dimensional symplectic space $V_0^\perp/V_0$, exactly two of which do not contain $\mathbf{f}_1$ and intersect $\mathbf{f}_1^\perp$ in V_0. Let $\mathbf{A}_0 \in \mathbb{Z}_2^{2n\times(n-1)}$ be a random basis matrix for V_0. Suppose that a good event occurs, namely that $(e_1, e_{n+1}) = (0,0)$. Conditioned on this event, either $u_1 = 0$ or $u_1 = 1$. If $u_1 = 1$, subtract from $\mathbf{u}$ the first column of $\mathbf{A}$ whose first entry is 1. If $u_1 = 0$, do nothing at this step. Denote by $\mathbf{u}' \in \mathbb{Z}_2^{2n}$ the outcome of this step. Note that conditioned on $\mathbf{A}_0$, $\mathbf{u}'$ is equidistributed as $\mathbf{A}_0\mathbf{x}' + \mathbf{e}'$, where $\mathbf{x}' \sim \mathbb{Z}_2^{n-1}$ and $\mathbf{e}'$ is independent depolarizing noise on pairs $(2, n+2), \ldots, (n, 2n)$ but $(e'_1, e'_{n+1}) = (0,0)$. Thus, we can equivalently express $\mathbf{u}' = \mathbf{A}_0\mathbf{x}' + \mathbf{e}'$. Set $q := \frac{\log^2 n}{n(1-\frac{4}{3}p)}$, $m := \lfloor nq \rfloor$, and $M := \{1, \ldots, m\}$.

Next, we sample and apply a random symplectic hyperplane rotation Clifford $\mathbf{C}$ from the ensemble in Definition 4.2. We condition on the pivot k of this rotation lying in M, an event of probability $1 - 2^{-m}$, where $\mathbf{r} = \mathbf{C}\mathbf{f}_1$. We apply $\mathbf{C}$ to $\mathbf{A}_0$ and $\mathbf{u}'$. By Lemma 4.3, $\mathbf{B} := \mathbf{C}\mathbf{A}_0$ is statistically indistinguishable from a uniformly random basis of a uniformly random isotropic subspace of dimension $n-1$. This additional conditioning changes the distribution by at most $2^{-m} = \mathrm{negl}(n)$. Meanwhile, $\mathbf{C}\mathbf{u}' = \mathbf{B}\mathbf{x}' + \mathbf{C}\mathbf{e}'$. The distribution of $\mathbf{C}\mathbf{e}'$ can be derived from the structural form of $\mathbf{C}$. Since $\mathbf{e}'$ is independent depolarizing noise $\mathcal{D}_p$ on the last $n-1$ qubits and $e'_1, e'_{n+1} = 0$, we may write $\mathbf{e}' = \sum_{j=2}^n (a_j\mathbf{e}_j + b_j\mathbf{f}_j)$, where $(a_j, b_j) \sim \mathcal{D}_p$ independently for $2 \le j \le n$, and we set $a_1 = b_1 = 0$. Let $\mathbf{\Pi}$ be the permutation matrix from Definition 4.2. Then, we can write

$$\mathbf{C}\mathbf{e}' = \mathbf{\Pi}\left(c\mathbf{e}_1 + \sum_{j=2}^n (a_j\mathbf{e}_j + b_j\mathbf{f}_j)\right) \tag{21}$$

$$= c\mathbf{e}_k + (a_k\mathbf{e}_1 + b_k\mathbf{f}_1) + \sum_{j\neq k,1} (a_j\mathbf{e}_j + b_j\mathbf{f}_j) \tag{22}$$

where the coefficient c of $\mathbf{e}_k$ has a potentially complicated distribution correlated with the (a_j, b_j). That is, $\mathbf{C}\mathbf{e}'$ takes the form of independent $\mathcal{D}_p$ noise on all but the kth pair, where the distribution is complicated. To adjust for this, we will add uniformly random bits to the kth pair (i.e. sample from $\mathcal{D}_{3/4}$), given by $\mathbf{s}_0 \in \mathbb{Z}_2^{2n}$ which is 0 on all indices, except uniformly random on k and $n+k$. This step erases any correlation the kth pair currently has with the $(a_j, b_j)_{j\neq k}$ (since this pair is now independently and uniformly random). The distribution of the error is therefore now $\mathbf{C}\mathbf{e}' + \mathbf{s}_0 \sim \mathcal{D}_p^{\otimes k-1} \otimes \mathcal{D}_{3/4} \otimes \mathcal{D}_p^{\otimes n-k}$. It is convenient to represent this distribution as the sum of two random variables, one $\mathbf{e}'' \sim \mathcal{D}_p^{\otimes n}$ and the other $\mathbf{s}$ which is the uniform distribution on the kth index and 0 elsewhere. Now, the conditions of Lemma 4.4 require that the error pairs (e_j, e_{n+j}) are 0 for all j outside a known set of size $m = \omega(\log n)$. In our case, add a vector $\mathbf{s}' \in \mathbb{Z}_2^{2n}$ which is uniformly random on the pairs in $M \setminus \{k\}$ and zero elsewhere. Define $\mathbf{t} := \mathbf{s} + \mathbf{s}'$, a vector which has uniform bits on m pairs and is $(0,0)$ on all other pairs. We add $\mathbf{s}'$ to our error, producing $\mathbf{e}'' + \mathbf{t}$. Note that $\mathbf{e}''$ and $\mathbf{t}$ are independent. The rotation changes no error pair outside M, while the added masks make all pairs in M uniform. Thus, conditional on $(\mathbf{A}, \mathbf{A}_0, \mathbf{C})$, the error has the same distribution $\mathcal{D}_{3/4}^{\otimes m} \otimes \mathcal{D}_p^{\otimes(n-m)}$, so this representation can be chosen independently of $(\mathbf{B}, \mathbf{x}')$. Applying Lemma 4.4, we may add an extra certain random vector $\mathbf{t}'$ and apply a random permutation π on the n index pairs such that $\pi(\mathbf{t} + \mathbf{t}')$ is within total variation distance $\mathrm{negl}(n)$ of $\mathcal{D}_q^{\otimes n}$. We use the sampler from its proof, choosing the additional pairs in increasing order. On the other hand, $\mathbf{e}''$ is permutation-invariant, so $\pi(\mathbf{e}'') \sim \mathbf{e}''$. Let $p' = p + \log^2 n/n$. Our choices satisfy $m/n \le q = \frac{p'-p}{1-\frac{4}{3}p} \le \frac{3}{4}$ and $m = \omega(\log n)$ for sufficiently large n, since $\frac{3}{4} - p = \Omega(1)$. Hence, by Lemma 4.5,

$$\mathrm{TV}\Big(\mathcal{L}\big(\pi(\mathbf{e}'' + \mathbf{t} + \mathbf{t}')\big), \mathcal{D}_{p'}^{\otimes n}\Big) \le \mathrm{negl}(n), \qquad p' = p + \left(1 - \frac{4}{3}p\right)q, \tag{23}$$

Up to negligible total variation distance, $\mathbf{B}$ is a uniform isotropic basis independent of $(\mathbf{x}', \mathbf{e}'', \mathbf{t}, \mathbf{t}', \pi)$. Since its distribution is invariant under each fixed π, the pair $(\pi\mathbf{B}, \pi(\mathbf{B}\mathbf{x}' + \mathbf{e}'' + \mathbf{t} + \mathbf{t}'))$ is therefore within negligible total variation distance of a structured $\mathsf{sympLPN}(n-1, n, p')$ instance, conditional on the good event. On the other hand, if the input were instead unstructured, then almost all of the operations we performed on $\mathbf{u}$ would leave its distribution—uniform over $\mathbb{Z}_2^{2n}$—invariant. The only step which does not is the first, wherein we alter $\mathbf{u}$ to $\mathbf{u}'$ which yields a uniformly random vector with first bit 0. After multiplication by $\mathbf{C}$, $\mathbf{C}\mathbf{u}'$ is uniform on $\mathbf{r}^\perp$, conditional on $\mathbf{A}$ and $\mathbf{C}$. Since $\mathbf{e}_k \odot \mathbf{r} = r_{n+k} = 1$, adding an independent uniform bit in direction $\mathbf{e}_k$ makes the result uniform over $\mathbb{Z}_2^{2n}$. This remains true after the remaining masks and permutation, conditional on the transformed public matrix. Therefore, conditioned on the good event in the structured case, this transformation produces the appropriate structured or unstructured target distribution up to negligible total variation distance. We submit our transformed instance to $\mathcal{O}$ and output its Decision. If no column of $\mathbf{A}$ has first entry 1, or the rotation has no pivot in M, we instead query $\mathcal{O}$ on a fresh unstructured target instance and return its output. These events have total probability at most $1/(2^n+1) + 2^{-m} = \mathrm{negl}(n)$. To complete the proof, we must address the cases in which the good event does not occur. That is, we discuss the cases when $(e_1, e_{n+1}) \neq (0,0)$. The other cases for the values of (e_1, e_{n+1}) are $(0,1), (1,0), (1,1)$. Let $p_{ij} = \Pr[(e_1, e_{n+1}) = (i,j)]$. Then $p_{00} = 1-p$ and $p_{01} = p_{10} = p_{11} = p/3$. Define q_{ij} to be the probability that $\mathcal{O}$ outputs `structured` when we receive a structured input wherein $(e_1, e_{n+1}) = (i,j)$; let $\bar{q}$ be the probability that $\mathcal{O}$ outputs `structured` on an unstructured input. By the above, $|q_{00} - \bar{q}| \geq \frac{1}{\mathrm{poly}(n)}$. In general,

$$Q_0 := \Pr_{p_{ij}=(1-p,p/3,p/3,p/3)}[\mathcal{O} = \texttt{structured} \,|\, \texttt{structured}] \tag{24}$$

$$= q_{00}(1-p) + \frac{p}{3}(q_{01} + q_{10} + q_{11}). \tag{25}$$

Now, consider an alternate reduction wherein we first add uniform noise to bits 1 and $n+1$ of $\mathbf{u}$. This has no effect on unstructured instances, but on structured instances, we may equivalently express the effect of the extra noise by modifying $p_{ij} = 1/4$ for all i, j. In this case,

$$Q_1 := \Pr_{p_{ij}=(1/4,1/4,1/4,1/4)}[\mathcal{O} = \texttt{structured} \,|\, \texttt{structured}] \tag{26}$$

$$= q_{00}\frac{1}{4} + \frac{1}{4}(q_{01} + q_{10} + q_{11}). \tag{27}$$

Suppose that both probabilities were negligibly close to unstructured probability, i.e. $|Q_0 - \bar{q}| = \mathrm{negl}(n)$ and $|Q_1 - \bar{q}| = \mathrm{negl}(n)$. Define

$$a := \frac{1}{1 - \frac{4}{3}p},\ b := -\frac{4}{3}ap. \tag{28}$$

Then $a + b = 1$ and $aQ_0 + bQ_1 = q_{00}$. By the triangle inequality,

$$\frac{1}{\mathrm{poly}(n)} \leq |q_{00} - \bar{q}| = |aQ_0 + bQ_1 - \bar{q}| \leq a|Q_0 - \bar{q}| + |b| \cdot |Q_1 - \bar{q}| \tag{29}$$

$$= a \cdot \mathrm{negl}(n) + |b| \cdot \mathrm{negl}(n) = \mathrm{negl}(n), \tag{30}$$

where in the last line we used the fact that $\frac{3}{4} - p = \Omega(1)$ so that $a = O(1)$ and thus $|b| = O(1)$. This is a contradiction, and therefore either $|Q_0 - \bar{q}| \geq 1/\mathrm{poly}(n)$ or $|Q_1 - \bar{q}| \geq 1/\mathrm{poly}(n)$. In other words, at least one of the two reductions solves Decision $\mathsf{sympLPN}(n, p)$ with non-negligible advantage. □

We may now proceed to construct cryptographic protocols from sympLPN, starting with a simple one-way function, and then constructing public-key cryptography and oblivious transfer schemes that rely on the above result.

5 Public-key encryption from low-noise sympLPN

While private-key cryptography is readily constructible from LPN at constant noise rate, public-key encryption is substantially more challenging to construct from LPN at constant noise rate. Alekhnovich-style LPN-based PKE schemes with known attacks running in time $2^{O(\sqrt{n})}$ are correct only when $p = O(1/\sqrt{n})$ [Ale03, DP12]. We here construct a PKE scheme based on sympLPN with the same $\Theta(1/\sqrt{n})$ noise rate.

Construction 5.1 (PKE from low-noise sympLPN)**.** *Let $n \in \mathbb{N}$ be the security parameter and $p \in (0,1)$. The* PKE *scheme $\Sigma = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is given by:*

- $\mathsf{Gen}(1^n)$: *sample a random full-rank isotropic matrix $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$, $\mathbf{x} \sim \mathbb{Z}_2^n$ and $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$; output public key $\mathsf{pk} = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e})$ and secret key $\mathsf{sk} = \mathbf{x}$.*
- $\mathsf{Enc}(\mathsf{pk}, \mu)$: *to encrypt a single bit $\mu \in \{0,1\}$ using the public key $(\mathbf{A}, \mathbf{b})$, sample $\mathbf{f} \sim \mathcal{D}_p^{\otimes n}$ and output the ciphertext pair $\mathsf{ct} = (\mathbf{f} \odot \mathbf{A}, \mathbf{f} \odot \mathbf{b} + \mu)$.*
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$*: to decrypt $\mathsf{ct} = (\mathbf{u}, c)$ using the secret key $\mathsf{sk} = \mathbf{x}$, output $c + \mathbf{u} \cdot \mathbf{x}$.*

We next state the correctness and security of Construction 5.1. Our security proof demonstrates the CPA security of the scheme.

Theorem 5.2 (Correctness)**.** *For any $\delta > 0$, there exists $p = \Theta\left(1/\sqrt{n}\right)$ such that the* PKE *scheme Σ in Construction 5.1 is $(1-\delta)$-correct, i.e., for any message bit $\mu \in \{0,1\}$,*

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \mu \,\middle|\, \substack{(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{Gen}(1^n) \\ \mathsf{ct}\leftarrow\mathsf{Enc}(\mathsf{pk},\mu)}\right] \geq 1 - \delta. \tag{31}$$

Remark (Correctness amplification). For the PKE and OT applications, we amplify the scheme at $p = \Theta(1/\sqrt{n})$ to have negligible decryption error by encrypting each bit $2\lceil \log^2 n \rceil + 1$ times under the same public key with fresh independent encryption randomness and taking the majority of the decrypted bits. This leaves key generation unchanged and preserves IND-CPA security.

The proof is deferred to Appendix C. Our security proof relies on the following indistinguishability lemma, which one can think of as the *dual mode* of sympLPN.

Lemma 5.3. *Let $n \in \mathbb{N}$ be the security parameter. Suppose that there exists an efficient (quantum or classical) algorithm which runs in time $\mathrm{poly}(n)$ and, with non-negligible advantage, distinguishes*

$$(\mathbf{H}, \mathbf{f} \odot \mathbf{H}) \quad \textit{from} \quad (\mathbf{H}, \mathbf{r}), \tag{32}$$

where $\mathbf{H} = (\mathbf{B} \,|\, \mathbf{v}) \in \mathbb{Z}_2^{2n\times(n+1)}$ consists of a random full-rank isotropic matrix $\mathbf{B} \in \mathbb{Z}_2^{2n\times n}$ and a random column vector $\mathbf{v} \sim \mathbb{Z}_2^{2n}$, and where $\mathbf{f} \sim \mathcal{D}_p^{\otimes n}$ and $\mathbf{r} \sim \mathbb{Z}_2^{n+1}$. Then there exists an efficient (quantum or classical) algorithm which solves Decision $\mathsf{sympLPN}(n-1, n, p)$.

Proof. Suppose we are given as input the $\mathsf{sympLPN}(n-1, n, p)$ instance $(\mathbf{A} \in \mathbb{Z}_2^{2n\times(n-1)}, \mathbf{b} \in \mathbb{Z}_2^{2n})$, where $\mathbf{b}$ is either structured with $\mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{f}$, for $\mathbf{f} \sim \mathcal{D}_p^{\otimes n}$, or unstructured with $\mathbf{b} \sim \mathbb{Z}_2^{2n}$. Note that the matrix $\mathbf{A}$ has full column rank $n-1$, and thus $S = \mathrm{im}(\mathbf{A})$ spans a $(n-1)$-dimensional subspace within $\mathbb{Z}_2^{2n}$. Consequently, the symplectic dual $S^\perp$—the space of vectors whose symplectic inner product with vectors in S is zero—is a subspace of dimension $n+1$. Our reduction proceeds as follows:

1. Sample $\mathbf{u} \sim S^\perp \backslash S$. Let $\mathbf{B} \in \mathbb{Z}_2^{2n \times n}$ be a random basis for $\mathrm{im}(\mathbf{A}) \oplus \mathrm{span}(\mathbf{u})$. Note that $\mathbf{B}$ is isotropic with $\dim \mathrm{im}(\mathbf{B}) = n$. Since n is the maximum dimension of an isotropic subspace, $\mathrm{im}(\mathbf{B}) = \mathrm{im}(\mathbf{B})^\perp$. Then, let $\mathbf{v}$ be a random vector in $S^\perp \setminus \mathrm{im}(\mathbf{B})$. Set $\mathbf{H} = (\mathbf{B} \,|\, \mathbf{v})$. We argue that $\mathbf{H}$ has negligible total variation distance from the random variable mentioned in Lemma 5.3.

2. Run the assumed distinguisher on input $(\mathbf{H}, \mathbf{b} \odot \mathbf{H})$.

Since each column of $\mathbf{H}$ is in $S^\perp$, $\mathbf{H}^\intercal \odot \mathbf{A} = 0$. Consequently,

- if $\mathbf{b}$ is structured with $\mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{f}$, our reduction computes

$$\mathbf{b} \odot \mathbf{H} = (\mathbf{H}^\intercal \odot \mathbf{b})^\intercal = (\mathbf{H}^\intercal \odot (\mathbf{A}\mathbf{x} + \mathbf{f}))^\intercal = (\mathbf{H}^\intercal \odot \mathbf{f})^\intercal = \mathbf{f} \odot \mathbf{H}; \tag{33}$$

- if $\mathbf{b}$ is unstructured with $\mathbf{b} \sim \mathbb{Z}_2^{2n}$, then our reduction computes $\mathbf{r} = \mathbf{b} \odot \mathbf{H}$.

In both cases, assuming a negligible total variation distance between $\mathbf{H}$ and the random variable mentioned above, we claim that the input to the distinguisher is negligibly close to the desired distribution. In the structured case, this is immediate, whereas in the unstructured case it readily follows from the fact that $\mathbf{r} = \mathbf{b} \odot \mathbf{H}$ is uniformly random over $\mathbb{Z}_2^{n+1}$ when $\mathbf{b} \sim \mathbb{Z}_2^{2n}$ itself is uniform. This is because $\mathbf{H}$ is a full-rank matrix, so that every bitstring in $\mathbb{Z}_2^{n+1}$ has the same number of pre-images under $\mathbf{H}^\intercal$.

We need only justify the assertion in Step 1 regarding the distribution of $\mathbf{H}$. First, we claim that $\mathbf{B}$ is a uniformly random full-rank isotropic matrix. Indeed, $\mathbf{A} \in \mathbb{Z}_2^{2n \times (n-1)}$ is a uniformly random full-rank isotropic matrix, and there are exactly $2^{n+1} - 2^{n-1}$ choices for $\mathbf{u}$ no matter what $\mathbf{A}$ is. Hence, the probability $p_{\mathbf{B}}$ of sampling any given $\mathbf{B}$ that is full rank and isotropic is $\frac{1}{(2^{n+1}-2^{n-1})N_{\mathbf{A}}}$, where $N_{\mathbf{A}}$ is the number of full-rank isotropic matrices $\mathbf{A} \in \mathbb{Z}_2^{2n \times (n-1)}$. This probability is equal for any such $\mathbf{B}$, so $\mathbf{B}$ is indeed uniformly distributed.

Next, we claim that $\mathbf{v}$ is negligibly close in distribution to a uniformly random vector outside of $\mathrm{im}(\mathbf{B})$. By definition, $\mathbf{v}$ is a random vector, not contained in $\mathrm{im}(\mathbf{B})$, that is symplectically orthogonal to a random $(n-1)$-dimensional subspace S of $\mathrm{im}(\mathbf{B})$, namely $\mathrm{im}(\mathbf{A})$. For any nonzero $\mathbf{v} \notin \mathrm{im}(\mathbf{B})$, $\mathbf{v}$ has an orthogonal complement of dimension $2n-1$, and its intersection with $\mathrm{im}(\mathbf{B})$ therefore has dimension $n-1$, one less than the maximum possible n. This is because not every element of $\mathrm{im}(\mathbf{B})$ is orthogonal to $\mathbf{v}$, as $\mathbf{v} \notin \mathrm{im}(\mathbf{B}) = \mathrm{im}(\mathbf{B})^\perp$. For each $\mathbf{v} \notin \mathrm{im}(\mathbf{B})$, therefore, there is exactly one $(n-1)$-dimensional subspace of $\mathrm{im}(\mathbf{B})$ which is orthogonal to $\mathbf{v}$. Say that the number of $(n-1)$-dimensional subspaces of $\mathrm{im}(\mathbf{B})$ is $N_{\mathbf{B}}$. Then the probability of sampling any $\mathbf{v} \notin \mathrm{im}(\mathbf{B})$ is $\frac{1}{(2^{n+1}-2^n)N_{\mathbf{B}}}$, a constant not depending on $\mathbf{v}$ as desired. ($2^{n+1} - 2^n$, above, is the number of vectors $\mathbf{v} \notin \mathrm{im}(\mathbf{B})$ orthogonal to any given $(n-1)$-dimensional $V \subseteq \mathbf{B}$.)

Recall that the total variation distance between uniform distributions over sets $\mathcal{X}, \mathcal{Y}$ where $\mathcal{X} \subseteq \mathcal{Y}$, is given by $1 - |\mathcal{X}|/|\mathcal{Y}|$. Thus, for each $\mathbf{B}$, $\mathbf{v}$ has total variation distance 2^{-n} from uniform over all of $\mathbb{Z}_2^{2n}$, since it is uniform over $\mathbb{Z}_2^{2n} \backslash \mathrm{im}(\mathbf{B})$, which is a $1 - 2^{-n}$ fraction of the full set. Therefore, the distribution of $\mathbf{H} = (\mathbf{B} \,|\, \mathbf{v})$ has negligible total variation distance from one wherein $\mathbf{B}$ is a uniformly random full-rank isotropic matrix and $\mathbf{v} \sim \mathbb{Z}_2^{2n}$. □

Theorem 5.4 (Security)**.** *Let $n \in \mathbb{N}$ be the security parameter and Σ be the public-key encryption scheme in Construction 5.1 with parameter p. Suppose there is a (quantum or classical) algorithm $\mathcal{A}$, running in time $\mathrm{poly}(n)$, which breaks the IND-CPA security of Σ. Then there is a (quantum or classical) algorithm $\mathcal{B}$ which solves either Decision $\mathsf{sympLPN}(n, p)$ or Decision $\mathsf{sympLPN}(n-1, n, p)$.*

Proof. Let $n \in \mathbb{N}$. For each fixed $\mu \in \{0, 1\}$, consider the following hybrid distributions of $(\mathsf{pk}, \mathsf{ct})$:

- H_0 : The public key pk and ciphertext ct are generated by Σ in Construction 5.1 with

$$\mathsf{ct} = (\mathbf{f} \odot \mathbf{A}, \mathbf{f} \odot \mathbf{b} + \mu) \tag{34}$$

  where $\mathsf{pk} = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e})$ and $\mathsf{sk} = \mathbf{x}$ are output by $\mathsf{Gen}(1^n)$ such that $\mathbf{A} \in \mathbb{Z}_2^{2n \times n}$ is a random full-rank isotropic matrix, $\mathbf{x} \sim \mathbb{Z}_2^n$, and $\mathbf{e}, \mathbf{f} \sim \mathcal{D}_p^{\otimes n}$.

- H_1 : Same as H_0, except that $\mathbf{b}$ in the public key $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$ is instead sampled uniformly at random over $\mathbb{Z}_2^{2n}$.

- H_2 : Same as H_1, except that ct is chosen uniformly at random over $\mathbb{Z}_2^{n+1}$.

Recall that the IND-CPA security game for a one-bit PKE scheme is defined as follows. The challenger samples $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$ and $\mu \leftarrow \{0, 1\}$. Then the challenger sends $\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \mu)$ to the adversary, who responds with a guess $\hat{\mu}$. The adversary wins if $\hat{\mu} = \mu$, and we define the adversary's advantage as $|\Pr[\hat{\mu} = \mu] - 1/2|$. Importantly, in H_2 the encryption ct is completely independent of μ, and hence the distinguishing advantage in the IND-CPA experiment is zero. Thus an advantageous adversary in this game implies a distinguisher with non-negligible advantage for at least one of these hybrids. Consequently, it suffices to show that the three hybrids are computationally indistinguishable.

First we show that an efficient distinguisher between H_0 and H_1 implies an efficient solver for Decision $\mathsf{sympLPN}(n, p)$. Suppose we are given as input $(\mathbf{A}, \mathbf{b})$, where $\mathbf{b}$ is either structured (i.e. $\mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e}$) or unstructured (i.e. $\mathbf{b} \sim \mathbb{Z}_2^{2n}$). Then we can generate the ciphertexts for each μ ourselves, simulating the two hybrids. Thus, an efficient algorithm distinguishing H_0 and H_1 with non-negligible advantage implies an efficient solver for Decision $\mathsf{sympLPN}(n, p)$.

Next, we argue that the hybrids H_1 and H_2 are indistinguishable. To prove this, we will view the public key $(\mathbf{A}, \mathbf{b})$ as a matrix $\mathbf{H} \in \mathbb{Z}_2^{2n \times (n+1)}$. This matrix $\mathbf{H}$ satisfies the property that the first n columns form a uniformly random full-rank isotropic matrix, while the final column is uniformly random. In H_1, $\mathsf{ct} = \mathbf{f} \odot \mathbf{H} + (0^n, \mu)$, whereas in H_2, $\mathsf{ct} = \mathbf{r} \sim \mathbb{Z}_2^{n+1}$. For each fixed $\mu \in \{0, 1\}$, any distinguisher between H_1, which gives $(\mathbf{H}, \mathbf{f} \odot \mathbf{H} + (0^n, \mu))$, and H_2, which gives $(\mathbf{H}, \mathbf{r})$, implies a distinguisher between $(\mathbf{H}, \mathbf{f} \odot \mathbf{H})$ and $(\mathbf{H}, \mathbf{r})$ by way of adding $(0^n, \mu)$ ourselves (in the case of $(\mathbf{H}, \mathbf{r})$, adding $(0^n, \mu)$ has no effect on the distribution of $\mathbf{r}$). Moreover, a distinguisher for the latter problem implies a solver for Decision $\mathsf{sympLPN}(n - 1, n, p)$ by Lemma 5.3. We conclude therefore that H_1 and H_2 are computationally indistinguishable under the hardness of $\mathsf{sympLPN}(n - 1, n, p)$. □

Previously, in Section 4.2, we showed in Theorem 4.6 that Decision $\mathsf{sympLPN}(n, p_0)$ reduces to $\mathsf{sympLPN}(n - 1, n, p)$ where $p = p_0 + \log^2 n/n$. Hence, taking $p = p_0 + \log^2 n/n$ in Construction 5.1, its security is based entirely on the hardness of Decision $\mathsf{sympLPN}(n, p_0)$, for $p_0 = \Theta(1/\sqrt{n})$: Decision $\mathsf{sympLPN}(n, p_0)$ also reduces to Decision $\mathsf{sympLPN}(n, p)$ by adding independent depolarizing noise, using Lemma 4.5. Since $\log^2 n/n = o(1/\sqrt{n})$, the scheme still uses $p = \Theta(1/\sqrt{n})$, as desired.

6 Strongly uniform public-key encryption

In this section, we alter our previous PKE construction to upgrade it into a so-called Strongly Uniform Type-A PKE (SU-PKE). A post-quantum SU-PKE scheme is known to imply oblivious transfer (OT) and secure multiparty computation with constant-round ε-simulation or polynomial-round full simulation [CLPY25].

Definition 6.1 (Strongly Uniform Type-A Public-Key Encryption)**.** A PKE scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called "Strongly Uniform of Type A" if the public key pk generated by $\mathsf{Gen}(1^n)$ is computationally

indistinguishable from a uniform distribution over some efficiently sampleable group parameterized by n, $G(n)$.

For our purposes, the public key takes values in $\mathbb{Z}_2^m$ for some m depending on n, and this is the corresponding group. However, the PKE scheme presented in Section 5 is not strongly uniform. The public key is of the form $(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{e})$—while $\mathbf{A}\mathbf{x} + \mathbf{e}$ is computationally indistinguishable from uniform, $\mathbf{A}$ is a uniformly random full-rank isotropic, and is thus far from uniform. Fortunately, it is possible to change the cryptographic protocol to remedy this problem. To do so, we first prove a lemma that relates the random variable $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$ to a uniform distribution over $\mathbb{Z}_2^{4n^2}$.

Lemma 6.2 (A uniformly random public key)**.** *Sample $\mathbf{s} \sim \mathbb{Z}_2^{4n^2}$ and let $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$ be a uniformly random full-rank isotropic matrix. There exists a deterministic, polynomial-time classical algorithm $\mathcal{A}$ and a polynomial-time, randomized classical algorithm $\mathcal{B}$ such that $\mathcal{A}(\mathbf{s})$ is statistically indistinguishable from $\mathbf{A}$, $\mathcal{B}(\mathbf{A})$ is statistically indistinguishable from $\mathbf{s}$, and*

$$\Pr_{\mathcal{B},\mathbf{A}}[\mathcal{A}(\mathcal{B}(\mathbf{A})) = \mathbf{A}] = 1 - \mathrm{negl}(n). \tag{35}$$

Proof. Intuitively, $\mathcal{A}$ uses $\mathbf{s}$ as a source of randomness to deterministically construct $\mathbf{A}$ such that if $\mathbf{s}$ is uniformly random, then $\mathbf{A}$ is a uniformly random full-rank isotropic matrix. We construct $\mathcal{A}$ as follows. Given $\mathbf{s} \sim \mathbb{Z}_2^{4n^2}$, we build $\mathbf{A}$ column-by-column. Let $\widetilde{\mathbf{A}}_i \in \mathbb{Z}_2^{2n\times i}$ be a matrix with i columns, and let $\widetilde{\mathbf{A}}_0$ be an empty matrix. For $i = 1, \ldots, 2n$, we use a deterministic algorithm to calculate an ordered basis for the symplectic dual space of $\mathrm{im}(\widetilde{\mathbf{A}}_{i-1})$. (By convention, the dual of the empty matrix is $\mathbb{Z}_2^{2n}$.) This orthogonal complement has some dimension $d_i \leq 2n$, and we may consume the next d_i unused bits of $\mathbf{s}$ to sample a random vector $\mathbf{w} \in \mathrm{im}(\widetilde{\mathbf{A}}_{i-1})^\perp$. Then, we can set $\widetilde{\mathbf{A}}_i = (\widetilde{\mathbf{A}}_{i-1} \,|\, \mathbf{w})$. This process yields a matrix $\widetilde{\mathbf{A}}_{2n}$, and there are always enough bits of $\mathbf{s}$ since there are $2n$ steps taking $d_i \leq 2n$ bits each. $\widetilde{\mathbf{A}}_{2n}$ is almost what we want, except that it has twice as many columns as needed and is not necessarily full rank.

Therefore, we define $\mathbf{A}$ by iteratively adding the ith column of $\widetilde{\mathbf{A}}_{2n}$ if it is linearly independent to all previous columns. We then pad $\mathbf{A}$ with zero columns until all n columns are filled in (this is an edge-case event which we will momentarily show occurs with only negligible probability). Note that the number of columns is never larger than n, since there can be at most n linearly independent vectors that are symplectically orthogonal.

Now, we claim that $\mathcal{A}(\mathbf{s})$ is statistically indistinguishable from a uniformly random full-rank isotropic matrix $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$. Conditioned on the event L—that $\mathbf{A}$ was not padded with any zero columns—we are constructing a matrix column by column by sampling symplectically orthogonal, linearly independent vectors, which yields precisely the same distribution as $\mathbf{A}$. Hence, we need only show $\Pr[L^c] = \mathrm{negl}(n)$. For the ith column of $\widetilde{\mathbf{A}}_{2n}$, the chance that it does not increase the rank from the previous $i-1$ columns is precisely $\frac{2^{2n-d_i}}{2^{d_i}}$. For $d_i \geq n+1$ this probability is at most $1/4$. At $i = 1$, d_i begins at $2n$, and decreases by 1 each time a linearly independent vector is added. If $\mathbf{A}$ does not have n columns prior to padding, then $\widetilde{\mathbf{A}}_{2n}$ does not have rank n, so this event must occur at least $n+1$ times. Each time this event occurs, d_i does not decrease, which means d_i decreased at most $n-1$ times. Before rank n is reached, each step fails to increase the rank with conditional probability at most $1/4$. The number of such failures is therefore stochastically dominated by $X \sim \mathsf{Bin}(2n, 1/4)$, and a Chernoff bound gives $\Pr[L^c] \leq \Pr[X \geq n+1] \leq \exp(() - n/6) = \mathrm{negl}(n)$. We next construct algorithm $\mathcal{B}$. Given an input $\mathbf{A} \in \mathbb{Z}_2^{2n\times n}$ that is full-rank and isotropic, we will describe a procedure for $i = 1, \ldots, 2n$ to build matrices $\widetilde{\mathbf{A}}_i$, with $\widetilde{\mathbf{A}}_0$ empty.

1. Let $d_i := \dim \mathrm{im}(\widetilde{\mathbf{A}}_{i-1})^\perp$. With probability $1 - \frac{2^{2n-d_i}}{2^{d_i}}$, let $\widetilde{\mathbf{A}}_i = (\widetilde{\mathbf{A}}_{i-1} \,|\, \mathbf{v}_i)$, where $\mathbf{v}_i$ is the next column of $\mathbf{A}$ which has not yet been sampled.

2. Otherwise, let $\widetilde{\mathbf{A}}_i = (\widetilde{\mathbf{A}}_{i-1} \mid \mathbf{u}_i)$, where $\mathbf{u}_i$ is a random vector in the span of the columns in $\mathbf{A}$ which have already been sampled. (If no column has yet been sampled, then $\mathbf{u}_i = \mathbf{0}$.)

Notice that the columns are all symplectically orthogonal. After all $2n$ iterations, given $\widetilde{\mathbf{A}}_{2n}$, reconstruct the random bits $\mathbf{s}'$ of length $m \leq 4n^2$ that would have produced $\widetilde{\mathbf{A}}_{2n}$. Sample the remaining bits uniformly at random to produce $\mathbf{s}$ of length $4n^2$. Output $\mathbf{s}$.

By the same reasoning as before, $\widetilde{\mathbf{A}}_{2n}$ has rank less than n with only $\mathrm{negl}(n)$ probability. Moreover, conditioned on the event L that $\widetilde{\mathbf{A}}_{2n}$ has rank n, we have that $\mathcal{A}(\mathcal{B}(\mathbf{A})) = \mathbf{A}$. Indeed, applying $\mathcal{A}$ to the seed $\mathbf{s} = \mathcal{B}(\mathbf{A})$ produces a matrix $\widetilde{\mathbf{A}}_{2n}$, and the first n linearly independent columns obtained from it give $\mathbf{A}$. Hence, $\Pr[\mathcal{A}(\mathcal{B}(\mathbf{A})) = \mathbf{A}] = 1 - \mathrm{negl}(n)$. It now suffices to show that $\mathcal{B}(\mathbf{A})$ is statistically indistinguishable from a uniformly random $\mathbf{s}$. The intermediate matrices need not be uniformly distributed, because their probabilities depend on when linearly dependent columns occur. However, when $\mathbf{A}$ is uniformly random, each next unused column, conditioned on the columns already consumed, is uniform among the admissible extensions, since every such extension has the same number of completions to a full-rank isotropic matrix. Both samplers use the same rank-transition probabilities and uniform samples from the current span for dependent columns, so they generate the same distribution of column sequences. Reconstructing the unique seed prefix for each sequence using the same deterministic ordered bases, and appending fresh uniform unused bits, therefore reproduces the uniform seed distribution of the forward sampler. By the procedure of $\mathcal{B}$, every full-rank $\mathbf{A}$ has exactly the same number of seeds $\mathbf{s}$, since the number of seeds only depends on counting which columns increase the rank of $\widetilde{\mathbf{A}}_{2n}$, and not the actual values of the first n linearly independent columns. $\mathcal{B}(\mathbf{A})$ is therefore uniform over all $4n^2$-bit seeds, including those for which $\mathcal{A}$ outputs a rank-deficient matrix. Now, noting that the event L^c that $\mathcal{A}(\mathbf{s})$ is not full-rank has $\mathrm{negl}(n)$ probability, we conclude that there is a negligible fraction of seeds which are not in the preimage of full-rank $\mathbf{A}$, so that the uniform distribution over seeds $\mathbf{s}'$ has negligible total variation distance from $\mathbf{s} \sim \mathbb{Z}_2^{4n^2}$. □

Corollary 6.3. *Let $\mathbf{s} \sim \mathbb{Z}_2^{4n^2}$, $\mathbf{A} \in \mathbb{Z}_2^{2n \times n}$, and algorithm $\mathcal{A}$ be as in Lemma 6.2. Fix any randomized algorithms $\mathcal{A}_1, \mathcal{A}_2$ mapping to $\{0,1\}^m$ for $m = \mathrm{poly}(n)$. If $(\mathbf{A}, \mathcal{A}_1(\mathbf{A}))$ is computationally indistinguishable from $(\mathbf{A}, \mathcal{A}_2(\mathbf{A}))$, then $(\mathbf{s}, \mathcal{A}_1(\mathcal{A}(\mathbf{s})))$ and $(\mathbf{s}, \mathcal{A}_2(\mathcal{A}(\mathbf{s})))$ are computationally indistinguishable.*

Proof. Suppose for contradiction that there is a distinguisher $\mathcal{D}$ for the latter two distributions. Then we can evaluate $\mathcal{D}$ on the sample $(\mathcal{B}(\mathbf{A}), \mathcal{R}(\mathbf{A}))$, where $\mathcal{R}$ is either $\mathcal{A}_1$ or $\mathcal{A}_2$. By writing $\mathbf{s}' = \mathcal{B}(\mathbf{A})$, this is precisely $\mathcal{D}(\mathbf{s}', \mathcal{R}(\mathcal{A}(\mathbf{s}')))$ with probability $1 - \mathrm{negl}(n)$, since $\mathcal{A}(\mathcal{B}(\mathbf{A})) = \mathbf{A}$ with that probability. However, $\mathbf{s}'$ has negligible total variation distance from $\mathbf{s}$, and hence $\mathcal{D}$ can distinguish between $\mathcal{R}$ being $\mathcal{A}_1$ versus $\mathcal{A}_2$. This is a contradiction. □

Corollary 6.4. *Assuming* $\mathsf{sympLPN}(n, p_0)$ *with* $p_0 = \Theta(\frac{1}{\sqrt{n}})$, *there exists a IND-CPA-secure SU-PKE scheme.*

Proof. Take $p = p_0 + \log^2 n/n$. Using Lemma 6.2, the construction, correctness, and security of the scheme in Section 5 can be readily repeated, which we now outline. In the construction keep the same secret key, but take the public key pk to be $(\mathbf{s}, \mathbf{b})$ for $\mathbf{b} = \mathcal{A}(\mathbf{s}) \cdot \mathbf{x} + \mathbf{e}$, where $\mathbf{s} \sim \mathbb{Z}_2^{4n^2}$ is uniformly random. Assuming the hardness of $\mathsf{sympLPN}$, this pk is manifestly computationally indistinguishable from uniformly random, satisfying the requirements of $\mathsf{SU\text{-}PKE}$ given in Definition 6.1. Then, the encryption algorithm $\mathsf{Enc}(\mathsf{pk}, \mu)$ outputs $\mathsf{ct} = (\mathbf{f} \odot \mathcal{A}(\mathbf{s}), \mathbf{f} \odot \mathbf{b} + \mu)$, while the decryption algorithm $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ for $\mathsf{ct} = (\mathbf{u}, c)$ outputs $c + \mathbf{u} \cdot \mathbf{x}$. For the basic scheme, reconstructing $\mathbf{A} = \mathcal{A}(\mathbf{s})$ incurs a polynomial-time preprocessing cost for each public key. Once $\mathbf{A}$ is cached, encryption takes $O(n^2)$

time per bit and decryption takes $O(n)$ time per bit. Amplification multiplies these per-bit costs and the ciphertext length by $O(\log^2 n)$. Correctness with negligible error follows from Theorem 5.2 and the subsequent amplification remark, since the scheme is exactly the same as the one in Section 5, up to negligible total variation distance. The only remaining claim is IND-CPA security. In the security proof in Theorem 5.4, one can replicate the exact same hybrid argument, replacing $\mathbf{A}$ in the public key with $\mathbf{s}$. Our arguments that H_0 and H_1 are indistinguishable, and that H_1 and H_2 are indistinguishable, both follow in the SU-PKE construction from an application of Corollary 6.3. Indeed, in both cases the new hybrid argument is the same as the original, except that $\mathbf{A}$ is replaced in the public key with $\mathbf{s}$. Meanwhile, the rest of the public key and ciphertext is one of two different randomized functions of $\mathbf{A}$, as formulated in Corollary 6.3. □

Our post-quantum SU-PKE scheme is a dense cryptosystem: its public keys are computationally indistinguishable from uniformly random bitstrings. Consequently, the results of Chatterjee, Liang, Pandey, and Yamakawa [CLPY25, Theorems 12, 13, and 20] yield both constant-round ε-simulatable OT and polynomial-round OT with full simulation against malicious quantum adversaries. Both guarantees follow from the same low-noise sympLPN hardness assumption. Here, ε-simulation allows distinguishing advantage at most $\varepsilon(n) + \mathrm{negl}(n)$ between the real and ideal executions, for every noticeable $\varepsilon(n)$, with a quantum simulator running in time $\mathrm{poly}(n, 1/\varepsilon)$ [CLPY25, Definition 7]. Full simulation requires negligible distinguishing advantage with a quantum simulator running in time $\mathrm{poly}(n)$.

Corollary 6.5. *Assuming the computational hardness of* $\mathsf{sympLPN}(n, p_0)$ *with* $p_0 = \Theta(1/\sqrt{n})$*, there exist (i) a constant-round ε-simulatable oblivious transfer protocol for every noticeable $\varepsilon = \varepsilon(n)$, and (ii) a polynomial-round oblivious transfer protocol with full simulation. Both protocols are secure against malicious quantum adversaries.*

The corresponding MPC guarantees follow from [CLPY25, Theorems 3 and 21].

Corollary 6.6. *Assuming the computational hardness of* $\mathsf{sympLPN}(n, p_0)$ *with* $p_0 = \Theta(1/\sqrt{n})$*, there exist (i) a constant-round ε-simulatable secure multiparty computation protocol for every noticeable $\varepsilon = \varepsilon(n)$, and (ii) a polynomial-round secure multiparty computation protocol with full simulation. Both protocols are secure against malicious quantum adversaries.*

These results demonstrate that low-noise sympLPN can underlie the same central cryptographic primitives that low-noise LPN can, including public-key encryption, oblivious transfer, and secure multiparty computation. It is open, however as to the comparative practical security of these schemes.

Acknowledgments

We thank Alexandru Gheorghiu, Gregory Kahanamoku-Meyer, Peter Shor and Vinod Vaikuntanathan for many insightful discussions, particularly on the state-of-the-art attacks on LPN and its many cryptographic applications. We would also like to credit Kabir Tomer with an independent discovery of how to construct one-way functions from the LSN assumption.

JZL is funded in part by a National Defense Science and Engineering Graduate (NDSEG) Fellowship. YQ is supported by a collaboration between the US DOE and other Agencies. This material is based upon work supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator.

References

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

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '09, page 595–618, Berlin, Heidelberg, 2009. Springer-Verlag.

[AF24] Victor V. Albert and Philippe Faist, editors. *The Error Correction Zoo*. 2024.

[AG11] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming*, pages 403–415. Springer, 2011.

[AHKI+17] Benny Applebaum, Naama Haramaty-Krasne, Yuval Ishai, Eyal Kushilevitz, and Vinod Vaikuntanathan. Low-Complexity Cryptographic Hash Functions. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 7:1–7:31, Dagstuhl, Germany, 2017. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[AJOP20] Gorjan Alagic, Stacey Jeffery, Maris Ozols, and Alexander Poremba. On quantum chosen-ciphertext attacks and learning with errors. *Cryptography*, 4(1), 2020.

[Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '03, page 298, USA, 2003. IEEE Computer Society.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states, 2022.

[BCG+02] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 449–458, 2002.

[BCG+19] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more. Cryptology ePrint Archive, Paper 2019/448, 2019.

[BCL+19] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Edoardo Persichetti Ruben Niederhagen, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, and Wen Wang. Classic mceliece: conservative code-based cryptography. Round-2 submission to the NIST Post-Quantum Cryptography Standardization Project, 2019. https://cryptojedi.org/papers/#mceliecenistr2.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996.

[BEM+26] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary Complexity and the Uhlmann Transformation Problem. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:17, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Beu22] Ward Beullens. Breaking rainbow takes a weekend on a laptop. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 464–479, Cham, 2022. Springer Nature Switzerland.

[BFKL94] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, pages 278–291, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[BHHP25] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient Quantum Pseudorandomness from Hamiltonian Phase States. In Bill Fefferman, editor, *20th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2025)*, volume 350 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM*, 50(4):506–519, jul 2003.

[BL17] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, September 2017.

[BLVW19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. Worst-case hardness for LPN and cryptographic hashing via code smoothing. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 619–635. Springer, 2019.

[BMvT78] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, 43(2):831–871, 2014.

[CCLST22] Ryann Cartor, Max Cartor, Mark Lewis, and Daniel Smith-Tone. Iprainbow. In *Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography*, volume 13512. Proceedings of PQCrypto 2022: The Thirteenth International Conference on Post-Quantum Cryptography, virtual, DC, US, 2022-09-28 04:09:00 2022.

[CDMT24] Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Reduction from sparse LPN to LPN, dual attack 3.0. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 286–315. Springer, Heidelberg, may 2024. Artifact available at https://artifacts.iacr.org/tches/2022/a10.

[CGGH24] Bruno P. Cavalar, Eli Goldin, Matthew Gray, and Peter Hall. A meta-complexity characterization of quantum cryptography, 2024.

[CGHKV24] Henry Corrigan-Gibbs, Alexandra Henzinger, Yael Tauman Kalai, and Vinod Vaikuntanathan. Somewhat homomorphic encryption from linear homomorphism and sparse LPN. Cryptology ePrint Archive, Paper 2024/1760, 2024.

[Che24] Yilei Chen. Quantum algorithms for lattice problems. Cryptology ePrint Archive, Paper 2024/555, 2024.

[CJL+16] Lidong Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography, 2016-04-28 2016.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Paper 2018/383, 2018.

[CLPY25] Rohit Chatterjee, Xiao Liang, Omkant Pandey, and Takashi Yamakawa. The round complexity of black-box post-quantum secure computation, 2025. Version 1; theorem numbering as cited.

[DDN14] Bernardo David, Rafael Dowsley, and Anderson CA Nascimento. Universally composable oblivious transfer based on a variant of LPN. In *International Conference on Cryptology and Network Security*, pages 143–158. Springer, 2014.

[DGH+20] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, Daniel Masny, and Daniel Wichs. Two-round oblivious transfer from CDH or LPN. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 768–797. Springer, 2020.

[DGJ+20] Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. Secure multi-party quantum computation with a dishonest majority. In *Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III*, page 729–758, Berlin, Heidelberg, 2020. Springer-Verlag.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DP12] Ivan Damgard and Sunoo Park. How practical is public-key encryption based on LPN and ring-LPN? *Cryptology ePrint Archive*, 2012.

[DS18] Yfke Dulek and Florian Speelman. Quantum ciphertext authentication and key recycling with the trap code, 2018.

[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, January 2005.

[EH22] Lior Eldar and Sean Hallgren. An efficient quantum algorithm for lattice problems achieving subexponential approximation factor, 2022.

[Eld23] Lior Eldar. An efficient quantum decoder for prime-power fields, 2023.

[ES16] Lior Eldar and Peter W. Shor. An efficient quantum algorithm for a variant of the closest lattice-vector problem, 2016.

[FGKP06] Vitaly Feldman, Parikshit Gopalan, Subhash Khot, and Ashok Kumar Ponnuswami. New results for learning noisy parities and halfspaces. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '06, page 563–574, USA, 2006. IEEE Computer Society.

[FGSY25] Bill Fefferman, Soumik Ghosh, Makrand Sinha, and Henry Yuen. The hardness of learning quantum circuits and its cryptographic applications, 2025.

[FMV19] Daniele Friolo, Daniel Masny, and Daniele Venturi. A black-box construction of fully-simulatable, round-optimal oblivious transfer from strongly uniform key agreement. In *Theory of Cryptography Conference*, pages 111–130. Springer, 2019.

[FS96] Jean-Bernard Fischer and Jacques Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 245–255. Springer, 1996.

[Gen09] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, Stanford, CA, USA, 2009. AAI3382729.

[GJL+25] Riddhi Ghosal, Aayush Jain, Paul Lou, Amit Sahai, and Neekon Vafa. Post-quantum PKE from unstructured noisy linear algebraic assumptions: Beyond lwe and alekhnovich's LPN. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025*, pages 64–93, Cham, 2025. Springer Nature Switzerland.

[GKZ19] Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning-with-errors problem is easy with quantum samples. *Phys. Rev. A*, 99:032314, Mar 2019.

[Got24] Daniel Gottesman. Quantum error correction and fault-tolerant quantum computation. https://www.cs.umd.edu/~dgottesm/QECCbook-2024.pdf, 2024. Lecture notes, University of Maryland.

[GRS08] Henri Gilbert, Matthew JB Robshaw, and Yannick Seurin. How to encrypt with the LPN problem. In *International Colloquium on Automata, Languages, and Programming*, pages 679–690. Springer, 2008.

[HB01] Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, page 52–66, Berlin, Heidelberg, 2001. Springer-Verlag.

[HH13] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6), June 2013.

[HHM25] Taiga Hiroka, Min-Hsiu Hsieh, and Tomoyuki Morimae. Hardness of quantum distribution learning and quantum cryptography, 2025.

[HLG11] Min-Hsiu Hsieh and Fran çois Le Gall. Np-hardness of decoding quantum error-correction codes. *Phys. Rev. A*, 83:052331, May 2011.

[HM25] Taiga Hiroka and Tomoyuki Morimae. *Quantum Cryptography and Meta-Complexity*, page 545–574. Springer Nature Switzerland, 2025.

[HP07] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, sep 2007.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In *Proceedings of the 3rd International Symposium on Algorithmic Number Theory (ANTS III)*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[ILL89] Russell Impagliazzo, Leonid A Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 12–24, 1989.

[Imp95] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995.

[IP15] Pavithran Iyer and David Poulin. Hardness of decoding quantum stabilizer codes. *IEEE Transactions on Information Theory*, 61(9):5209–5223, 2015.

[JW05] Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human protocols. In *Proceedings of the 25th Annual International Conference on Advances in Cryptology*, CRYPTO'05, page 293–308, Berlin, Heidelberg, 2005. Springer-Verlag.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC, 2007.

[KL20] Kao-Yueh Kuo and Chung-Chin Lu. On the hardnesses of several quantum decoding problems. *Quantum Information Processing*, 19(4):123, 2020.

[KLP+26] Andrey Boris Khesin, Jonathan Lu, Alexander Poremba, Akshar Ramkumar, and Vinod Vaikuntanathan. Average-case complexity of quantum stabilizer decoding. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*, pages 857–868, 2026.

[KLS25] Andrey Boris Khesin, Jonathan Z Lu, and Peter W Shor. Universal graph representation of stabilizer codes. *PRX Quantum*, 6(4):040325, 2025.

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197, pages 2:1–2:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

[KSS10] Jonathan Katz, Ji Sun Shin, and Adam Smith. Parallel and concurrent security of the hb and hb+ protocols. *Journal of cryptology*, 23(3):402–421, 2010.

[KT25] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #P hardness. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 178–188, New York, NY, USA, 2025. Association for Computing Machinery.

[Kup04] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, 2004.

[LM24] Yi-Kai Liu and Dustin Moody. Post-quantum cryptography, and the quantum future of cybersecurity. *Physical Review Applied*, 21(21):040501, 2024-04-09 04:04:00 2024.

[Lyu05] Vadim Lyubashevsky. The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In Chandra Chekuri, Klaus Jansen, José D. P. Rolim, and Luca Trevisan, editors, *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques*, pages 378–389, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[Mel24] Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner's tutorial. *Quantum*, 8:1340, 2024.

[Mer78] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, April 1978.

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries, 2024.

[MR09] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post-Quantum Cryptography*, Springer Books, pages 147–191. Springer, March 2009.

[MX24] Tomoyuki Morimae and Keita Xagawa. Quantum group actions, 2024.

[MY24] Tomoyuki Morimae and Takashi Yamakawa. One-Wayness in Quantum Cryptography. In Frédéric Magniez and Alex Bredariol Grilo, editors, *19th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2024)*, volume 310 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:21, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[Pie12] Krzysztof Pietrzak. Cryptography from learning parity with noise. In *Proceedings of the 38th International Conference on Current Trends in Theory and Practice of Computer Science*, SOFSEM'12, page 99–114, Berlin, Heidelberg, 2012. Springer-Verlag.

[PQS26] Alexander Poremba, Yihui Quek, and Peter Shor. The Learning Stabilizers with Noise Problem. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 108:1–108:19, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Pra62] E. Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[PRV26] Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan. Cloning Games, Black Holes and Cryptography. In Shubhangi Saraf, editor, *17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 109:1–109:21, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Reg03] Oded Regev. Quantum computation and lattice problems, 2003.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), September 2009.

[Reg24] Oded Regev. An efficient quantum factoring algorithm, 2024.

[Rob22] Damien Robert. Breaking SIDH in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sat26] Or Sattath. Microcrypt zoo. https://sattath.github.io/microcrypt-zoo/, 2026. Accessed: 2026-02-08.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Smi06] Graeme Stewart Baird Smith. *Upper and lower bounds on quantum codes*. PhD thesis, California Institute of Technology, USA, 2006. AAI3235592.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In *Proceedings of the 3rd International Colloquium on Coding Theory and Applications*, page 106–113, Berlin, Heidelberg, 1988. Springer-Verlag.

[vdB21] Ewout van den Berg. A simple method for sampling random Clifford operators, 2021.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[WKB10] Mark M. Wilde, Hari Krovi, and Todd A. Brun. Convolutional entanglement distillation. In *2010 IEEE International Symposium on Information Theory*, page 2657–2661. IEEE, June 2010.

[YK17] Beni Yoshida and Alexei Kitaev. Efficient decoding for the Hayden-Preskill protocol, 2017.

[YZ16] Yu Yu and Jiang Zhang. Cryptography with auxiliary input and trapdoor from constant-noise LPN. In *Annual International Cryptology Conference*, pages 214–243. Springer, 2016.

[YZ20] Yu Yu and Jiang Zhang. Smoothing out binary linear codes and worst-case sub-exponential hardness for LPN. Cryptology ePrint Archive, Paper 2020/870, 2020.

[YZW+19] Yu Yu, Jiang Zhang, Jian Weng, Chun Guo, and Xiangxue Li. Collision resistant hashing from sub-exponential learning parity with noise. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–24. Springer, 2019.

A Further discussion of LPN

For completeness, we here give a formal definition of LPN and give a simple reduction from $\mathsf{LPN}(k, n, p)$ to $\mathsf{LPN}(k - k', n, p)$, where $k' = O(\log n)$.

Definition A.1 (Decision Learning Parity with Noise, LPN)**.** For positive integers n, k and $p \in (0, 1)$, let $\mathbf{A} \sim \mathbb{Z}_2^{n\times k}$, $\mathbf{x} \sim \mathbb{Z}_2^k$, and $\mathbf{e} \sim \mathsf{Ber}_p^{\otimes n}$, i.e. each e_i is i.i.d. 1 with probability p and 0 with probability $1-p$. Let $\mathbf{u} \sim \mathbb{Z}_2^n$. Here $\mathbf{A}$, $\mathbf{x}$, and $\mathbf{u}$ are uniformly random. $\mathsf{LPN}(k, n, p)$ is the task of distinguishing between the two distributional samples

$$(\mathbf{A}, \mathbf{A}\mathbf{x} + \mathbf{e}) \quad \text{or} \quad (\mathbf{A}, \mathbf{u} \sim \mathbb{Z}_2^n) \tag{36}$$

with advantage at least $1/\operatorname{poly}(n)$. The former case is called *structured* and the latter *unstructured*.

Lemma A.2 (Reducing a logical bit in LPN)**.** *Let $p \in (0, 1)$ and positive integers k, k', n satisfy $k > k'$ and $k \le \operatorname{poly}(n)$. Let $\mathcal{O}$ be an oracle which solves Decision $\mathsf{LPN}(k - k', n, p)$ with advantage δ. Then there is an algorithm $\mathcal{A}$, using $O(\operatorname{poly}(n))$ time apart from the oracle call, which solves Decision $\mathsf{LPN}(k, n, p)$ with advantage $\delta/2^{k'}$ using a single call to $\mathcal{O}$.*

Proof. Let the Decision $\mathsf{LPN}(k, n, p)$ instance be $(\mathbf{A} \sim \mathbb{Z}_2^{n\times k}, \mathbf{u})$. Define $\mathbf{A}' \in \mathbb{Z}_2^{n\times(k-k')}$ by discarding the last k' columns of $\mathbf{A}$, and define $\bar{\mathbf{A}} \in \mathbb{Z}_2^{n\times k'}$ to be the last k' columns of $\mathbf{A}$. The algorithm will run $\mathcal{O}$ on $(\mathbf{A}', \mathbf{u})$ and output its answer. Suppose that the LPN instance is structured, so $\mathbf{u} = \mathbf{A}\mathbf{x}+\mathbf{e}$ for $\mathbf{x} \sim \mathbb{Z}_2^k$ and $\mathbf{e} \sim \mathsf{Ber}_p^{\otimes n}$. Let $\mathbf{x} = (\mathbf{x}', \bar{\mathbf{x}})$ with dimensions $k - k'$ and k'. With probability $1/2^{k'}$, $\bar{\mathbf{x}} = \mathbf{0}$. Conditioned on this event, $(\mathbf{A}', \mathbf{u})$ is precisely a structured instance of $\mathsf{LPN}(k - k', n, p)$. Otherwise, $\bar{\mathbf{x}} \neq 0$ and $\mathbf{u} = \mathbf{A}'\mathbf{x}' + \bar{\mathbf{A}}\bar{\mathbf{x}} + \mathbf{e}$. But $\bar{\mathbf{A}}\bar{\mathbf{x}}$ is a uniformly random bitstring since the columns of $\bar{\mathbf{A}}$ are uniformly random and $\bar{\mathbf{x}} \neq \mathbf{0}$. Hence, $\mathbf{u}$ is independent from $\mathbf{A}'$ and marginally $\mathbf{u} \sim \mathbb{Z}_2^n$, i.e. $(\mathbf{A}', \mathbf{u})$ is an unstructured instance. Let $p_0 := \Pr[\mathcal{A} = \texttt{structured} \,|\, \texttt{structured}]$ and $p_1 := \Pr[\mathcal{A} = \texttt{structured} \,|\, \texttt{unstructured}]$. Define q_0, q_1 similarly for $\mathcal{O}$ as an oracle solving $\mathsf{LPN}(k - k', n, p)$. Then

$$p_0 = \frac{1}{2^{k'}} q_0 + \left(1 - \frac{1}{2^{k'}}\right) q_1, \quad p_1 = q_1. \tag{37}$$

By definition, the advantage of $\mathcal{A}$ is $\frac{|p_0-p_1|}{2}$, and by assumption, $\frac{|q_0-q_1|}{2} = \delta$. Consequently,

$$\frac{|p_0 - p_1|}{2} = \frac{1}{2^{k'}} \frac{|q_0 - q_1|}{2} = \frac{\delta}{2^{k'}} \tag{38}$$

as claimed. □

This proof implies a reduction from $\mathsf{LPN}(k, n, p)$ to $\mathsf{LPN}(k - k', n, p)$ for any $k' = O(\log n)$ logical bits.

B One-way function from high-noise stateLSN

We here construct a one-way function family (OWFF) such that any algorithm inverting the OWFF implies an algorithm solving stateLSN.

Definition B.1 (OWFF)**.** Let $\mathcal{F}_n := \{ f_I : \mathcal{D}_I \to \mathcal{R}_I \}_{I\in\mathcal{I}_n}$ be a collection of functions f_I from a domain set $\mathcal{D}_I$ to a range set $\mathcal{R}_I$, where I is an index drawn from an index set $\mathcal{I}_n$ which depends on the security parameter n. Then $\mathcal{F}_n$ is a *one-way function family* (OWFF) if the following conditions hold.

(1) There exists a classical algorithm $\mathsf{Gen}(1^n)$, running in time $O(\mathrm{poly}(n))$, which produces an index $I \in \mathcal{I}_n$.

(2) There exists a classical algorithm $\mathsf{Sample}(I)$ such that for any $I \in \mathcal{I}_n$, $\mathsf{Sample}(I)$ samples a uniformly random element of $\mathcal{D}_I$ in time $O(\mathrm{poly}(n))$.

(3) There exists a classical algorithm $\mathsf{Eval}(I, x)$ such that for any $I \in \mathcal{I}_n$ and any $x \in \mathcal{D}_I$, $\mathsf{Eval}(I, x)$ outputs $f_I(x) \in \mathcal{R}_I$ in time $O(\mathrm{poly}(n))$.

(4) For any (quantum or classical) algorithm $\mathcal{A}$ running in time $\mathrm{poly}(n)$,

$$\Pr_{\mathcal{A},I,x}[f_I(\mathcal{A}(I, f_I(x))) = f_I(x)] = \mathrm{negl}(n) \tag{39}$$

where in the randomness, $I \sim \mathsf{Gen}(1^n)$ and $x \sim \mathsf{Sample}(I)$.

The existence of OWFF is equivalent to the existence of a standard one-way function, which in turn implies pseudorandom generators, pseudorandom functions, and all other primitives of private-key cryptography [KL07]. Our OWFF construction is indexed by LSN instances, but we will show that its security is bounded below by that of stateLSN.

Construction B.2 (OWFF candidate from Search stateLSN)**.** *We instantiate a* OWFF *candidate based on Search* $\mathsf{stateLSN}(k, n, p)$ *as follows.*

- $\mathsf{Gen}(1^n)$ *samples the* LSN *matrices* $I = (\mathbf{A}, \mathbf{B})$.
- *Define* $\mathcal{D}_I = \mathbb{Z}_2^n \times \mathbb{Z}_2^k \times \mathbb{Z}_2^{m(n)}$, *where* $m(n) = \mathrm{poly}(n)$ *is a sufficiently large number of bits so as to enable a sample from* $\mathcal{D}_p^{\otimes n}$. $\mathsf{Sample}(I)$ *ignores* I *and outputs* $(\mathbf{r}, \mathbf{y}, \mathbf{s})$ *where* $\mathbf{r} \sim \mathbb{Z}_2^n$, $\mathbf{y} \sim \mathbb{Z}_2^k$, *and* $\mathbf{s} \sim \mathbb{Z}_2^{m(n)}$.
- $f_I(x) = f_{\mathbf{A},\mathbf{B}}(\mathbf{y}, \mathbf{r}, \mathbf{s}) = (\mathbf{A}, \mathbf{B}, \mathbf{Ar} + \mathbf{By} + \mathbf{e})$. *Here* $\mathbf{e}$ *is defined as follows. Let* $\mathcal{W}_d$ *be the set of length-*$2n$ *bitstrings representing* n*-qubit Paulis with weight at most* d. *We use* $\mathbf{s}$ *as a random seed to draw a sample from* $\mathcal{D}_p^{\otimes n}$. *If* $|\mathbf{e}| > 2.01np$ *then* Sample *instead outputs* $\mathbf{0}$ *for the error so as to remain in* $\mathcal{W}_{2.01np}$*; however, the Chernoff bound implies that this event occurs with probability* $\mathrm{negl}(n)$ *so long as* $np = \omega(\log n)$. *Since this function is given by matrix multiplication,* f_I *can be efficiently computed as required.*

We now show that inverting f_I with non-negligible probability is at least as hard as solving Search $\mathsf{LSN}(k, n, p)$, for any reasonable choice of k and p as functions of n.

Theorem B.3 (OWFF secured by stateLSN)**.** *Let* $\mathcal{F}$ *be the* OWFF *candidate in Construction B.2, with parameters* k, p *such that* $k = \omega(\log n)$ *and* $p = \omega(\frac{\log n}{n})$. *Further, with* $\delta := 4.03p$ *and* $R := k/n$, *assume that* (δ, R) *satisfies the quantum Gilbert-Varshamov bound*

$$H_2(\delta) + \delta \log 3 < 1 - R, \tag{40}$$

where $H_2(x) = -x \log x - (1 - x) \log(1 - x)$ *is the binary entropy. Suppose that there exists an algorithm* $\mathcal{A}$, *running in time* T, *such that*

$$\Pr_{\mathcal{A},I,x}[f_I(\mathcal{A}(I, f_I(x))) = f_I(x)] = \frac{1}{\mathrm{poly}(n)}. \tag{41}$$

Then there exists an algorithm $\mathcal{B}$, *running in time* $T + \mathrm{poly}(n)$, *which solves Search* stateLSN *with probability* $\frac{1}{2^k} + \frac{1}{\mathrm{poly}(n)} = \frac{1}{\mathrm{poly}(n)}$.

Proof. Let $(\mathbf{C}, \mathbf{EC}\,|0^{n-k}, \psi\rangle)$ be the $\mathsf{stateLSN}(k, n, p)$ instance given to $\mathcal{B}$. $\mathcal{B}$ first measures the syndrome, and chooses a uniformly random Pauli $\mathbf{P}_0$ with the same syndrome. Hence, $\mathbf{P}_0\mathbf{E}$ commutes with all stabilizers. Then, choose a uniformly random logical Pauli $\mathbf{L}$ and multiply onto $\mathbf{P}_0$. Let $\mathbf{A}_0 \in \mathbb{Z}_2^{2n\times n}$ be the matrix whose columns are symplectic representations of the $n-k$ stabilizers and k logical $\mathbf{Z}_i$ Paulis, and let $\mathbf{B}_0 \in \mathbb{Z}_2^k$ likewise represent the logical $\mathbf{X}_i$ Paulis. The symplectic representation of $\mathbf{LP_0}$ is given by $\mathbf{A}_0\mathbf{r}_0 + \mathbf{B}_0\mathbf{y}_0 + \mathbf{e}$, where $\mathbf{e} = \mathrm{Symp}(\mathbf{E})$, and $\mathbf{r}_0, \mathbf{y}_0$ are uniformly random. Choose random invertible matrices $\mathbf{Q}_1 \in \mathbb{Z}_2^{n\times n}$ and $\mathbf{Q}_2^{k\times k}$, and define $\mathbf{A} := \mathbf{A}_0\mathbf{Q}_1$, $\mathbf{B} := \mathbf{B}_0\mathbf{Q}_2$, $\mathbf{r} := \mathbf{Q}_1^{-1}\mathbf{r}_0$, and $\mathbf{y} := \mathbf{Q}_2^{-1}\mathbf{y}_0$. One can now check that these objects follow the distribution of a Search LSN sample $([\mathbf{A}\,|\,\mathbf{B}], \mathbf{Ar} + \mathbf{By} + \mathbf{e})$.

Next, $\mathcal{B}$ will set $I = (\mathbf{A}, \mathbf{B})$ and $f_I(x) = \mathbf{Ar} + \mathbf{By} + \mathbf{e}$ before running $\mathcal{A}$ on input $(I, f_I(x))$, yielding a guess

$$(\hat{\mathbf{r}}, \hat{\mathbf{y}}, \hat{\mathbf{e}}) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^k \times \mathcal{W}_{n\delta}, \tag{42}$$

where $\hat{\mathbf{e}}$ comes from a guess of the seed $\hat{\mathbf{s}}$ which is then deterministically mapped into a corresponding depolarizing error. By assumption, with probability at least $1/\operatorname{poly}(n)$,

$$\mathbf{A}\hat{\mathbf{r}} + \mathbf{B}\hat{\mathbf{y}} + \hat{\mathbf{e}} = \mathbf{Ar} + \mathbf{By} + \mathbf{e}. \tag{43}$$

Thus, $\mathbf{e} + \hat{\mathbf{e}} = \mathbf{A}(\hat{\mathbf{r}} + \mathbf{r}) + \mathbf{B}(\hat{\mathbf{y}} + \mathbf{y})$ commutes with all stabilizers. For (δ, R) satisfying the quantum Gilbert-Varshamov bound, a random n-qubit stabilizer code with rate $R = k/n$ has distance at least δn with probability $1 - \mathrm{negl}(n)$ [KLS25, PQS26, NC10]. Note that $|\hat{\mathbf{e}}|$ and $|\mathbf{e}|$ are both at most $2.01np$. Since the distance of the corresponding quantum stabilizer code is at least $4.03np$ (more than twice the error weight) with probability $1 - \mathrm{negl}(n)$, $\mathbf{e} + \hat{\mathbf{e}}$ cannot be a logical operator. Since $\mathbf{e} + \hat{\mathbf{e}}$ commutes with all stabilizers, it must itself be a stabilizer. Hence, by a union bound, with probability at least $\frac{1}{\operatorname{poly}(n)} - \mathrm{negl}(n) = \frac{1}{\operatorname{poly}(n)}$, $\hat{\mathbf{e}}$ differs from $\mathbf{e}$ by a stabilizer. Now, $\mathcal{B}$ can apply $\mathrm{Symp}^{-1}(\hat{\mathbf{e}})$ to the original noisy code state, yielding $\mathbf{C}\,|0^{n-k}, \psi\rangle$. Inverting $\mathbf{C}$, we recover $|\psi\rangle$ exactly. Thus, the total fidelity between our reconstructed state and $|\psi\rangle$ is at least $1/\operatorname{poly}(n)$ as desired. □

C Additional proofs

We here provide proofs which were deferred in the main text.

Proof of Lemma 4.3. We first check directly that the above construction preserves the symplectic inner product, and then show that this Clifford matrix produces a uniformly random basis of a uniformly random isotropic subspace of dimension $n-1$. In the edge case $\mathbf{C} = \mathbf{I}$, it is clearly symplectic. Otherwise, the sampling procedure constructed $\mathbf{C}$ as $\mathbf{\Pi C}_0$, so it suffices to show separately that $\mathbf{C}_0$ and $\mathbf{\Pi}$ are symplectic matrices. First, for $\mathbf{\Pi}$, we need to show that $(\mathbf{\Pi e}_i) \odot (\mathbf{\Pi e}_j) = 0$, $(\mathbf{\Pi f}_i) \odot (\mathbf{\Pi f}_j) = 0$, and $(\mathbf{\Pi e}_i) \odot (\mathbf{\Pi f}_j) = \delta_{ij}$. Once these relations are shown, by bilinearity of the inner product $\mathbf{\Pi}$ must be symplectic. However, since $\mathbf{\Pi}$ applies the *same* permutation on each pair $(\mathbf{e}_i, \mathbf{f}_i)$, these relations are immediate.

Meanwhile, we observe that $\mathbf{C}_0$ translates $\mathbf{e}_j$ and $\mathbf{f}_j$ by a multiple of $\mathbf{e}_1$ for any $j = 2, \ldots, n$. Their orthogonality relations with each other are therefore preserved, because $\mathbf{e}_1$ is orthogonal to each $\mathbf{e}_j$, $\mathbf{f}_j$, and to itself. Moreover, for any $j = 2, \ldots, n$, $\mathbf{C}_0\mathbf{e}_j$ and $\mathbf{C}_0\mathbf{f}_j$ do not include any $\mathbf{f}_1$, so they are also orthogonal to $\mathbf{C}_0\mathbf{e}_1 = \mathbf{e}_1$. Since $\mathbf{C}_0\mathbf{e}_1 = \mathbf{e}_1$, $(\mathbf{C}_0\mathbf{e}_1) \odot (\mathbf{C}_0\mathbf{e}_1) = 0$ as desired. It only remains to check the orthogonality relations for $\mathbf{C}_0\mathbf{f}_1$:

$$\mathbf{C}_0\mathbf{e}_1 \odot \mathbf{C}_0\mathbf{f}_1 = \mathbf{e}_1 \odot \mathbf{r}' = 1 \tag{44}$$

$$\mathbf{C}_0\mathbf{f}_i \odot \mathbf{C}_0\mathbf{f}_1 = (\mathbf{f}_i + (\mathbf{r}' \odot \mathbf{f}_i)\mathbf{e}_1) \odot \mathbf{r}' = 0 \quad \text{for } 2 \le i \le n, \tag{45}$$

$$\mathbf{C}_0\mathbf{e}_i \odot \mathbf{C}_0\mathbf{f}_1 = (\mathbf{e}_i + (\mathbf{r}' \odot \mathbf{e}_i)\mathbf{e}_1) \odot \mathbf{r}' = \delta_{i1} \quad \text{for } 2 \le i \le n \tag{46}$$

where we use in each equality that $\mathbf{e}_1 \odot \mathbf{r}' = 1$, since $r'_{n+1} = 1$. We conclude that $\mathbf{C}$ is symplectic, since both $\mathbf{C}_0$ and $\mathbf{\Pi}$ are.

Next, we argue that $\mathcal{R}_n$ maps a uniformly random basis of a random $(n-1)$-dimensional isotropic subspace orthogonal to $\mathbf{f}_1$ and not containing $\mathbf{f}_1$ to (up to negligible total variation distance) a uniformly random basis of a random $(n-1)$-dimensional isotropic subspace. For any $\mathbf{w} \neq 0$, let

$$S_{\mathbf{w}} = \{(\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}) \mid (\mathbf{u}_i) \text{ basis for isotropic } V \subseteq \mathbb{Z}_2^{2n}, \mathbf{w} \in V^\perp \setminus V\}. \tag{47}$$

Condition on the existence of a pivot k, an event of probability $1-2^{-n}$. Then, $\mathbf{C}$ maps $S_{\mathbf{f}_1}$ bijectively to $S_{\mathbf{r}}$, with inverse $\mathbf{C}^{-1}$ (in particular, all $S_{\mathbf{w}}$ have the same cardinality). Hence, since $(\mathbf{v}_1, \ldots, \mathbf{v}_{n-1})$ is a uniformly random element of $S_{\mathbf{f}_1}$, $(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1})$ is a uniformly random element of $S_{\mathbf{r}}$. Under this conditioning, $\mathbf{r}$ is uniformly random over vectors with $r_{n+i} = 1$ for some $1 \leq i \leq n$, so its distribution is within total variation distance 2^{-n} of a uniformly random nonzero vector. Hence, $(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1})$ is statistically indistinguishable from a random element $(\mathbf{u}_1, \ldots, \mathbf{u}_{n-1})$ of a uniformly randomly $S_{\mathbf{w}}$.

But notice that any basis $(\mathbf{u}_1, \ldots, \mathbf{u}_{n-1})$ of any isotropic V is included in exactly $2^{n+1} - 2^{n-1}$ sets $S_{\mathbf{w}}$—one for each $\mathbf{w} \in V^\perp \setminus V$. Each $S_{\mathbf{w}}$ has exactly the same cardinality, and every $(\mathbf{u}_1, \ldots, \mathbf{u}_{n-1})$ is present in exactly $2^{n+1} - 2^{n-1}$ of these sets. It follows that a random element of a randomly selected $S_{\mathbf{w}}$ is identical in distribution to a uniformly random element of

$$S = \{(\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}) \mid (\mathbf{u}_i) \text{ basis for isotropic } V \subseteq \mathbb{Z}_2^{2n}\}. \tag{48}$$

Removing the conditioning changes the distribution by at most 2^{-n} in total variation distance. Every $(n-1)$-dimensional isotropic subspace has exactly the same number of bases, so we conclude that $(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1})$ has negligible total variation distance from a uniformly random basis of a uniformly random $(n-1)$-dimensional isotropic subspace V. □

Proof of Lemma 4.4. Sample $T \sim \mathsf{Bin}(n, \frac{4}{3}q)$, so that $\mathbb{E}[T] = \frac{4}{3}nq \geq \frac{4}{3}m$. We use the Chernoff bound on the binomial distribution, i.e. for $X \sim \mathsf{Bin}(n,p)$, $\Pr[X \leq (1-\delta)\mathbb{E}[X]] \leq \exp\left(-\delta^2\mathbb{E}[X]/2\right)$. Thus,

$$\Pr[T \leq m] \leq \Pr[T \leq \tfrac{3}{4}\mathbb{E}[T]] \leq \exp\left(() - \mathbb{E}[T]/32\right) \leq \exp\left(() - m/24\right) = \mathrm{negl}(n) \tag{49}$$

because $m = \omega(\log n)$. If $T < m$, output $\mathbf{e}' = \mathbf{0}$. Otherwise, proceed as follows. Sample $\mathbf{e}'$ by choosing T indices, including the m indices in M and $T-m$ arbitrary others; on each chosen index j, sample (e'_j, e'_{n+j}) independently from $\mathcal{D}_{3/4}$, and set all other pairs to $(0,0)$. Now, $\mathbf{e} + \mathbf{e}' \sim \mathbf{e}'$ since the noise in $\mathbf{e}'$ manifestly subsumes the noise in $\mathbf{e}$. Next, the random permutation π scrambles any index asymmetry. Conditioned on $T \geq m$, the random permutation makes the chosen index set uniform among all T-element subsets. Without this conditioning, sampling $T \sim \mathsf{Bin}(n, \frac{4}{3}q)$ and then a uniform T-element subset is equivalent to selecting each index independently with probability $\frac{4}{3}q$; placing independent $\mathcal{D}_{3/4}$ noise at the selected indices therefore gives $\mathcal{D}_q^{\otimes n}$. The actual output and this comparison distribution can be coupled to agree whenever $T \geq m$. Thus, the total variation distance between the law of $\pi(\mathbf{e} + \mathbf{e}')$ and $\mathcal{D}_q^{\otimes n}$ is at most $\Pr[T < m] = \mathrm{negl}(n)$. □

Proof of Theorem 5.2. Let $\mu \in \{0,1\}$ be any message bit. Suppose that $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$ and $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mu)$. We can parse the two keys as $\mathsf{pk} = (\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{x} + \mathbf{e})$ and $\mathsf{sk} = \mathbf{x}$, and we can parse the ciphertext as $\mathsf{ct} = (\mathbf{f} \odot \mathbf{A}, \mathbf{f} \odot \mathbf{b} + \mu)$, for some $\mathbf{e}, \mathbf{f} \sim \mathcal{D}_p^{\otimes n}$. Then, the output of $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ on input $\mathsf{ct} = (\mathbf{u}, c)$ is

$$c + \mathbf{u} \cdot \mathbf{x} = \mathbf{f} \odot \mathbf{b} + \mu + (\mathbf{f} \odot \mathbf{A}) \cdot \mathbf{x} = \mathbf{f} \odot \mathbf{A}\mathbf{x} + \mathbf{f} \odot \mathbf{e} + \mu + \mathbf{f} \odot \mathbf{A}\mathbf{x} \tag{50}$$

$$= \mu + \mathbf{f} \odot \mathbf{e} \pmod 2, \tag{51}$$

where we used that $(\mathbf{f} \odot \mathbf{A}) \cdot \mathbf{x} = \mathbf{f} \odot (\mathbf{A} \cdot \mathbf{x})$. Therefore, it suffices to show that for appropriate choices of $p \in (0,1)$, $\mathbf{f} \odot \mathbf{e} = 0$ with high probability.

Recall that $\mathbf{e}, \mathbf{f}$ are two independent depolarizing errors, so we may express $\mathbf{e} = (\mathbf{a}, \mathbf{b})$ where (a_i, b_i) are i.i.d. (over i) distributed such that $(0,0)$ occurs with probability $1-p$ and the remaining 3 possibilities $(1,0), (0,1), (1,1)$ occur each with probability $p/3$. Similarly, express $\mathbf{f} = (\mathbf{a}', \mathbf{b}')$. Thus,

$$\mathbf{e} \odot \mathbf{f} = \sum_{i=1}^{n} a_i b_i' + a_i' b_i. \tag{52}$$

Note that $a_i b_i' + a_i' b_i = 1$ occurs with probability $r := \frac{2}{3}p^2$, since there are six possible ways to satisfy $a_i b_i' + a_i' b_i = 1$, each occurring with probability $(p/3)^2 = p^2/9$. Hence, $a_i b_i' + a_i' b_i \sim \mathsf{Ber}(r)$, and $\Pr[\mathbf{e} \odot \mathbf{f} = 0]$ is precisely the probability that a $\mathsf{Bin}(n, r)$ random variable is even. The latter probability is well-known to be $\frac{1}{2} + \frac{1}{2}(1-2r)^n$, so

$$\Pr[\mathbf{e} \odot \mathbf{f} = 0] = \frac{1}{2} + \frac{1}{2}\left(1 - \frac{4}{3}p^2\right)^n \geq \frac{1}{2} + \frac{1}{2}\exp\left(-\frac{n\frac{4}{3}p^2}{1-\frac{4}{3}p^2}\right) \tag{53}$$

by the standard inequality $\ln(1-x) \geq -\frac{x}{1-x}$ for $x \in (0,1)$. Thus, for any $\delta > 0$, we can choose $p = \Theta\left(1/\sqrt{n}\right)$ such that the scheme is $1-\delta$ correct. □

Justification of the amplification remark. Except with negligible probability over key generation, $w_P(\mathbf{e}) \leq 2np$. Conditional on any such $\mathbf{e}$, the repetitions decrypt independently with success probability $\frac{1}{2} + \frac{1}{2}(1-\frac{4}{3}p)^{w_P(\mathbf{e})} = \frac{1}{2} + \Omega(1)$. A Chernoff bound therefore gives negligible majority error for $2\lceil \log^2 n \rceil + 1$ repetitions. IND-CPA security follows by a standard hybrid argument, and key generation is unchanged. □

D Barriers to a reduction from sympLPN to LPN

It is known that there exists a reduction from $\mathsf{LPN}(k, 2n, p/6)$ to $\mathsf{sympLPN}(n, n, p)$, for $k = \lfloor pn/6 \rfloor$ [KLP+26]. This reduction is only meaningful for certain regimes of p. $\mathsf{LPN}(k, n, p)$ is easy for any $p = O(k^{-1})$, as a $k \times k$ sub-block of the encoding matrix has substantial probability of experiencing no error at all, and thus being directly invertible. Meanwhile, when $p = \Omega(k^{-c})$ for $c < 1$, there is no known algorithm that runs in polynomial time in k. It follows that the reduction from LPN to sympLPN gives a strong lower bound on the hardness of sympLPN when $p = \Omega\left(n^{-c}\right)$ for $c < 1/2$. However, in the regime for our proposed PKE and OT schemes, $p = \Theta\left(n^{-1/2}\right)$, so the reduction becomes vacuous. It is therefore open as to whether sympLPN-based schemes inherit security from the hardness of LPN.

A more pressing concern one might raise with low-noise sympLPN-based proposals is, on the other hand, the possibility of a *converse* reduction from sympLPN to LPN with $p = \Theta(1/\sqrt{n})$. If such a reduction exists, then any low-noise sympLPN-based scheme is no more secure than one based off of low-noise LPN. We here show that there are significant barriers to natural linear reductions from $\mathsf{sympLPN}(n, p)$ to LPN. Thus, despite their similarities, low-noise LPN and sympLPN are not currently known to be reducible to one another. It is unknown as to how the security of the two cryptographic hardness assumptions rigorously compare in theory and in practice.

Given a sample of sympLPN, $(\mathbf{A}, \mathbf{r})$, where $\mathbf{r}$ is either of the form $\mathbf{Ax} + \mathbf{e}$ or $\mathbf{u}$, a natural class of reductions would proceed by preparing

$$(\mathbf{BA}, \mathbf{Br}), \tag{54}$$

where $\mathbf{B} \in \mathbb{Z}_2^{m \times 2n}$ is sampled using $\mathbf{A}$ and fresh randomness. If $\mathbf{r} = \mathbf{u}$, then $\mathbf{Br}$ is uniformly random as long as $\mathbf{B}$ has full row rank; if $\mathbf{r} = \mathbf{Ax} + \mathbf{e}$ then $\mathbf{Br} = \mathbf{BAx} + \mathbf{Be}$. If one could show that $\mathbf{BA}$ were statistically close to a uniform distribution, while $\mathbf{Be}$ were independent Bernoulli noise, independent of $\mathbf{BA}$, then this approach would constitute a reduction from $\mathsf{sympLPN}$ to LPN. We focus on the regime $m \geq cn$ for a fixed $c > 1$. (If we allowed $m \leq n$, then one could simply set $\mathbf{B}$ to remove the last $(1+\delta)n$ rows of $\mathbf{A}$ for any constant $\delta \in (0,1)$ with $(1-\delta)n \in \mathbb{N}$. Then $\mathbf{BA} \in \mathbb{Z}_2^{(1-\delta)n \times n}$ is indeed close to uniformly random, but produces an information-theoretically unsolvable instance of LPN.)

It is not clear at all, a priori, that such a reduction would not exist. A random isotropic code $\mathbf{A} \in \mathbb{Z}_2^{2n \times n}$ has roughly $\frac{3}{2}n^2$ bits of entropy, since there are $\binom{n}{2}$ symplectic orthogonality conditions between the pairs of columns. Hence, choosing $m = cn$ for $1 < c < \frac{3}{2}$, it is a priori possible that even for some fixed $\mathbf{B}$, $\mathbf{BA}$ could be statistically indistinguishable from a uniform distribution. However, we demonstrate that the random variable $\mathbf{A}$ cannot be randomized in this manner—in fact, $\mathbf{BA}$ for any fixed $\mathbf{B}$ is severely deficient in entropy. In what follows, let $H(X)$ denote the entropy of a random variable X.

Theorem D.1. *Let $m \geq cn$ for $c > 1$. Then there exists a constant $d > 0$, such that for sufficiently large n and any fixed choice of $\mathbf{B} \in \mathbb{Z}_2^{m \times 2n}$, $H(\mathbf{BA}) \leq (1-d)mn$.*

This is a strong bound because we require $\mathbf{BA}$ to be close in total variation distance to a uniformly random $m \times n$ matrix in the reduction to $\mathsf{LPN}(n, m, p')$. To satisfy this closeness, $\mathbf{BA}$ must have entropy negligibly close to mn. But by Theorem D.1, any fixed $\mathbf{B}$ is off in entropy by at least a constant factor, and thus $\mathbf{B}$ itself must be chosen from a distribution random enough to supplement $\Omega(n^2)$ bits of entropy. Intuitively, when $\mathbf{B}$ has that much entropy, it cannot possibly be very sparse, and therefore it should be forced to blow up the error $\mathbf{Be}$ in the transformed codeword $(\mathbf{BA})\mathbf{x} + \mathbf{Be}$, beyond even the information-theoretic decoding limit perhaps. However, placing this intuition on rigorous grounds to prove the implication requires additional technical subtlety. We show that randomizing $\mathbf{BA}$ forces $\mathbf{Be}$ to have large expected weight. At constant rate, making the errors independent by adding fresh noise then leaves too much noise for reliable decoding.

This result holds for $\mathsf{sympLPN}$ with error rate $p = \omega(1/n)$. If $p = O(1/n)$, then there is a polynomial-time brute-force error enumeration algorithm to solve $\mathsf{sympLPN}(n, n, p)$, so this ultra-low-noise regime is of no cryptographic interest.

Theorem D.2. *Let $m = \mathrm{poly}(n)$ with $m > cn$ for some $c > 1$, and let $p = \omega(1/n)$ with $0 < p \leq 3/4$. Suppose that $\mathbf{B} \in \mathbb{Z}_2^{m \times 2n}$ is a random variable such that $\mathbf{BA} \in \mathbb{Z}_2^{m \times n}$ is statistically indistinguishable from uniformly random. Fix any $\delta > 0$ and let $r := n/m$ be the rate of the transformed code $\mathrm{im}(\mathbf{BA})$. Then $|\mathbf{Be}|$, the weight of the distorted error, satisfies*

$$\Pr_{\mathbf{B}}\left[\mathop{\mathbb{E}}_{\mathbf{e} \sim \mathcal{D}_p^{\otimes n}}[|\mathbf{Be}|] \geq \left(\frac{1-r-\delta}{2}\right) m\right] \geq 1 - \mathrm{negl}(n). \tag{55}$$

In other words, this theorem states that if $\mathbf{B}$ can randomize the code distribution well, $\mathbf{Be}$ has expected weight lower bounded by $(\frac{1-r-\delta}{2})m$ for any $\delta > 0$. For $m = O(n)$, we can interpret this as a strong barrier on decoding. Indeed, $\frac{1-r}{2} > H_2^{-1}(1-r)$ for any $r \in (0,1)$, where $H_2(x) := -x \log x - (1-x)\log(1-x)$ is the binary entropy. For independent Bernoulli noise of rate p', Shannon's noisy coding converse rules out reliable decoding when $H_2(p') > 1 - r$. By Lemma D.9, each bit of $\mathbf{Be}$ has probability at most $1/2$ of being 1, so adding noise independent of $\mathbf{e}$ conditional on $(\mathbf{A}, \mathbf{B})$ cannot decrease its expected weight. Thus, if the resulting error is, jointly with $\mathbf{BA}$, negligibly close to independent $\mathsf{Ber}(p')^{\otimes m}$ noise with $p' \leq 1/2$, then $p' \geq (1-r-\delta)/2 - \mathrm{negl}(n) > H_2^{-1}(1-r)$ for sufficiently small fixed $\delta > 0$ in the constant-rate regime.

When $m = \omega(n)$, the result shows that the output error has expected relative weight at least $\frac{1}{2} - \delta$ for any constant δ, since $r = o(1)$. This bound is not sufficient to fully rule out decodability. We believe that it should be possible to do so for any $m = \text{poly}(n)$—however, the primary case of interest for the result was to rule out a reduction where $m = (1+\epsilon)n$, i.e. when the number of rows decreased rather than increasing. It seems unlikely that reductions that resort to adding many more rows will do a better job of randomizing the code instance without amplifying the error.

In order to prove these theorems, we will begin by introducing new notions in symplectic linear algebra and establishing basic lemmas that will be necessary for the proofs. First, we define the *radical* of a vector space $V \subseteq \mathbb{Z}_2^{2n}$.

Definition D.3. For a vector space $V \subseteq \mathbb{Z}_2^{2n}$, define the *radical* $\text{rad}(V) := V \cap V^\perp$, i.e. it is the set of all vectors $\mathbf{v} \in V$ such that $\mathbf{v} \odot \mathbf{w} = 0$ for any $\mathbf{w} \in V$.

For example, $\text{rad}(\mathbb{Z}_2^{2n}) = \{\mathbf{0}\}$, and $\text{rad}(\text{span}(\{\mathbf{v}\})) = \text{span}(\{\mathbf{v}\})$, since $\mathbf{v}$ is always symplectically orthogonal to itself.

We will now prove an upper bound on the dimension of $\text{rad}(V)$ for a uniformly random $V \subseteq \mathbb{Z}_2^{2n}$ of a given dimension. In order to do so, we first establish that a random vector space $V \subseteq \mathbb{Z}_2^{2n}$ is very unlikely to be isotropic.

Lemma D.4 (Random subspaces are not isotropic)**.** *Let $\epsilon > 0$ be a constant. If $V \subseteq \mathbb{Z}_2^{2n}$ is a random subspace of dimension $m \geq \epsilon n$, then there exists a constant $\delta > 0$ so that, for all sufficiently large n,*

$$\Pr[V \subseteq V^\perp] \leq 2^{-\delta n^2}. \tag{56}$$

Proof. If $m > n$, the probability is zero, so assume $m \leq n$. Instead of V, we consider a random matrix $\mathbf{M}$ formed by the following random process: new uniformly random (linearly independent) columns are added to $\mathbf{M}$ until it has dimension m. The span of such a random matrix is a uniformly random subspace, since it is obtained by repeatedly adding new random vectors to a given subspace. However, the chance that the result is isotropic is at most $2^{-\delta_0 m^2}$ for some $\delta_0 > 0$. Indeed, say that k columns have been added to $\mathbf{M}$ and their span is isotropic. Then, the chance that the subsequent column lies in the symplectic dual of the previous ones is $\frac{2^{2n-k}-2^k}{2^{2n}-2^k}$, because the current column span has dimension k (none of the vectors in this span can be added) and the symplectic dual has dimension $2n-k$. Since $m \leq n$ for any isotropic vector space, the value of k must satisfy $k < n$, and therefore

$$\frac{2^{2n-k}-2^k}{2^{2n}-2^k} \leq \frac{2^{2n-k}}{2^{2n}-2^k} \leq 2\frac{2^{2n-k}}{2^{2n}} = \frac{1}{2^{k-1}}. \tag{57}$$

Taking the product of these values from $k = 1$ to $k = m-1$ (the probability is exactly 1 for $k = 0$) yields $2^{-\frac{(m-1)(m-2)}{2}}$. In particular, since $m \geq \epsilon n$, there exists some δ for which $\delta n^2 \leq \frac{(m-1)(m-2)}{2}$ for all sufficiently large n, and therefore $2^{-\delta n^2} \geq 2^{-\frac{(m-1)(m-2)}{2}}$. □

We also record a standard result on the number of subspaces V satisfying $U \subseteq V \subseteq W$ of fixed dimension.

Lemma D.5 (Number of sandwiched subspaces)**.** *There exist constants $C_1, C_2 > 0$ such that for any vector spaces $U \subseteq W$ over $\mathbb{Z}_2$ of respective dimensions k and m, the number N of vector spaces V of dimension l with $k \leq l \leq m$ for which $U \subseteq V \subseteq W$ satisfies*

$$C_1 2^{(l-k)(m-l)} \leq N \leq C_2 2^{(l-k)(m-l)}. \tag{58}$$

Using the previous two lemmas, we may bound the size of $\mathrm{rad}(V)$ for a random subspace V of fixed dimension. Recall that if $W \subseteq \mathbb{Z}_2^{2n}$ has dimension t, then $\dim(W^\perp) = 2n - t$.

Lemma D.6 (Dimension of a random radical)**.** *Let $\epsilon > 0$ and $\alpha > 0$ be constants. If $V \subseteq \mathbb{Z}_2^{2n}$ is a random subspace of dimension $m \geq \alpha n$, then there exists a constant $\delta > 0$ such that, for all sufficiently large n,*

$$\Pr[\dim(\mathrm{rad}(V)) \geq \epsilon n] \leq 2^{-\delta n^2}. \tag{59}$$

Proof. Let $k = \lceil \epsilon n \rceil$. If $k > \min\{m, 2n - m\}$, the probability is zero; otherwise, assume $k \leq m \leq 2n - k$. A vector space V has radical of dimension at least ϵn if and only if there is some isotropic subspace W with dimension k such that $W \subseteq V \subseteq W^\perp$. Indeed, a subspace $W \subseteq V$ is contained in the radical of V if and only if $V \subseteq W^\perp$, i.e. every vector in W is orthogonal to every vector in V.

The number N_k^{iso} of isotropic vector spaces of dimension k, by lemma D.4 and lemma D.5, satisfies $N_k^{\mathrm{iso}} \leq C_2 2^{k(2n-k)-\delta' n^2}$ for some $\delta' > 0$. Meanwhile, for some fixed isotropic W of dimension k, let M be the number of vector spaces V for which $W \subseteq V \subseteq W^\perp$. By lemma D.5, since $\dim(W^\perp) = 2n - k$, $M \leq C_2 2^{(m-k)(2n-m-k)}$. It follows that the number of vector spaces V of dimension m with radical of dimension at least k has upper bound

$$M N_k^{\mathrm{iso}} \leq C_2^2 2^{k(2n-k)+(m-k)(2n-m-k)-\delta' n^2}. \tag{60}$$

Meanwhile, the total number of vector spaces N_m of dimension m satisfies the lower bound $C_1 2^{m(2n-m)} \leq N_m$. Hence, the fraction of vector spaces V of dimension m with radical of dimension at least k is at most

$$\frac{M N_k^{\mathrm{iso}}}{N_m} \leq \frac{C_2^2}{C_1} 2^{k(2n-k)+(m-k)(2n-m-k)-m(2n-m)-\delta' n^2} \tag{61}$$

$$= D 2^{-\delta' n^2}, \tag{62}$$

where $D := \frac{C_2^2}{C_1}$. This shows that a randomly sampled V of dimension m has a radical of dimension at least ϵn with probability at most $D 2^{-\delta' n^2}$. Taking $\delta = \delta'/2$, we have $D 2^{-\delta' n^2} \leq 2^{-\delta n^2}$ for all sufficiently large n, giving the desired result. □

With these lemmas, we can now prove a technical result that will be instrumental for Theorem D.1.

Lemma D.7 (Symmetrized product of random matrices is nearly full rank)**.** *Let $\epsilon > 0$ be a constant. Say that $\mathbf{C}, \mathbf{B}$ are independent, uniformly random $m \times n$ matrices, such that $\alpha n \leq m \leq n$ for some constant $\alpha \in (1/2, 1)$. Then for sufficiently large n, there exists a constant $\delta > 0$ such that*

$$\Pr[\mathrm{rank}(\mathbf{C}^\intercal \mathbf{B} + \mathbf{B}^\intercal \mathbf{C}) \leq (1 - \epsilon) n] \leq 2^{-\delta n^2}. \tag{63}$$

Proof. It suffices to prove the claim for $0 < \epsilon < 1$. Express

$$\mathbf{C}^\intercal \mathbf{B} + \mathbf{B}^\intercal \mathbf{C} = \begin{bmatrix} \mathbf{C}^\intercal & \mathbf{B}^\intercal \end{bmatrix} \begin{bmatrix} 0 & \mathbf{I} \\ \mathbf{I} & 0 \end{bmatrix} \begin{bmatrix} \mathbf{C} \\ \mathbf{B} \end{bmatrix} \tag{64}$$

We first may note that $\mathbf{T} := \begin{bmatrix} \mathbf{C} \\ \mathbf{B} \end{bmatrix} \in \mathbb{Z}_2^{2m \times n}$ is uniformly random, and therefore since $2m \geq n$ it has rank at least $\left(1 - \frac{\epsilon}{2}\right) n$ with probability at least $1 - 2^{-\delta_0 n^2}$ for some $\delta_0 > 0$. To see this, note that in order for $\mathbf{T}$ to have rank less than $(1 - \frac{\epsilon}{2})n$, then there must be at least $\frac{\epsilon n}{2}$ columns that are contained in the span of the previous columns (whose rank is bounded by $(1 - \frac{\epsilon}{2})n$). For any fixed

set of $\lceil \epsilon n/2 \rceil$ column positions, the probability that each of these columns lies in the span of its predecessors while that span has dimension less than $(1-\epsilon/2)n$ is at most $2^{-\epsilon^2 n^2/4}$. Taking a union bound over at most 2^n choices of these positions gives a rank-failure probability at most $2^{n-\epsilon^2 n^2/4}$. Hence, setting $\delta_0 = \epsilon^2/8$ yields the desired bound for sufficiently large n.

Therefore, with this probability, $W := \mathrm{im}(\mathbf{T}) \subseteq \mathbb{Z}_2^{2m}$ has dimension at least $\left(1-\frac{\epsilon}{2}\right)n$. Let $t = \dim(W)$, and note that W is a uniformly random subspace with dimension t. We must now bound the dimension of $\mathrm{rad}(W)$, because this dimension constrains the rank of $\mathbf{C}^\intercal\mathbf{B} + \mathbf{B}^\intercal\mathbf{C}$. Indeed, say that some vector $\mathbf{u}$ satisfies $(\mathbf{C}^\intercal\mathbf{B} + \mathbf{B}^\intercal\mathbf{C})\mathbf{u} = 0$. Then, by Eqn. (64) this is equivalent to $(\mathbf{T}\mathbf{u}') \odot (\mathbf{T}\mathbf{u}) = 0$ for any $\mathbf{u}'$, i.e. that $\mathbf{T}\mathbf{u} \in \mathrm{rad}(W)$. It follows that with probability at least $1 - 2^{-\delta_0 n^2}$,

$$\dim(\ker(\mathbf{C}^\intercal\mathbf{B} + \mathbf{B}^\intercal\mathbf{C})) = \dim(\mathrm{rad}(W)) + \dim(\ker(\mathbf{T})) \tag{65}$$

$$\leq \dim(\mathrm{rad}(W)) + \frac{\epsilon}{2}n, \tag{66}$$

by the rank-nullity theorem. By Lemma D.6, there exists some δ_1 for which the probability that $\dim(\mathrm{rad}(W)) \geq \frac{\epsilon}{2}n$ is at most $2^{-\delta_1 n^2}$. Choosing $\delta < \min(\delta_0, \delta_1)$, we have that $2^{-\delta_0 n^2} + 2^{-\delta_1 n^2} \leq 2^{-\delta n^2}$ for sufficiently large n as claimed. □

With the tools in place, we may now prove Theorem D.1. Before we give the proof, we recall the existence of a standard, useful basis for any subspace $V \subseteq \mathbb{Z}_2^{2n}$. The standard symplectic basis $\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{f}_1, \ldots, \mathbf{f}_n$ of $\mathbb{Z}_2^{2n}$ has convenient orthogonality relations: $\mathbf{e}_i \odot \mathbf{e}_j = 0$, $\mathbf{f}_i \odot \mathbf{f}_j = 0$, and $\mathbf{e}_i \odot \mathbf{f}_j = \delta_{ij}$. For a general V, there is a similar convenient basis.

Lemma D.8 (Symplectic basis of a subspace)**.** *Let $V \subseteq \mathbb{Z}_2^{2n}$ be a subspace. There exists a basis $\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_1, \ldots, \mathbf{v}_l, \mathbf{w}_1, \ldots, \mathbf{w}_l$ such that*

(1) $\mathbf{u}_i \in V^\perp$ *for* $i = 1, \ldots, k$.

(2) $\mathbf{v}_i \odot \mathbf{v}_j = 0$ *for* $i, j = 1, \ldots, l$.

(3) $\mathbf{w}_i \odot \mathbf{w}_j = 0$ *for* $i, j = 1, \ldots, l$.

(4) $\mathbf{v}_i \odot \mathbf{w}_j = \delta_{ij}$ *for* $i, j = 1, \ldots, l$.

This basis is almost precisely analogous to $(\mathbf{e}_i, \mathbf{f}_i)$ in the case of $\mathbb{Z}_2^{2n}$—the $\mathbf{v}_i$ correspond to the $\mathbf{e}_i$, while the $\mathbf{w}_i$ correspond to the $\mathbf{f}_i$. The additional vectors $\mathbf{u}_i$ give a basis for $\mathrm{rad}(V)$.

Proof of Theorem D.1. Let $\mathcal{S}$ denote the set of $2n \times n$ isotropic matrices, and let $F_{\mathbf{B}} = \{\mathbf{B}\mathbf{A} \mid \mathbf{A} \in \mathcal{S}\}$. We will start by showing that for some constant $d' > 0$, for any $\mathbf{B}$, $|F_{\mathbf{B}}| \leq 2^{mn - d'n^2}$. This implies that $H(\mathbf{B}\mathbf{A}) \leq mn - d'n^2$, and with a short additional argument we will conclude that $H(\mathbf{B}\mathbf{A}) \leq (1-d)mn$ for some $d > 0$. It suffices to consider $1 < c < 2$. We may also assume $m \leq 2n$ and that $\mathbf{B}$ has full row rank. Indeed, for $m \leq 2n$, extend a basis of the row space of $\mathbf{B}$ to m linearly independent rows; the original product $\mathbf{B}\mathbf{A}$ is a fixed linear image of the resulting product, so its support cannot be larger. For $m > 2n$, the case $\mathbf{B} = \mathbf{I}_{2n}$ gives $|F_{\mathbf{B}}| \leq |\mathcal{S}| \leq 2^{2n^2 - d'n^2} \leq 2^{mn - d'n^2}$ for every such $\mathbf{B}$. First, note that $|F_{\mathbf{B}}| = |F_{\mathbf{TBS}}|$, where $\mathbf{T}$ is any invertible $m \times m$ matrix, and $\mathbf{S} \in \mathbb{Z}_2^{2n \times 2n}$ is any matrix that preserves the symplectic inner product. Indeed, consider the map that takes $\mathbf{M} \in F_{\mathbf{B}}$ to $\mathbf{T}\mathbf{M}$. Writing $\mathbf{M} = \mathbf{B}\mathbf{A}$, $\mathbf{T}\mathbf{M} = (\mathbf{T}\mathbf{B}\mathbf{S})(\mathbf{S}^{-1}\mathbf{A})$, and hence $\mathbf{T}\mathbf{M} \in F_{\mathbf{TBS}}$ because $\mathbf{S}^{-1}\mathbf{A}$ is an isotropic matrix. Likewise, the inverse map $\mathbf{M} \mapsto \mathbf{T}^{-1}\mathbf{M}$ for $\mathbf{M} = (\mathbf{T}\mathbf{B}\mathbf{S})\mathbf{A}$ also places $\mathbf{T}^{-1}\mathbf{M} \in F_{\mathbf{B}}$. Thus, $|F_{\mathbf{B}}| = |F_{\mathbf{TBS}}|$.

Let $W := \ker(\mathbf{B}) \subseteq \mathbb{Z}_2^{2n}$. By Lemma D.8, W has a basis of the form $\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_1, \ldots, \mathbf{v}_l, \mathbf{w}_1, \ldots, \mathbf{w}_l$, where $\mathbf{v}_i \odot \mathbf{w}_j = \delta_{ij}$, $\mathbf{v}_i \odot \mathbf{v}_j = 0$, $\mathbf{w}_i \odot \mathbf{w}_j = 0$, and $\mathbf{u}_i \in W^\perp$. Let

$\mathbf{S}$ be a symplectic matrix which sends the standard symplectic basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_{l+k}, \mathbf{f}_1, \dots, \mathbf{f}_l$ to $\mathbf{v}_1, \dots, \mathbf{v}_l, \mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{w}_1, \dots, \mathbf{w}_l$. Then, $\ker(\mathbf{BS})$ is spanned by $\mathbf{e}_1, \dots, \mathbf{e}_{l+k}, \mathbf{f}_1, \dots, \mathbf{f}_l$, while $\mathrm{im}(\mathbf{BS})$ is spanned by the images of $\mathbf{e}_{l+k+1}, \dots, \mathbf{e}_n, \mathbf{f}_{l+1}, \dots, \mathbf{f}_n$. By choosing an appropriate invertible $\mathbf{T} \in \mathbb{Z}_2^{m \times m}$, we can construct a $\mathbf{P} = \mathbf{TBS}$ which is a projector onto this latter set of coordinates. As a consequence, $|F_{\mathbf{B}}| = |F_{\mathbf{P}}|$.

It therefore suffices to prove that for any projection $\mathbf{P}$, $|F_{\mathbf{P}}| \leq 2^{mn - d'n^2}$. Say that $\mathbf{P}$ is a projection onto the coordinates $\mathbf{e}_{l+k+1}, \dots, \mathbf{e}_n, \mathbf{f}_{l+1}, \dots, \mathbf{f}_n$. In particular, $m = (n-l) + (n-l-k) = 2n - 2l - k$. By our bound on m, it follows that $2n - 2l - k \geq cn$, i.e.

$$2l + k \leq (2 - c)n. \tag{67}$$

Let $\mathbf{M}$ be a uniformly random element of $\mathbb{Z}_2^{m \times n}$. We will consider the conditions under which there exists $\mathbf{N} \in \mathcal{S}$ for which $\mathbf{M} = \mathbf{PN}$. We may decompose $\mathbf{N}$ as

$$\mathbf{N} = \begin{bmatrix} \mathbf{B}_1 \\ \mathbf{B}_2 \\ \mathbf{B}_3 \\ \mathbf{C}_1 \\ \mathbf{C}_2 \\ \mathbf{C}_3, \end{bmatrix} \tag{68}$$

where $\mathbf{B}_1, \mathbf{C}_1 \in \mathbb{Z}_2^{l \times n}$, $\mathbf{B}_2, \mathbf{C}_2 \in \mathbb{Z}_2^{k \times n}$, and $\mathbf{B}_3, \mathbf{C}_3 \in \mathbb{Z}_2^{(n-l-k) \times n}$. The only condition on $\mathbf{N}$ is that its columns are symplectically orthogonal, which translates to the requirement that $\mathbf{D} := \mathbf{C}_1^\intercal \mathbf{B}_1 + \mathbf{C}_2^\intercal \mathbf{B}_2 + \mathbf{C}_3^\intercal \mathbf{B}_3$ is symmetric. Then,

$$\mathbf{M} = \mathbf{PN} = \begin{bmatrix} \mathbf{B}_3 \\ \mathbf{C}_2 \\ \mathbf{C}_3 \end{bmatrix}. \tag{69}$$

Hence, $\mathbf{M} \in F_{\mathbf{P}}$ if and only if there is some choice of $\mathbf{B}_1, \mathbf{B}_2, \mathbf{C}_1$ for which $\mathbf{D}$ is symmetric. Let $\mathbf{R}^\intercal \in \mathbb{Z}_2^{n \times n}$ be an invertible matrix chosen so that $\mathrm{im}(\mathbf{R}^\intercal \mathbf{C}_2^\intercal)$ is contained in the last k coordinate vectors. This is possible, since $\mathbf{C}_2^\intercal \in \mathbb{Z}_2^{n \times k}$ has rank at most k. Then, define $\mathbf{D}' := \mathbf{R}^\intercal \mathbf{D} \mathbf{R} = \mathbf{C}_1'^\intercal \mathbf{B}_1' + \mathbf{C}_2'^\intercal \mathbf{B}_2' + \mathbf{C}_3'^\intercal \mathbf{B}_3'$, where $\mathbf{C}_i' = \mathbf{C}_i \mathbf{R}$ and $\mathbf{B}_i' = \mathbf{B}_i \mathbf{R}$. $\mathbf{D}'$ is symmetric if and only if $\mathbf{D}$ is symmetric, and so we need to select $\mathbf{B}_1', \mathbf{B}_2'$, and $\mathbf{C}_1'$ for which $\mathbf{D}'$ is symmetric.

By construction of $\mathbf{R}^\intercal$, $\mathbf{C}_2'^\intercal \mathbf{B}_2' \in \mathbb{Z}_2^{n \times n}$ is only nonzero in the last k rows, since $\mathrm{im}(\mathbf{C}_2'^\intercal \mathbf{B}_2') \subseteq \mathrm{im}(\mathbf{R}^\intercal \mathbf{C}_2^\intercal)$. It immediately follows that the top $(n-k) \times (n-k)$ block of $\mathbf{C}_1'^\intercal \mathbf{B}_1' + \mathbf{C}_3'^\intercal \mathbf{B}_3'$ must be symmetric. Equivalently, defining $\widetilde{\mathbf{C}}_i$ to be the first $n-k$ columns of $\mathbf{C}_i'$ and $\widetilde{\mathbf{B}}_i$ as the first $n-k$ columns of $\mathbf{B}_i'$,

$$(\widetilde{\mathbf{C}}_1^\intercal \widetilde{\mathbf{B}}_1 + \widetilde{\mathbf{B}}_1^\intercal \widetilde{\mathbf{C}}_1) + (\widetilde{\mathbf{C}}_3^\intercal \widetilde{\mathbf{B}}_3 + \widetilde{\mathbf{B}}_3^\intercal \widetilde{\mathbf{C}}_3) = \mathbf{0}. \tag{70}$$

Notice that for arbitrary $\widetilde{\mathbf{C}}_1, \widetilde{\mathbf{B}}_1$, $\widetilde{\mathbf{C}}_1^\intercal \widetilde{\mathbf{B}}_1 + \widetilde{\mathbf{B}}_1^\intercal \widetilde{\mathbf{C}}_1$ is the sum of two matrices with rank at most l, and hence must have rank at most $2l$.

Meanwhile, since $\mathbf{M}$ is uniformly random, $\widetilde{\mathbf{B}}_3$ and $\widetilde{\mathbf{C}}_3$ are uniformly random as well. Then we claim that $\widetilde{\mathbf{B}}_3, \widetilde{\mathbf{C}}_3 \in \mathbb{Z}_2^{(n-l-k) \times (n-k)}$ satisfy the conditions of Lemma D.7. The relevant condition to establish is that

$$\alpha(n-k) \leq n - l - k \leq (n-k), \tag{71}$$

for some $\alpha \in (1/2, 1)$. The upper bound on $n - l - k$ is immediate. Meanwhile, by Eqn. (67), we write that $l \leq \frac{(2-c)n-k}{2} \leq \frac{(2-c)(n-k)}{2}$, since $2 - c \leq 1$. Thus,

$$n - l - k \geq (n-k) - (n-k)\frac{(2-c)}{2} = \left(\frac{c}{2}\right)(n-k). \tag{72}$$

By assumption, $c > 1$, which gives the desired lower bound with $\alpha := \frac{c}{2}$.

Now, applying the lemma with $\epsilon := c-1$, $\widetilde{\mathbf{C}}_3^\intercal \widetilde{\mathbf{B}}_3 + \widetilde{\mathbf{B}}_3^\intercal \widetilde{\mathbf{C}}_3$ has rank strictly larger than $(1-\epsilon)(n-k) = (2-c)(n-k)$ with probability at least $1 - 2^{-\delta(n-k)^2}$, for some $\delta > 0$. Using Eqn. (67), we see that $k \leq (2-c)n$ or $n - k \geq (c-1)n$, implying that $2^{-\delta(n-k)^2} \leq 2^{-\delta(c-1)^2 n^2}$. Hence this rank bound holds with probability at least $1 - 2^{-\delta(c-1)^2 n^2}$. Furthermore,

$$(2-c)(n-k) \geq (2-c)n - k \geq 2l. \tag{73}$$

Consequently, the rank of

$$\widetilde{\mathbf{C}}_1^\intercal \widetilde{\mathbf{B}}_1 + \widetilde{\mathbf{B}}_1^\intercal \widetilde{\mathbf{C}}_1, \tag{74}$$

for *any* choice of $\widetilde{\mathbf{C}}_1, \widetilde{\mathbf{B}}_1$ (which is $\leq 2l$) is strictly less than that of

$$\widetilde{\mathbf{C}}_3^\intercal \widetilde{\mathbf{B}}_3 + \widetilde{\mathbf{B}}_3^\intercal \widetilde{\mathbf{C}}_3 \tag{75}$$

with probability at least $1 - 2^{-\delta(c-1)^2 n^2}$. Conditioned on this event,

$$(\widetilde{\mathbf{C}}_1^\intercal \widetilde{\mathbf{B}}_1 + \widetilde{\mathbf{B}}_1^\intercal \widetilde{\mathbf{C}}_1) + (\widetilde{\mathbf{C}}_3^\intercal \widetilde{\mathbf{B}}_3 + \widetilde{\mathbf{B}}_3^\intercal \widetilde{\mathbf{C}}_3) \neq \mathbf{0}, \tag{76}$$

since the first term must have the same rank of the second term to cancel it out. By the previous argument, therefore, $\mathbf{M} \notin F_{\mathbf{P}}$. Now, set $d' = \delta(c-1)^2$. Then at most a $2^{-d'n^2}$ fraction of matrices $\mathbf{M} \in \mathbb{Z}_2^{m \times n}$ lie in $F_{\mathbf{P}}$. Thus, $|F_{\mathbf{P}}| \leq 2^{mn - d'n^2}$. It follows that $H(\mathbf{BA}) \leq mn - d'n^2$.

To complete the proof, we observe that $H(\mathbf{A}) \leq 2n^2$, so by the data processing inequality, $H(\mathbf{BA}) \leq 2n^2$. Then, the bound

$$H(\mathbf{BA}) \leq \left(1 - \frac{\min(d', 1)}{3}\right) mn \tag{77}$$

always holds, since when $m \leq 3n$, $mn - d'n^2 \leq mn - \frac{d'}{3}mn$ and when $m \geq 3n$, $2n^2 \leq mn - \frac{1}{3}mn$. Setting $d = \frac{\min(d',1)}{3}$ completes the proof. □

Before proving Theorem D.2, we record a simple result about the distribution of $\mathbf{b} \cdot \mathbf{e}$, where $\mathbf{b}$ is any fixed vector and $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$.

Lemma D.9. *Let $\mathbf{b} \in \mathbb{Z}_2^{2n}$ be a fixed vector and $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$ for $p \leq \frac{3}{4}$. Then $\mathbf{b} \cdot \mathbf{e} \sim \mathsf{Ber}(q)$, where $\eta(|\mathbf{b}|, p) \leq q \leq \frac{1}{2}$ for*

$$\eta(w, p) = \frac{1 - \left(1 - \frac{4}{3}p\right)^{\frac{w}{2}}}{2}. \tag{78}$$

Note that $\eta(w, p)$ is non-negative, and is increasing in both w and p.

Proof. Since $\mathbf{e} \sim \mathcal{D}_p^{\otimes n}$,

$$\mathbf{b} \cdot \mathbf{e} \;=\; \sum_{k \in T} e_k, \tag{79}$$

where T is the set of indices where $\mathbf{b}$ is nonzero. For any $k \in [n]$, let

$$e'_k \;=\; b_k e_k \;+\; b_{n+k} e_{n+k}. \tag{80}$$

By direct calculation,

$$e'_k \sim \begin{cases} \mathsf{Ber}(0) & k, n+k \notin T, \\ \mathsf{Ber}(\frac{2}{3}p) & \text{else.} \end{cases} \tag{81}$$

For $S = \{\, k \le n \mid k \in T \text{ or } k+n \in T \,\}$, we may rewrite

$$\sum_{k \in T} e_k = \sum_{k \in S} e'_k. \tag{82}$$

These e'_k are independent Bernoulli random variables with probability $q = \frac{2}{3}p$, and note that

$$|S| \;\ge\; \frac{|\mathbf{b}|}{2}. \tag{83}$$

Using the fact that the probability that a $\mathsf{Binomial}(m, q)$ random variable is odd with probability $\frac{1}{2} - \frac{1}{2}(1-2q)^m$,

$$\Pr\left[\sum_{k \in S} e'_k = 1\right] = \frac{1 - \left(1 - \frac{4}{3}p\right)^{|S|}}{2}, \tag{84}$$

which satisfies

$$\frac{1 - \left(1 - \frac{4}{3}p\right)^{|\mathbf{b}|/2}}{2} \le \frac{1 - \left(1 - \frac{4}{3}p\right)^{|S|}}{2} \le \frac{1}{2} \tag{85}$$

as desired. □

Proof of Theorem D.2. Let

$$\mu(\mathbf{B}_0) := \mathop{\mathbb{E}}_{\mathbf{e} \sim \mathcal{D}_p^{\otimes n}} [|\mathbf{B}_0 \mathbf{e}|], \tag{86}$$

for any $\mathbf{B}_0 \in \mathbb{Z}_2^{m \times 2n}$. Let $\mathbf{B}$ be any random variable such that $\mathbf{BA}$ has negligible total variation distance from a uniformly random matrix. Recalling that $r := \frac{n}{m}$, let A be the event that $\mu(\mathbf{B}) < (\frac{1-r-\delta}{2})m$. We will show that $\Pr[A] = \mathrm{negl}(n)$. When $\Pr[A] = 0$ there is nothing to prove; otherwise $\delta < 1 - r$. We claim that it suffices to show that

$$H(\mathbf{BA} | A) = mn - \Omega(mn). \tag{87}$$

Suppose for contradiction that $\Pr[A] \ge \frac{1}{\mathrm{poly}(n)}$ for infinitely many n, but Eqn. (87) holds. We restrict to this subsequence. Then we may describe the probability distribution $h : \mathbb{Z}_2^{m \times n} \to [0,1]$ of $\mathbf{BA} \in \mathbb{Z}_2^{m \times n}$, as

$$h = pf + (1-p)g, \tag{88}$$

where $p := \Pr[A] \ge \frac{1}{\mathrm{poly}(n)}$ and $H(f) = mn - \Omega(mn)$. From this decomposition, there is a resulting bound on entropy of

$$\begin{aligned} H(h) &\le pH(f) + (1-p)H(g) + H_2(p) && (89)\\ &\le p(mn - \Omega(mn)) + (1-p)mn + O(p \log(2/p)) && (90)\\ &= mn - \Omega(pmn) + O(p \log(n)) && (91)\\ &\le mn - \frac{1}{\mathrm{poly}(n)}, && (92) \end{aligned}$$

where in the second inequality we use the fact that $H_2(p) = O(p \log(2/p))$ for $0 < p \leq 1$.

However, h is the probability distribution of $\mathbf{BA}$, and since $mn = \text{poly}(n)$, negligible total variation distance from uniform implies a negligible difference in entropy. Since h has negligible distance from uniform by assumption, and the entropy of the uniform distribution is mn, this is a contradiction.

We will now bound the entropy $H(\mathbf{BA}|A)$. Define a random variable $\mathbf{\Pi} \in \mathbb{Z}_2^{m \times m}$, which is the permutation matrix such that the rows of $\mathbf{B'} := \mathbf{\Pi B}$ are sorted in descending order by weight. Note that $H(\mathbf{\Pi BA}|\mathbf{A}, \mathbf{\Pi}) = H(\mathbf{BA}|\mathbf{A}, \mathbf{\Pi})$ since $\mathbf{\Pi}$ is a permutation, so that

$$H(\mathbf{\Pi BA}|A) \geq H(\mathbf{\Pi BA}|A, \mathbf{\Pi}) = H(\mathbf{BA}|A, \mathbf{\Pi}) \tag{93}$$

$$\geq H(\mathbf{BA}|A) - H(\mathbf{\Pi}|A). \tag{94}$$

Thus,

$$H(\mathbf{BA}|A) \leq H(\mathbf{\Pi BA}|A) + H(\mathbf{\Pi}|A) \tag{95}$$

$$\leq H(\mathbf{B'A}|A) + m \log(m). \tag{96}$$

Since $m = \text{poly}(n)$, $m \log(m) = o(mn)$, it therefore suffices to show that $H(\mathbf{B'A}|A) = mn - \Omega(mn)$.

Let $\mathbf{b}'_i$ denote the ith row of $\mathbf{B'}$. Then, by linearity of expectation and Lemma D.9,

$$\mu(\mathbf{B'}) = \sum_i \mathop{\mathbb{E}}_{\mathbf{e} \sim \mathcal{D}_p^{\otimes n}} [\mathbf{b}'_i \cdot \mathbf{e}] \geq \sum_i \eta(|\mathbf{b}'_i|, p) \tag{97}$$

where we recall that $\eta(w, p) = \frac{1}{2}\left[1 - \left(1 - \frac{4}{3}p\right)^{\frac{w}{2}}\right]$. Because $\mathbf{B'e}$ and $\mathbf{Be}$ have exactly the same weight,

$$\mu(\mathbf{B}) = \mu(\mathbf{B'}). \tag{98}$$

Hence, the event A is also the event that $\mu(\mathbf{B'}) < (\frac{1-r-\delta}{2})m$. The use of $\mathbf{\Pi}$ to sort $\mathbf{B}$ into $\mathbf{B'}$ is helpful because it will allow us to split the entropy analysis into two cases: for the first few rows of $\mathbf{B'}$, the entropy is large and we will not be able to give a non-trivial bound, but for all remaining rows, we will show that their weight is relatively small, and thus have a much lower entropy. Define this "cutoff" row to be $k = \lceil m(1 - r - \frac{\delta}{2}) \rceil$. We claim that for any $d_0 > 0$, for sufficiently large n, $\Pr_{\mathbf{B}}[|\mathbf{b}'_k| \geq d_0 n \,|\, A] = 0$. This is because if $|\mathbf{b}'_k| \geq d_0 n$, then

$$\sum_i \eta(|\mathbf{b}'_i|, p) \geq \sum_{i=1}^{k} \eta(|\mathbf{b}'_k|, p) \geq k\eta(d_0 n, p) \tag{99}$$

$$= k\left(\frac{1}{2} - \frac{\left(1 - \frac{4}{3}p\right)^{d_0 n/2}}{2}\right) = \frac{k}{2} - o(k). \tag{100}$$

Note that $\frac{k}{2} \geq \left(\frac{1-r}{2} - \frac{\delta}{4}\right) m$, so this immediately implies that for sufficiently large n, $\mu(\mathbf{B}) \geq \frac{k}{2} - o(k) > \left(\frac{1-r-\delta}{2}\right) m$, contradicting the conditioned event A. Hence, for sufficiently large n, $|\mathbf{b}'_k| < d_0 n$, and by construction $|\mathbf{b}'_j| < d_0 n$ for all $j \geq k$. Now, we consider the $m - k$ bottom rows, which all satisfy this weight bound.

$$m - k \geq m\left(r + \frac{\delta}{2}\right) - 1 \gtrsim m\left(r + \frac{\delta}{4}\right) \geq n\left(1 + \frac{c\delta}{4}\right), \tag{101}$$

where $\gtrsim$ indicates that inequality holds for sufficiently large n. If $\mathbf{B}'_1$ denotes the first k rows of $\mathbf{B}'$ and $\mathbf{B}'_2$ denotes the remaining $m-k$ rows, then by the support-size bound in the proof of theorem D.1,

$$H(\mathbf{B}'_2\mathbf{A}|A) \leq H((\mathbf{B}'_2, \mathbf{B}'_2\mathbf{A})|A) = H(\mathbf{B}'_2\mathbf{A}|\mathbf{B}'_2, A) + H(\mathbf{B}'_2|A) \tag{102}$$

$$\leq (m-k)n - d(m-k)n + H(\mathbf{B}'_2|A) \tag{103}$$

$$\leq (m-k)n - d\left(r + \frac{\delta}{4}\right)mn + H(\mathbf{B}'_2|A) \tag{104}$$

for some $d > 0$, that depends on the constant $\frac{c\delta}{4}$.

Each row of $\mathbf{B}'_2$ has weight at most $d_0 n$. Thus, the entropy of each row is at most the entropy of a uniformly random length-$2n$ bitstring of weight at most $\lfloor d_0 n \rfloor$, which is $\log \sum_{j=0}^{\lfloor d_0 n \rfloor} \binom{2n}{j} \leq 2nH_2(d_0/2)$; the entropy overall of $\mathbf{B}'_2$ is at most the sum of the entropies of its rows, so

$$H(\mathbf{B}'_2 \mid A) \leq (m-k) \log \left(\sum_{j=0}^{\lfloor d_0 n \rfloor} \binom{2n}{j} \right) \leq 2mnH_2(d_0/2). \tag{105}$$

Choose $0 < d_0 < 1$ sufficiently small so that $H_2(d_0/2) \leq d'/4$, where $d' := d\delta/4$. Then

$$H(\mathbf{B}'_2|A) \leq \frac{d'}{2}mn. \tag{106}$$

As a consequence, we obtain that $H(\mathbf{B}'_2\mathbf{A}|A) \leq (m-k)n - \frac{d'}{2}mn$. Meanwhile, by a trivial dimension bound, $H(\mathbf{B}'_1\mathbf{A}|A) \leq kn$. Together, these bounds imply that

$$H(\mathbf{B}'\mathbf{A}|A) \leq H(\mathbf{B}'_1\mathbf{A}|A) + H(\mathbf{B}'_2\mathbf{A}|A) \tag{107}$$

$$\leq mn - \frac{d'}{2}mn. \tag{108}$$

Hence, as desired, we have that $H(\mathbf{B}'\mathbf{A}|A) = mn - \Omega(mn)$, and as a result $\Pr[A] = \mathrm{negl}(n)$. □