# Good Gottesman-Kitaev-Preskill codes from the NTRU cryptosystem

Jonathan Conrad[1,2], Jens Eisert[1,2,3], and Jean Pierre Seifert[4,5]

[1]Dahlem Center for Complex Quantum Systems, Physics Department, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany
[2]Helmholtz-Zentrum Berlin für Materialien und Energie, Hahn-Meitner-Platz 1, 14109 Berlin, Germany
[3]Fraunhofer Heinrich Hertz Institute, Einsteinufer 37, 10587 Berlin, Germany
[4]Electrical Engineering and Computer Science Department, Technische Universität Berlin, Straße des 17. Juni 135, 10587 Berlin, Germany
[5]Fraunhofer Institute for Secure Information Technology, Rheinstraße 75, 64295 Darmstadt, Germany
10.4.2023



**We introduce a new class of random Gottesman-Kitaev-Preskill (GKP) codes derived from the cryptanalysis of the so-called NTRU cryptosystem. The derived codes are *good* in that they exhibit constant rate and average distance scaling $\Delta \propto \sqrt{n}$ with high probability, where $n$ is the number of bosonic modes, which is a distance scaling equivalent to that of a GKP code obtained by concatenating single mode GKP codes into a qubit-quantum error correcting code with linear distance. The derived class of NTRU-GKP codes has the additional property that *decoding* for a stochastic displacement noise model is equivalent to *decrypting* the NTRU cryptosystem, such that every random instance of the code naturally comes with an efficient decoder. This construction highlights how the GKP code bridges aspects of classical error correction, quantum error correction as well as post-quantum cryptography. We underscore this connection by discussing the computational hardness of decoding GKP codes and propose, as a new application, a simple public key quantum communication protocol with security inherited from the NTRU cryptosystem.**

## 1 Introduction

In recent years, notions of bosonic quantum-error correction with the *Gottesman-Kitaev-Preskill* (GKP) code [1] have seen a rapid increase of interest both in theory and in experiment, primarily due to the perspective of them contributing to a viable route towards large scale quantum computing using integrated *photonic* [2, 3] and *superconducting platforms* [4]. Such codes have highly attractive features for systems in which quantum information is encoded in continuous variable degrees of freedom and are specifically suitable to accommodate photon loss [5, 6, 7, 8]. While much research has been dedicated to obtain effective qubits from single-mode systems that are to be integrated into larger qubit-based networks [9, 10], this approach is arguably only scratching the surface of possibilities offered by the GKP code within its more general, lattice theoretic perspective [11, 12, 13, 14].

Jonathan Conrad: j.conrad1005@gmail.com

To corroborate this claim, in this work, we construct random *good* GKP codes derived from a cryptographic attack on the NTRU cryptosystem [15]. We define and discuss a goodness property for GKP codes in the lattice theoretic framework analogous to the notion of goodness in conventional quantum- and classical error correcting codes as a stepping stone towards scalable codes. We investigate the decoding problem of this class of codes and show how the native *decryption* routine of the NTRU cryptosystems with access to its secret key can serve as decoder for the corresponding GKP code.

We investigate the complexity of decoding general GKP codes and highlight how our *NTRU-GKP* codes can be viewed as a *trapdoor decodable quantum error correcting code*, where decoding of the associated quantum error correcting code is expected to by computationally hard in general but becomes significantly easier when supplemented with additional (secret) information about the structure of the code. We consider this a first step towards cryptographic protocols built on the decoding problem of GKP codes which we believe can have wide application for secure quantum communication and cloud-based quantum computing and hope that this article stimulates interest in this new direction of research.

This article is structured as follows. In Section 2, we introduce basic principles of the GKP code, describe relevant aspects of the general decoding problem for the GKP code and define *goodness* of a GKP code family. In Section 3, we discuss a selection of notable examples of GKP codes and summarize their properties. The NTRU cryptosystem and GKP codes built on this are discussed in Section 4 where we provide evidence that they form a family of *good* randomized GKP codes.

The goodness property of GKP codes is established

through proposition 1 and conjecture 1, 2. Proposition 1 establishes that NTRU-GKP codes built on schemes to sample the public key prescribing the NTRU lattice according to the procedure originally proposed in ref. [15], often referred to as NTRU-HPS, are good with overwhelming probability. This proposition foots on a proof provided by Bi and Qi in ref. [16] and establishes goodness for GKP codes built on a specific distribution of ($q-$symplectic) matrices and lattices. We observe numerically that random public keys for the NTRU cryptosystem well satisfy the good scaling property which is summarized in conjecture 1. Finally, a variation of the NTRU cryptosystem has been proposed by Stehle and Steinfeld [17], who show that their procedure yields pseudo-random public keys for the NTRU cryptosystem. We numerically confirm the expected goodness of NTRU-GKP codes drawn according to their procedure which is summarized in conjecture 2. An additional rigorously minded perspective is provided in the appendix, where with proposition 3 we establish average-case goodness for a class of symplectic lattices slightly larger than that produced by the NTRU-cryptosystem. This proof is constructive. We discuss the decoding problem for the NTRU-GKP codes in Section 5 and discuss a quantum *public key cryptosystem* (PKC) designed around the NTRU-GKP codes. Finally, we conclude and provide outlook in Section 6.

## 2 The GKP code

We build our framework on our recent exposition [12] which we refer to for an in-depth discussion; see also the original work [1] as well as refs. [11, 18, 13, 14]. The *GKP code* [1] is a *stabilizer code* acting on the Hilbert space of $n$ bosonic modes, where stabilizers are given by displacement operators

$$D(\boldsymbol{\xi}) = \exp\left\{-i\sqrt{2\pi}\boldsymbol{\xi}^T J\hat{\boldsymbol{x}}\right\}, \tag{1}$$

where

$$J_{2n} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes I_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \tag{2}$$

is the symplectic form, $\boldsymbol{\xi} \in \mathbb{R}^{2n}$, and $\hat{\boldsymbol{x}} = (\hat{q}_1, \hat{q}_2, \ldots, \hat{p}_{n-1}, \hat{p}_n)^T$ is the generalized quadrature operator. Its stabilizer group is specified by fixing $2n$ linearly independent vectors $\boldsymbol{\xi}_i$, $i = 1, \ldots, 2n$,

$$\mathcal{S} = \langle D(\boldsymbol{\xi}_1) \ldots D(\boldsymbol{\xi}_{2n}) \rangle = \left\{ e^{i\phi_M(\boldsymbol{\xi})} D(\boldsymbol{\xi}),\ \boldsymbol{\xi} \in \mathcal{L} \right\}, \tag{3}$$

where $M = (\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{2n})^T$ is a generator for the lattice $\mathcal{L} = \mathbb{Z}^{2n} M$ [1] and we have

$$\phi_M(\boldsymbol{\xi}) = \pi \boldsymbol{a}^T A_{\blacktriangleleft} \boldsymbol{a},\ \boldsymbol{a}^T = \boldsymbol{\xi}^T M^{-1}, \tag{4}$$

[1] For clarity of presentation, we sometimes assume row- vs. column vector conventions to be clear from context.

to denote the phase-sector when we have chosen $M$ to be the basis for which each associated displacement operator is fixed to eigenvalue $+1$ by eq. (3). $A = MJM^T$ denotes the symplectic Gram matrix and $A_{\blacktriangleleft}$ its left lower triangle.

While the stabilizer group $\mathcal{S} \sim \mathcal{L}$ is isomorphic to the lattice $\mathcal{L}$, its centralizer within the displacements $\mathcal{C}(\mathcal{S}) \sim \mathcal{L}^\perp$ – i.e., the set of displacement operators that commute with every element in $\mathcal{S}$ – is isomorphic to its symplectic dual lattice $\mathcal{L}^\perp := \left\{\boldsymbol{x} \in \mathbb{R}^{2n},\ \boldsymbol{x}^T J\boldsymbol{\xi} \in \mathbb{Z} \forall \boldsymbol{x} \in \mathcal{L}\right\}$. $\mathcal{S}$ is Abelian iff $\mathcal{S} \subseteq \mathcal{C}(\mathcal{S})$ which is equivalent to $\mathcal{L} \subseteq \mathcal{L}^\perp$ and $A$ being integer. Compactly, GKP codes are represented by *weakly symplectically self-dual* lattices $\mathcal{L} \subseteq \mathcal{L}^\perp$ where the elements in the symplectic dual quotient $\mathcal{L}^\perp/\mathcal{L}$ label the group of logical Pauli-operations of the code encoding $D$ dimensions, which has size $|\det(A)| = D^2$. When we encode collections of qubits, $k = \log_2(D) = \log_2(|\det(M)|) = \log_2(|\det(\mathcal{L})|)$ denotes the number of encoded logical qubits, which grows logarithmically with the determinant of the stabilizer lattice.

**Code distance.** The (Euclidean) code *distance* of the GKP code is defined as $\Delta = \min_{\boldsymbol{x} \in \mathcal{L}^\perp \setminus \mathcal{L}} \|x\|$, the length of the shortest vector in $\mathcal{L}^\perp$ not in $\mathcal{L}$. The distance as defined here is a meaningful indicator for the code performance in a stochastic displacement error model if the probability that a certain displacement is realized scales inversely with its length.

The distance is also the smallest power of $q$ in the complex polynomial

$$Q_\mathcal{L}(z) = \Theta_{\mathcal{L}^\perp}(z) - \Theta_\mathcal{L}(z) = N_{\Delta^2} q^{\Delta^2} + O\left(q^{\Delta^2}\right), \tag{5}$$

where $q = e^{i\pi z}$, $z \in \mathcal{H} = \{z \in \mathbb{C},\ \mathrm{Im}\, z > 0\}$ and

$$\Theta_\mathcal{L}(z) = \sum_{\boldsymbol{x} \in \mathcal{L}} q^{\|\boldsymbol{x}\|^2} \tag{6}$$

is the *theta function* of the lattice $\mathcal{L}$ and $N_{\Delta^2}$ in $Q_\mathcal{L}(z)$ counts the number of lattice points in $\mathcal{L}^\perp \setminus \mathcal{L}$ of squared length $\Delta^2$. It is expected that the relative scaling of $N_{\Delta^2}$ with $\Delta^2$ significantly impacts the existence and scale of the threshold of a GKP code family and is responsible for the entropic contribution to the decoding problem [9, 19]. We comment on this further in Appendix B. The theta function and distance are by construction symmetric under orthogonal transformations $O \in \mathcal{O}(2n)$ of the lattice $\mathcal{L} \mapsto O\mathcal{L}$, while $N_{\Delta^2}$ scales with the number of orthogonal automorphisms of the lattice.

**Decoding GKP codes via the closest vector problem.** Upon measuring the stabilizers on displacement error $D(\boldsymbol{e})$ and obtaining the syndromes $\boldsymbol{s} = MJ\boldsymbol{e} \mod 1$, one strategy is to correct back to the code space by applying a displacement in phase

```
function NearestPlane(B, t)
    if len(B) == 0 then
        return 0^{len(t)}
    else
        set B* = GramSchmidt(B)
        set c = ⌊t^T B*_{-1} / ||B*_{-1}||^2⌉
        return cB_{-1} + NearestPlane(B_{:-1}, t − cB_{-1})
    end if
end function
```

Figure 1: Babai's nearest plane algorithm [20].

space with $\boldsymbol{\eta} = (MJ)^{-1}\boldsymbol{s}$. Since the choice of the generator $M$ is ambiguous, it is generally necessary to append this initial correction by a logical post-correction to minimize the probabilty of imposing a logical error. Algorithms finding the correction that minimizes logical errors given the syndromes are called *decoders* in this context. Assuming a Gaussian displacement error model with variance $\overline{\sigma}^2$ [2], one derives the optimal post-correction [12] to be applied after an initial correction $\boldsymbol{\eta}$ to be given by *maximum likelihood decoding* (MLD)

$$\overline{\boldsymbol{\xi}}^{\perp} = \underset{\boldsymbol{\xi}^{\perp}\in\mathcal{L}^{\perp}/\mathcal{L}}{\arg\max}\, \Theta_{\boldsymbol{\eta}+\boldsymbol{\xi}^{\perp}+\mathcal{L}}\left(\frac{i}{2\pi\overline{\sigma}^2}\right). \tag{7}$$

For small error rates $\overline{\sigma}\to 0$, the most likely coset as computed in MLD is given by the most likely individual error consistent with the syndrome. We refer to decoding based on the most likely individual error consistent with the syndrome as *minimum energy decoding* (MED) [9], to which the solution is presented by the *closest vector problem* (CVP), $\overline{\boldsymbol{\xi}}^{\perp} = \mathtt{CVP}\left(\boldsymbol{\eta}, \mathcal{L}^{\perp}\right)$ (see ref. [12]), that is, in this limit MLD reduces to CVP.

**Bounded distance decoding (BDD).** By nature of the Gaussian error model, it is unlikely to sample an error larger than $\|\boldsymbol{e}\| > \sqrt{2n\overline{\sigma}^2}$ [18, 11]. Hence, it is reasonable to restrict the decoding problem to *bounded-distance-decoding* ($\mathtt{BDD}_{\epsilon}\left(\boldsymbol{\eta}, \mathcal{L}^{\perp}\right)$), which is CVP with an additional promise that $\mathrm{dist}\left(\boldsymbol{\eta}, \mathcal{L}^{\perp}\right) \leq \epsilon$. Given that typical Gaussian errors will be overwhelmingly of length $\|\boldsymbol{e}\| \leq \sqrt{2n\overline{\sigma}^2}$ we expect to decode successfully by solving $\mathtt{BDD}_{\epsilon}\left(\boldsymbol{\eta}, \mathcal{L}^{\perp}\right)$ with $\epsilon = \sqrt{2n\overline{\sigma}^2}$. Provided a lattice basis $M$ and its Gram-Schmidt orthogonalization $\tilde{M} = (\tilde{\boldsymbol{\xi}}_1, \ldots, \tilde{\boldsymbol{\xi}}_{2n})^T$ it is known that Babai's nearest plane algorithm solves BDD when $\epsilon < \min_i \|\tilde{\boldsymbol{\xi}}_i\|/2 =: \|\tilde{M}\|/2$ [20, 21], that is when we are in possession of a lattice basis such that its Gram-Schmidt reduced vectors are sufficiently long $\|\tilde{M}\| \geq \sqrt{8n\overline{\sigma}^2}$.

When considering code families with growing dimension $2n$, errors up to the typical length $\sqrt{2n\overline{\sigma}^2}$ are correctible via CVP decoding only if $\Delta = \Omega\left(\sqrt{n}\right)$. The scaling $\Delta \propto \sqrt{n}$ is the distance scaling of a GKP code obtained by concatenating fixed single-mode GKP codes with a qubit quantum error correcting code with linear distance $d \propto n$. Such scaling in error correction performance is predicted to exist by the quantum Gilbert-Varshamov bound [22, 23] and explicit or randomized constructions exhibiting such distance scaling have been investigated in the literature, see, e.g., refs. [24, 25, 26, 27] and references therein. We define the analogous *goodness* property for families of GKP codes.

**Definition 1** (Good GKP codes)**.** *A GKP code family $\mathcal{L}_n \subset \mathbb{R}^{2n}$ parametrized by lattice dimension $2n$ with asymptotically non-vanishing rate*

$$\lim_{n\to\infty} \log\det\left(\mathcal{L}_n\right)/n > 0 \tag{8}$$

*and distance scaling*

$$\Delta^2 = \Omega\left(n\right) \tag{9}$$

*is good.*

The existence of such a family of good GKP codes has been established by Harrington and Preskill in refs. [18, 11]. Their proof, based on the existence of good GKP codes obtained from re-scaling symplectically self-dual lattices with shortest vector length $\lambda_1\left(\mathcal{L}\right) = \Omega\left(\sqrt{n}\right)$, whose existence had been shown by Buser and Sarnak [28], however, is non-constructive. In the following, we will review this construction of GKP codes, which we have called *scaled GKP codes* in ref. [12], list some notable examples and show how the NTRU scheme [15] yields a randomized construction of good GKP codes.

## 3 Constructions of GKP codes

**Scaled GKP codes** Central to the construction of GKP codes are the class of *scaled GKP codes*, first introduced and analysed in refs. [1, 11], where a GKP code is obtained by scaling a symplectically self-dual lattice (which we will refer to as *symplectic lattice*) by a factor $\sqrt{\lambda}$, $\lambda \in \mathbb{N}$. Let $\mathcal{L}_0 = \mathcal{L}\left(M_0\right)$ be such a $2n-$dimensional lattice, where we choose $M_0$ as the symplectic basis [29], i.e., $M_0$ is such that

$$A_0 = M_0 J M_0^T = J. \tag{10}$$

Clearly, $A_0$ is integer. Hence the scaled lattice $M = \sqrt{\lambda}M_0$, $\lambda \in \mathbb{N}$, also retains a symplectically integral Gram matrix

$$A = MJM^T = \lambda J. \tag{11}$$

Such lattices are sometimes also called *q-symplectic* [30] with $q = \lambda$. The total encoded dimension and distance are

$$D = \sqrt{|\det\left(A\right)|} = \lambda^n, \tag{12}$$

$$\Delta = \lambda^{-\frac{1}{2}}\lambda_1\left(\mathcal{L}_0\right), \tag{13}$$

[2] We use the overline to denote the rescaled variance that for shifts implemented by the non-standard choice of displacement operators in eq. (1). The physical variance $\sigma^2$ is related to it by $\sigma^2 = 2\pi\overline{\sigma}^2$.

where $\lambda_1(\mathcal{L}_0)$ is the length of the shortest vector in the symplectic lattice $\mathcal{L}_0$. The sympletic dual lattice is generated by $M^\perp = \lambda^{-\frac{1}{2}} M_0$. If $M_0$ is stated in the symplectic basis one can immediately read off pairs of vectors with *symplectic inner product*

$$\left(\boldsymbol{\xi}_i^\perp\right)^T J \boldsymbol{\xi}_{i+n}^\perp = \frac{1}{\lambda};\ i = 1, \ldots, n \tag{14}$$

and symplectic inner product 0 with any other row in $M_0$. The corresponding displacement operators anti-commute up to phase $\omega_\lambda = e^{i\frac{2\pi}{\lambda}}$ and commute with each displacement associated to every other row of $M^\perp$, such that they form the logical generalized Pauli group

$$\overline{X}_i = D\left(\boldsymbol{\xi}_i^\perp\right), \overline{Z}_i = D\left(\boldsymbol{\xi}_{n+i}^\perp\right); \quad \overline{X}_i^\lambda, \overline{Z}_i^\lambda \in \mathcal{S}. \tag{15}$$

Some examples of symplectically self-dual lattices are well known in the literature and also have been re-derived by exhaustive numerical search in ref. [11], which we list in fig. 2 along with other symplectically integral lattices that produce notable GKP codes. The smallest GKP lattices in that table include

- **The** $\mathbb{Z}^2$ lattice with basis

$$M_{\mathbb{Z}^2} = I_2. \tag{16}$$

  This is also the *symplectic basis* [29] for $\mathbb{Z}^2$, i.e., it is such that $M_{\mathbb{Z}^2} J M_{\mathbb{Z}^2}^T = J$. We refer to the scaling of this lattice or its $N$-fold direct sum by the factor $\sqrt{\lambda} = \sqrt{2}$ as the *square GKP code*

$$\mathcal{L}_{N\square} = \sqrt{2}\mathbb{Z}^{2N}. \tag{17}$$

  It has already been noticed in ref. [1] that all Clifford operation for this code can be performed by means of symplectic operations. Furthermore, ref. [31] noticed that performing stabilizer measurements and corrective shifts on the vaccum produces the logical $|H+\rangle$ magic state vector. This is due to the fact that $J_2$ is a symplectic orthogonal automorphism (the logical Hadamard) of the lattice. This is by far the most simple and most popular GKP code discussed in the literature, which also is owed to the fact the lattice is orthogonal such that decoding via CVP becomes a simple one-dimensional rounding protocol [20].

- **The hexagonal** $A_2$ **lattice** with symplectic basis

$$M_{A_2} = \frac{1}{\sqrt[4]{12}} \begin{pmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{pmatrix}. \tag{18}$$

  This lattice is one of the *root lattices* in 2 dimensions and is known to yield the densest sphere packing there, capable of tightly packing spheres of radius $\lambda_1(A_2)/2 = \frac{1}{\sqrt[4]{12}} \approx 0.537\ldots$. The scaling to a qubit-GKP code $\mathcal{L} = \sqrt{2}A_2$ has distance

$$\Delta_{\sqrt{2}A_2} = \frac{1}{\sqrt[4]{3}} \approx 0.76\ldots, \tag{19}$$

  which is the highest distance one can obtain for a single-mode GKP code encoding a single qubit as it is the densest lattice packing in two dimensions [32]. Interestingly, code states of the hexagonal GKP code have also been rederived in a numerical search for the most robust encoding of a qubit into an oscillator under photon loss [6].

Other high dimensional GKP codes built by scaling symplectic self-dual root lattices become increasingly complex and interesting, such as the GKP code built upon the dihedral root system $D_4$ examined in ref. [13], the *Gosset lattice* obtained from the exceptional Lie algebra $E_8$ or the Leech lattice $\Lambda_{24}$, and warrant much further investigation in the future.

**Concatenated GKP codes.** Once a logical qubit is obtained by means of a scaled GKP code, one can concatenate it with a *quantum error correcting-* or *quantum error detecting code* (QECC/QEDC) $\mathcal{Q} = [\![N, k, d]\!]$ to obtain a GKP lattice with larger minimum distance. If $Q$ is the set of symplectic vectors representing the stabilizers of a QECC/QEDC or generally, any set of (binary) vectors such that $\forall p, q \in Q : \ p^T J q = 0 \mod 2$, we can construct a GKP lattice by means of *Construction A* [32, 12], which yields

$$\Lambda(Q) := \left\{ \boldsymbol{x} \in \mathbb{R}^{2n} \middle| \sqrt{2}\boldsymbol{x} \mod 2 \in Q \right\}. \tag{20}$$

This lattice can be interpreted as the full-rank embedding of $Q$ into $\mathbb{R}^{2n}$ and inherits its main properties immediately from the code properties of $Q$ including decoding algorithms. In refs. [34, 35, 9, 36, 37, 38], known decoding algorithms for quantum error correcting codes such as *minimum-weight-perfect-matching* (MWPM, which is an MED decoder) have been adapted to decode diverse concatenations of the single mode square GKP code with the popular *surface*, *toric*, *color*, and *quantum low-density-parity-check* (QLDPC) codes, where the corresponding GKP-lattices can all be understood as Construction A lattices. As noted previously, we denote the underlying multi-mode square-GKP code as $\mathcal{L}_{N\square}$ and the full lattice corresponding to the concatenated code as $\mathcal{L} = \Lambda(Q)$, such that we have $\mathcal{L}_{N\square} \subseteq \mathcal{L}$ and reversely $\mathcal{L}^\perp \subseteq \mathcal{L}_{N\square}^\perp$. These procedures have in common that one decodes in two steps provided the syndrome and a generic correction $\boldsymbol{\eta}$: 1. Solve CVP on the superlattice $\mathcal{L}_{N\square}^\perp$, perform the corresponding correction. This step returns one to $\mathcal{L}_{N\square}^\perp$ and the residual syndrome is a genuine binary syndrome for $Q$. 2. The qubit-level decoder solves some version of (approximate) CVP on $\mathcal{L}^\perp$ provided that one starts out from $\mathcal{L}_{N\square}^\perp$. Before applying this decoder one computes a metric from the syndrome on $\mathcal{L}_{N\square}$ to take advantage of the continuous information held by the full GKP syndrome. Finally one applies the qubit-level decoder with the amended metric. In total, this decoder can

| $n$ | $\dim(\mathcal{L}_0)$ $(\mathcal{L})$ | $\mathcal{L}_0$ | $(\lambda_1(\mathcal{L}))^2$ | Symp. self-dual | Eucl. self-dual | Concatenated (trivial sublattice) |
|---|---|---|---|---|---|---|
| 1 | 2 | $\mathbb{Z}^2$ | 1 | ✓ | ✓ | – |
| 1 | 2 | $A_2$ | $\frac{2}{\sqrt{3}}$ | ✓ | ✓ | – |
| 2 | 4 | $D_4$ | $\sqrt{2}$ | ✓[11] | ✓ | $\mathcal{L}_{\text{triv}} \sim \mathbb{Z}^4$ w/ repetition code [13] |
| 4 | 8 | $E_8$ | 2 | ✓ | ✓ | $\mathcal{L}_{\text{triv}} \sim 2\mathbb{Z}^8$ w/ Hamming code [32] $\mathcal{H}_8 = [8,4,4]$ |
| 6 | 12 | $K_{12}$ | $\frac{4}{\sqrt{3}}$ [11] | ✓[11] | ✓ | $\mathcal{L}_{\text{triv}} \sim A_2^6$ [33] |
| 12 | 24 | $\Lambda_{24}$ | 4 [32] | ✓[28] | ✓ | $\mathcal{L}_{\text{triv}} \sim 2\mathbb{Z}^8$ w/ Golay code* [32] $\mathcal{C}_{24} = [24,12,8]$ |
| $n$ | $2n$ | $\sqrt{\lambda/q}L_{\text{NTRU}}$ | $\Delta \sim \Omega\left(\sqrt{n/\lambda}\right)$ | ✓ | ✓ | $\mathcal{L}_{\text{triv}} \sim \sqrt{\lambda q}\mathbb{Z}^{2n}$ |
| $N$ | $2N$ | $\Lambda_\square(\mathcal{Q})$ | $\Delta \geq \sqrt{d/2}$ | x | x | $\mathcal{Q} = [\![N,k,d]\!]$ |
| $N$ | $2N$ | $\Lambda_\circ(\mathcal{Q})$ | $\Delta = \sqrt{d/\sqrt{3}}$ | x | x | $\mathcal{Q} = [\![N,k,d]\!]$ |

Figure 2: Some notable weakly symplectically self-dual (symplectic) lattices that yield GKP codes. The lower block indicates the concatenation of single mode $\mathcal{L}_\square = \sqrt{2}\mathbb{Z}^2$ square GKP and $\mathcal{L}_\circ = \sqrt{2}A_2$ hexagonal GKP codes with qubit quantum error correcting- or detecting codes. Note that concatenation with $\mathcal{L}_\circ$ does not formally produce a Construction A lattice, but is related by a symplectic transformation $S_\circ^n = \oplus_i^n S_\circ$, $S_\circ = M_{A_2}^T$ to the concatenation with the square GKP code generated by $M_{\mathbb{Z}^2} = I_2$, which in fact is Construction A. The symplectically self-dual root lattices listed in this table and their use as GKP codes have previously been identified in ref. [11]. The re-scaled $L_{\text{NTRU}}$ lattices that we use here to to construct NTRU-GKP codes are indicated between those and the "more genuine" lattices corresponding to concatenated codes. The statements about (symplectic) self-duality are generally up to scaling and rotations.

be pictured as a sequence

$$\mathbb{R}^{2n} \to \mathcal{L}_{N\square}^{\perp} \xrightarrow{\texttt{CVP}(\mu)} \mathcal{L}^{\perp}. \tag{21}$$

It is also known that one can solve CVP exactly on any Construction A lattice provided a soft decoder for the underlying binary code $Q$, see ref. [32, p. 450]. This observation has, e.g., been used to construct CVP algorithms for the $E_8$, which can also be understood as a Construction A lattice on the $\mathcal{H}_8 = [8,4,4]$ Hamming code.

## 3.1 Decoding complexity of GKP codes

Due to the lattice theoretic nature of GKP codes and their respective decoding problems and the well developed literature on lattice problems, it is interesting to investigate the computational complexity of decoding GKP codes from this perspective. Before we continue to construct GKP codes from a cryptosystem proposed for post-quantum cryptography in the next section, we show that 1. for GKP codes, MLD decoding is at least as hard as MED decoding and 2. MED decoding a concatenated (qubit-) GKP code implies a decoder for the corresponding qubit-code.

We include these statements here because we find the proofs illustrative and wish to highlight that decoding complexity of GKP codes is an interesting question deserving of our attention. Denote by eMLD the problem of evaluating the MLD probabilty given by the theta function on the RHS in eq. (7).

**Lemma 1.** *(*$\texttt{eMLD} \geq \texttt{MED}$*) Given an oracle that evaluates*

$$\texttt{eMLD}\left(\boldsymbol{x}, \boldsymbol{\xi}^{\perp}, \mathcal{L}, \overline{\sigma}\right) = \Theta_{\mathcal{L}+\boldsymbol{\xi}^{\perp}+\boldsymbol{x}}\left(\frac{i}{2\pi\overline{\sigma}^2}\right),$$

$\texttt{CVP}\left(\boldsymbol{x}, \mathcal{L}^{\perp}\right)$ *can be solved efficiently.*

*Proof.* Denote by $\texttt{DecCVP}\left(\boldsymbol{x}, \mathcal{L}, r\right)$ the decisional CVP problem that outputs True if $\text{dist}\left(\boldsymbol{x}, \mathcal{L}\right) \leq r$. This is polynomially equivalent to the optimization- and search variants of CVP [39]. First notice that we generally have

$$\Theta_{\mathcal{L}^{\perp}+\boldsymbol{x}}\left(\frac{i}{2\pi\overline{\sigma}^2}\right) = \sum_{\boldsymbol{\xi}^{\perp}\in\mathcal{L}^{\perp}/\mathcal{L}} \Theta_{\mathcal{L}+\boldsymbol{\xi}^{\perp}+\boldsymbol{x}}\left(\frac{i}{2\pi\overline{\sigma}^2}\right) \geq e^{-\frac{1}{2\overline{\sigma}^2}\text{dist}\left(\boldsymbol{x},\mathcal{L}^{\perp}\right)^2}. \tag{22}$$

If $\texttt{DecCVP}\left(\boldsymbol{x}, \mathcal{L}, r\right)$ is true, then we further have

$$e^{-\frac{1}{2\overline{\sigma}^2}\text{dist}\left(\boldsymbol{x},\mathcal{L}^{\perp}\right)^2} \geq e^{-\frac{r^2}{2\overline{\sigma}^2}} \tag{23}$$

for all $\overline{\sigma} \in \mathbb{R}$, and hence we can solve $\texttt{DecCVP}\left(\boldsymbol{x}, \mathcal{L}^{\perp}, r\right)$ by checking if above condition is true for sufficiently small $\overline{\sigma} < r$. Alternatively, w.l.o.g. assume that $\mathcal{L} \subset \mathbb{Z}^n$ and $\boldsymbol{x} \in \mathbb{Z}$. Given access to

$$\Theta_{\mathcal{L}^{\perp}+\boldsymbol{x}}(z) = \sum_{m\in\mathbb{N}} a_m e^{i\pi z m},$$

we can compute

$$2a_m = e^{m\pi\tau}\int_{-1}^{1} dt\, e^{-it\pi m}\Theta_{\mathcal{L}^{\perp}+\boldsymbol{x}}(t+i\tau) \tag{24}$$

to evaluate $\{a_m\}$ for $m = 1,\ldots,M$, where $M$ can be bounded by Mikowskis convex body theorem, to find the smallest non-zero coefficient $a_m$. This solves optimization-CVP which is polynomially equivalent to its search version. □

Note that here we did not show that the full MLD problem

$$\texttt{MLD}\left(\boldsymbol{x}, \mathcal{L}, \overline{\sigma}\right) = \underset{\boldsymbol{\xi}^{\perp}\in\mathcal{L}^{\perp}/\mathcal{L}}{\arg\max}\, \Theta_{\mathcal{L}+\boldsymbol{\xi}^{\perp}+\boldsymbol{x}}\left(\frac{i}{2\pi\overline{\sigma}^2}\right) \tag{25}$$

is hard.

In ref. [32, p. 450], it has (constructively) been shown that given a soft decoder for a binary code

$C$, we can always solve CVP on the corresponding Construction A lattice $\Lambda(C)$. We explain this point, which also clarifies the geometric picture on decoding concatenated codes presented in eq. (21).

**Lemma 2** ([32], p. 450)**.**

$$\texttt{CVP}(\cdot, \Lambda(C)) = \texttt{Decode}(\texttt{C}). \tag{26}$$

*Proof.* $C$ is embedded in $\mathbb{Z}^n$ by identifying the (scaled and shifted) Construction A lattice $\Lambda(C) = 1 - 2C + 4\mathbb{Z}^n$, where every bit string $\boldsymbol{b} \in C$ is mapped to $1 - 2\boldsymbol{b} \in \{-1, 1\}^n$. In this representation we consecutively solve $\texttt{CVP}(\cdot, 4\mathbb{Z}^n)$ and then apply the soft decoder for $C$, which finds the closest transformed code word $\boldsymbol{c} \in 1 - 2C \in \{-1, 1\}^n$ to input $\boldsymbol{x}' \in \mathbb{R}^n$. As both decoders are exact, with a little care (see ref. [32, p. 450]), this solves CVP exactly. Note that the reverse direction is trivially true via the embedding of $C$ into $\mathbb{R}^n$ provided by Construction A and taking modulo $4\mathbb{Z}^n$. A hard decoder, that solves

$$\arg\min_{\boldsymbol{c} \in C} d_H(\boldsymbol{c}_b, \boldsymbol{x}_b) \tag{27}$$

on binary input $\boldsymbol{x} \in \{-1, 1\}^n$ is also derived from a soft decoder by noticing that $\|\boldsymbol{c} - \boldsymbol{x}\|_2^2 = 4 d_H(\boldsymbol{c}_b, \boldsymbol{x}_b)$, where $\boldsymbol{x}_b$ represents the binary $\{0, 1\}$ representation of $\boldsymbol{x}$ and $d_H$ is the Hamming distance. □

A strategy very similar to the one laid out in this proof has been e.g. employed in ref. [38] to decode the surface-GKP codes employing the minimum-weight-perfect-matching (MWPM) algorithm as soft decoder.

It is known that decoding classical error correcting codes, as specified in eq. (27) is a computationally hard problem in general [40, 41]. Hardness of decoding qubit-based quantum error correcting codes has previously been investigated by reduction to the related problem on classical codes [42] to show its NP-completeness, and by showing its relationship to computing weight enumerators of a linear code, ref. [43] has even shown its $\#P$-hardness in worst case complexity.

By a similar line of argumentation, one notes that the coefficients of the shifted lattice theta function

$$\Theta_{\mathcal{L}+\boldsymbol{x}}(z) = \sum_{m \in \mathbb{Z}} N_m(\mathcal{L}, \boldsymbol{x})\, q^m, \tag{28}$$

with

$$N_m(\mathcal{L}, \boldsymbol{x}) = \#\left\{\boldsymbol{y} \in \mathcal{L} + \boldsymbol{x} : \|\boldsymbol{y}\|^2 = m\right\} \tag{29}$$

counting the number of lattice vectors such that $\mathrm{dist}(\boldsymbol{x}, \mathcal{L})^2 = m$ are hard to compute in general. While we do not attempt to complete such a proof here, we expect a theta-function based analysis of the decoding complexity of quantum error correcting codes using concatenation with single-mode GKP codes to yield similar results as refs. [42, 43].

# 4 GKP codes from NTRU lattices

Random lattices and variations of lattice problems SVP and CVP play a prominent role in classical- and post-quantum cryptography due to their assumed hardness even for quantum computers in the worst-case, as well as due to the feature of worst-case to average-case reductions for such problems [44]. The proof of existence of what we termed *good* GKP codes provided by ref. [18] can in essence be formulated using a Haar average over the moduli space of all symplectic lattices [28]. The analogous heuristic to lower bound the shortest vector in a general lattice is given by the Gaussian heuristic.

**Gaussian Heuristic (GH).** *Let $L \subset \mathbb{R}^n$ be a sufficiently random full rank lattice with large $n$, then we expect the smallest non-zero vector in the lattice will satisfy*

$$\lambda_1(L) \approx \sqrt{\frac{n}{2\pi e}} \det(L)^{\frac{1}{n}}. \tag{30}$$

*Argument* [45, 46]: The moduli space of full rank lattices in $\mathbb{R}^n$ with unit covolume is given by $\mathcal{L}_n = \mathrm{SL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{R})$, where the left[3] quotient $\mathrm{SL}_{2n}(\mathbb{Z})$ indicates the equivalence up to changes of basis. There is a Haar measure $\mu_n$ over $\mathcal{L}_n$, normalized to $\mu_n(\mathcal{L}_n) = 1$, such that for Lebesque-integrable functions $f : \mathbb{R}^n \mapsto R$, we have that [47]

$$\int_{L \in \mathcal{L}_n} f(L \setminus \{0\})\, d\mu_n = \int_{\mathbb{R}^n} f(\boldsymbol{x})\, d\boldsymbol{x}, \tag{31}$$

$$\text{where} \qquad f(L \setminus \{0\}) = \sum_{\boldsymbol{x} \in L \setminus \{0\}} f(\boldsymbol{x}). \tag{32}$$

Let $f(\boldsymbol{x}) = \theta(\|\boldsymbol{x}\| \leq R)$, where $\theta$ is the Heaviside function. Equation (32) yields

$$\left\langle \#\left\{\boldsymbol{x} \in L : \|\boldsymbol{x}\| \leq R,\ \boldsymbol{x} \neq 0\right\} \right\rangle_{L \in \mathcal{L}_n} = V_n(R), \tag{33}$$

where

$$V_n(R) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2} + 1\right)} R^n \tag{34}$$

is the volume of the centered $n-$ball $B_n(R) \subset \mathbb{R}^n$.

We hence have that if lattices $L$ are sampled from a random distribution close to $\mu_n$ in the moduli space of all lattices with $\det(L) = 1$, the average number of non-zero lattice points of length at most $R$ is given by the volume of the $n$-ball, $V_n(R)$. Similarly, it is reasonable to expect that the average number of non-zero lattice points of length at most $R$, when the lattice has $\det(L) \neq 1$ and is sampled from an approximation to the Haar measure is given by $V_n(R) / \det(L)$.

[3] We write the left quotient because of the row-convention used in the definition of lattice bases. In the literature one more commonly uses a right-quotient associated to a column-convention.

Using Stirling's approximation, the smallest $R$ for which this number becomes non-zero is given by $R \approx \sqrt{n/2\pi e}\det(L)^{\frac{1}{n}}$. □

We remark that the Gaussian Heuristic is a statement accepted to be generally true in lattice theory and post-quantum cryptography. In the above "proof sketch" the "heuristic" enters in the assumption that the design property eq. (31) still holds for measures that only approximate the Haar measure on the space of lattices and that it moreover also still holds when the lattices are not of $\det(\mathcal{L}) = 1$.

The Gaussian heuristic motivates that lattices with $\lambda_1 = \Omega(\sqrt{n})$ can be found amongst sufficiently random sets of lattices. Buser and Sarnak [28] showed that there is also a Haar measure over the moduli space of *symplectic* lattices, using which Harrington and Preskill identified the existence of good GKP codes by a similar calculation as presented above [18].

The construction of random lattices is a crucial ingredient to lattice based cryptography.

In this section we introduce the NTRU cryptosystem and show that random *NTRU lattices* obtained from variations of the NTRU cryptosystem are in fact symplectic, such that they allow to construct GKP codes as scaled GKP codes. We discuss scenarios where NTRU lattices are sufficiently random to follow the Gaussian heuristic or, at least, can be shown to admit a lower bound $\lambda_1 \geq \Omega(\sqrt{n})$ with high probability.

The so-derived GKP codes share characteristics of both scaled- and concatenated GKP codes. These NTRU lattices have been originally formulated in the cryptanalysis of attacks on the NTRU cryptosystem [15, 48, 49, 50] and their symplecticity has been motivation to further the study of lattice reduction algorithms for symplectic lattices [30]. As GKP codes, these lattices are particularly interesting as they can be understood as certain generalization of *cyclic* quantum error correcting codes such as the well known $XZZX - [\![5, 1, 3]\!]$ quantum error correcting code [51] or the repetition code and have a similar algebraic basis as the recently introduced lifted product codes [25].

## 4.1 The NTRU cryptosystem

We describe the NTRU cryptosystem to the degree necessary to understand the structure of the corresponding lattices and GKP codes constructed here. For more detail we refer the reader to the cited literature. The presentation here is largely derived from the presentations in refs. [15, 49, 50, 52, 17, 53].

The NTRU cryptosystem is most natively formulated using polynomial rings $R = \mathbb{Z}[x]/\Phi$, where we will take the quotient $\Phi = x^n + \phi_{n-1}x^{n-1} + \ldots + \phi_0$ as $\Phi = \Phi_0 := x^n - 1$ in the bulk of this paper, as used in the original description of the (heuristically secure) NTRU cryptosystem [15]. We will keep $\Phi$ general whenever possible to be able to discuss the provably secure version of the NTRU cryptosystem [17] with irreducible $\Phi = x^n + 1$ later. We denote $R_q = R/qR$ with a typically large modulus parameter $q$ and $R_p = R/pR$ with a typically small $p$ coprime with $q$. Whenever we take the modulus, $\bmod q$ or $\bmod p$, we refer to the (coefficient-wise) reduction into the centered fundamental domains $\left[-\frac{q}{2}, \frac{q}{2}\right]$ resp. $\left[-\frac{p}{2}, \frac{p}{2}\right]$.

We denote multiplication in $R$ as $fg \bmod \Phi$, $f, g \in R$, where we assume the reduction $\bmod \Phi$ ($\bmod q/p$) to be implicit by specifying the image and use a bold $\boldsymbol{f} = \mathrm{coeff}(f)$ to refer to the coefficient vector $\boldsymbol{f} = (f_0, f_1, \ldots, f_{n-1})$ of $f \in R$ (note that any polynomial in $R$ can be represented with $n-1$ coefficients, for that every power $x^n$ can be replaced by $x^n - \Phi$ when working over $\bmod \Phi$.

Denote the uniform distribution of polynomials $p \in R_q$ with $d_1$ coefficients $+1$, $d_2$ coefficients $-1$ and $n - (d_1 + d_2)$ coefficients 0 as $D(d_1, d_2)$. Further denote the set of invertible elements in $R_q$, i.e., elements $f$ for which $f^{-1} \in R_q$ exists, as $R_q^\times$.

The NTRU cryptosystem, specified by parameters $(n, \Phi, d, q, p)$ operates as follows:

1. **Key generation**: Sample $\tilde{f} \hookleftarrow D(d, d)$ until $f = 1 + p\tilde{f} \in R_q^\times$, sample $\tilde{g} \hookleftarrow D(d, d)$ to obtain $g = p\tilde{g}$. Return the secret key pair $(f, g)$, and the public key $h = gf^{-1} \in R_q$.

2. **Encryption**: Given the public key $h \in R_q$ and a message $m \in R_p$, sample a random polynomial $r \in R_p$ and compute the ciphertext $c = hr + m \in R_q$.

3. **Decryption**: Given the ciphertext $c$ and secret key $f$, compute $cf \bmod q \bmod p = gr + fm \bmod q \bmod p = m \in R_p$.

The secret key polynomials $(f, g) \in R_q^\times \times R_q$ are by construction such that $f \bmod p = 1$ and $g \bmod p = 0$. Decryption is guaranteed to be successful whenever all the coefficients involved are sufficiently small, such that $cf = gr + fm$ holds as equality in $R$, and not just merely in $R_q$ [45].

## 4.2 Symplectic ideal and NTRU lattices

The security assumption underlying this cryptosystem as the in-retrievability of the secret key is the hardness of the polynomial factorization problem in $R_q$ and secret key retrieval attacks have been formulated already in early analyses of the NTRU cryptosystem [15, 48, 50].

**Assumption 1** (Polynomial factorization problem [50])**.** *Given a polynomial $h = f^{-1}g \in R_q$ where the coefficients are small compared to $q$. For suitable parameter settings it is intractable to find small polynomials $f', g' \in R_q$ such that $f'h = g' \in R_q$.*

Under the premise that the coefficient vectors of the secret key $(f, g)$ are *short*, a typical attack is formulated as the task of finding short polynomials $(f', g') \in R_q^2$ such that $fh = g \in R_q$, where the length of the polynomial pair is defined as the norm of their joined coefficient vectors $\|(f', g')\|_l = \|(\boldsymbol{f'}^T, \boldsymbol{g'}^T)\|_l$. We will use the $l = 2$ norm unless specified otherwise. The attack is carried out by defining the NTRU lattice as an $R$-module $L_R \subseteq R^2$, which admits a basis in its Hermite normal form

$$H_R = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}. \tag{35}$$

Elements of the $R$-lattice are of the form

$$\begin{aligned} (f'\ u)H_R &= (f'\ u)\begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} \\ &= (f'\ \ f'h + uq) \\ &= (f', f'h + uq),\ (f', u) \in R^2, \end{aligned} \tag{36}$$

each of which represent admissible solutions to the equation $f'h = g' \in R_q$, such that short vectors in $L_R$ are expected to correspond to the NTRU secret key pair. In a more general classification, one can view the $R$-lattice $L_R = L_R(h)$ as an rank-2 ideal lattice [54], corresponding to the principal ideal $I = \langle h \rangle \subseteq R$.

$H_R$ is, in fact, also a $q$-symplectic matrix in $R^{2\times 2}$, with respect to the symplectic form

$$J_R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in R^{2\times 2}, \tag{37}$$

with

$$H_R J_R H_R^T = \begin{pmatrix} h^T - h & q \\ -q & 0 \end{pmatrix} = qJ_R \in R^{2\times 2} \tag{38}$$

because $h$ is a scalar in $R$.

Analyses of lattices and associated algorithms are typically formulated over $\mathbb{Z}$-lattices, where linear combinations of basis vectors are taken with integer coefficients. We map the rank-2 $R$-lattice $L_R$ to a rank-$2n$ $\mathbb{Z}$-lattice $L \subseteq \mathbb{Z}^{2n\times 2n}$ by defining a homomorphism onto a $\mathbb{Z}^{n\times n}$ matrix

$$C_\Phi :\ R \to \mathbb{Z}^{n\times n} \tag{39}$$

$$f \mapsto C_\Phi(f), \tag{40}$$

$$(C_\phi(f))_{i,j} = (T_\Phi^i \boldsymbol{f})_j,\ i, j = 0, \ldots, n-1, \tag{41}$$

where the rows are given by the vectors $T_\Phi \boldsymbol{f}$ and

$$T_\Phi = \begin{pmatrix} \boldsymbol{0}^T & -\phi_0 \\ I_{n-1} & -\boldsymbol{\phi}_{1:n-1} \end{pmatrix} \tag{42}$$

implements the map $f \mapsto xf \mod \Phi \in R$ on the coefficient vector $\boldsymbol{f}$ of $f$ by left multiplication.

$C_\Phi$ is linear over $\mathbb{Z}$, such that we can express the homomorphism on every polynomial $f \in R$ as

$$\begin{aligned} C_\Phi(f) &= \sum_{i=0}^{n-1} f_i C_\Phi\left(x^i\right) \\ &= \sum_{i=0}^{n-1} f_i C_\Phi(1)\left(T_\Phi^T\right)^i, \\ &= \sum_{i=0}^{n-1} f_i \left(T_\Phi^T\right)^i, \end{aligned} \tag{43}$$

where we have used that $C_\Phi(1) = I_n\ \forall\Phi$. In this representation, it is evident that $C_\Phi(f)$ acts via right action

$$\text{coeff}(fg \mod \Phi) = \boldsymbol{f}^T C_\Phi(g) = \boldsymbol{g}^T C_\Phi(f) \tag{44}$$

and that

$$C_\Phi(fg \mod \Phi) = C_\Phi(f) C_\Phi(g) \tag{45}$$

indeed represents a homomorphism. When $\Phi = \Phi_0 = x^n - 1$, $C_\Phi(f)$ is simply the (row) circulant matrix of the coefficient vector $\boldsymbol{f}$. Circulant matrices are not symmetric, but have a mirror symmetry along the anti-diagonal, $R_n C_{\Phi_0}^T(f) R_n = C_{\Phi_0}(f)$, where $R_n$ is the anti-diagonal matrix $(R_n)_{i,j} = \delta_{i,n-1-j}$, $i, j = 0, \ldots, n-1$. We also define a related map

$$A_\Phi :\ R \to \mathbb{Z}^{n\times n}, \tag{46}$$

$$f \mapsto A_\Phi(f), \tag{47}$$

$$(A_\phi(f))_{i,j} = (T_\Phi^{-i}\boldsymbol{f})_j,\ i, j = 0, \ldots, n-1, \tag{48}$$

where $T_\Phi^{-i} = \left(T_\Phi^{-1}\right)^i$ and for $\Phi = \Phi_0 = x^n - 1$ this is the symmetric anti-circulant matrix of the coefficient vector $\boldsymbol{f}$, $A_{\Phi_0}^T(f) = A_{\Phi_0}(f)$. Since $A_\Phi$ is also $\mathbb{Z}$-linear, here we have

$$\begin{aligned} A_\Phi(f) &= \sum_{i=0}^{n-1} f_i A_\Phi\left(x^i\right) \\ &= A_\Phi(1) C_\Phi(f), \end{aligned} \tag{49}$$

where, for $\Phi = \Phi_0 = x^n - 1$, we have that

$$A_\Phi(1) = \begin{pmatrix} 1 & 0 \\ \boldsymbol{0} & \overline{I}_{n-1} \end{pmatrix} =: \sigma \tag{50}$$

is the orthogonal coefficient mirror $\sigma = \sigma^T$ that maps the coefficient vector $f(x) \in R$ to that of $f\left(x^{-1}\right) = f\left(x^{n-1}\right) \in R$ [50].

The so-defined maps allow us to map the earlier defined $R$-lattice $L_R$ onto a lattice $L = L(h) \subseteq \mathbb{Z}^{2n}$ by applying the corresponding homomorphism on the entries of the basis

$$H_R = \begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix} \mapsto H = \begin{pmatrix} I_n & C_\Phi(h) \\ 0 & qI_n \end{pmatrix}. \tag{51}$$

It can be checked that the lattice spanned by the basis contains all secret key pairs $(\boldsymbol{f'}^T\ \boldsymbol{g'}^T)$ corresponding

to solutions $fh = g \in R_q$. It is however not symplectic. For $\Phi = \Phi_0$ we, however, have that

$$H^{cs} = \begin{pmatrix} I_n & A_{\Phi_0}(h) \\ 0 & qI_n \end{pmatrix} = \begin{pmatrix} I_n & \sigma C_{\Phi_0}(h) \\ 0 & qI_n \end{pmatrix} \tag{52}$$

is indeed symplectic and corresponds to a rotation of the lattice $L$,

$$(\sigma \oplus I_n) H^{cs} = H_{\mathbb{Z}} (\sigma^T \oplus I_n), \tag{53}$$

since $(\sigma \oplus I_n)$ is unimodular. This is the basis used by Coppersmith and Shamir in their attack on the NTRU cryptosystem [48, 50]. We generalize this observation to the following statement.

**Lemma 3.** *An NTRU lattice $L \subseteq \mathbb{Z}^{2n} \subset \mathbb{R}^{2n}$ given by generator*

$$H_{\mathbb{Z}} = \begin{pmatrix} I_n & C_\Phi(h) \\ 0 & qI_n \end{pmatrix} \tag{54}$$

*is equivalent to a $q$-symplectic lattice $L' \subset \mathbb{R}^{2n}$ for all $h$ if there exists a signed permutation matrix $\sigma_\Phi \in \mathbb{Z}^{n\times n} \cap O(n)$ such that*

$$(\sigma_\Phi C_\Phi(h))^T = \sigma_\Phi C_\Phi(h) \tag{55}$$

*is symmetric.*

*Proof.* A lattice generated by $M$ is equivalent to a lattice generated by $M'$, such that $\det M = \det M'$ if and only if there exists a unimodular matrix $U$ and an orthogonal matrix $O$ such that $M' = UMO$ [32]. Take $O = \left(\sigma_\Phi^T \oplus I_n\right)$ and $U = (\sigma_\Phi \oplus I_n)$. □

**Corollary 1.** *NTRU lattices over $\Phi = \Phi_0$ and $\Phi = x^n + 1$ are equivalent to $q$-symplectic lattices*

*Proof.* For $\Phi = \Phi_0$ we already saw earlier that $\sigma_{\Phi_0} = \sigma$ provides a symmetric matrix $\sigma C_\Phi(h)$ for all $h$. For $\Phi = x^n + 1$ this is also the case, with

$$\sigma_\Phi = \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & -\overline{I}_{n-1} \end{pmatrix} = A_\Phi(1) \tag{56}$$

and $A_\Phi(1) C_\Phi(h) = A_\Phi(h)$ is such that the first row is $\boldsymbol{h}^T$ and every other row is generated by permuting the first element around the "periodic boundary" on the right to the left while adding a $-1$ factor. This matrix is clearly symmetric and $\sigma, \sigma_\Phi$ are signed permutations. □

Finally, the fact that these NTRU lattices $L$ corresponds to ideals $I = \langle h \rangle \subseteq R$ equips them with the symmetry $L = (T_\Phi \oplus T_\Phi)L$. When $\Phi = \Phi_0$ we have that the symmetry is $n$-fold, $T_{\Phi_0}^n = I$ and similarly for $\Phi = x^n + 1$ we have $T_\Phi^n = -I$.

Henceforth we will default to $\Phi = \Phi_0$ unless otherwise specified and omit the corresponding $\Phi_0$ index from $C_{\Phi_0}$ and $A_{\Phi_0}$. The anti-circulant matrix $A(h) = \sigma C(h)$ implements a homorphism from $R$ with respect to a modified matrix multiplication

$$A(f)\, \sigma A(h) = \sigma C(f)\, C(f) = A(fg). \tag{57}$$

We denote $A(f)\,\sigma =: A^\sigma(f)$, such that $A^\sigma(f)\, A(g) = A(f)$.

On $\mathbb{Z}^n$, ciphertexts produced by the NTRU encryption with secret key pair $(f, g)$ and public key $h$ take the form

$$\begin{aligned} \boldsymbol{c}^T &= \boldsymbol{m}^T + \boldsymbol{r}^T C(h) \mod q \\ &= \boldsymbol{m}^T + (\sigma \boldsymbol{r})^T \sigma C(h) \mod q \end{aligned} \tag{58}$$

and decryption is carried out by left-multiplying with $A^\sigma(f)$ and reducing $\mod q$ and $\mod p$.

The corresponding $q$-symplectic generator of the underlying lattice is given by

$$H = \begin{pmatrix} I_n & A(h) \\ 0 & qI_n \end{pmatrix}, \tag{59}$$

which is already a $q$-symplectic basis for the weakly symplectically self-dual lattice $L$.

We use this lattice as starting point to define a scaled GKP-code by taking $\mathcal{L} = \sqrt{(\lambda/q)}L$ with generator $M = \sqrt{(\lambda/q)}H$. Similar to the discussion earlier, the GKP code built this way will encode $D = \lambda^n$ logical dimensions with symplectic dual

$$\mathcal{L}^\perp = L/\sqrt{\lambda q} \tag{60}$$

and distance

$$\Delta = \lambda_1(L)/\sqrt{\lambda q}. \tag{61}$$

For randomly chosen $f, g \in \mathcal{R}$, the Gaussian heuristic gives an estimate for the shortest vector length and has been used in the original NTRU work to argue about the security of the scheme [15]. If the Gaussian heuristic were to hold, the so-constructed NTRU lattices would attain parameters

$$D = \lambda^n, \tag{62}$$

$$\Delta \geq \sqrt{\frac{n}{\lambda \pi e}}, \tag{63}$$

which are *good*.

However, the Gaussian heuristic does not always hold for NTRU lattices with arbitrary parameters. Due to the the sub-lattice $q\mathbb{Z}^{2n} \subset L$ there always exist trivial vectors $q\boldsymbol{e}_i$, $i \in [1, 2n]$ of length $q$ in $L$ which yield logically non-trival vectors of length $\sqrt{q/\lambda}$. A shortest vector length $\lambda_1(L)$ growing with $\sqrt{n}$ can however be maintained by choosing suitably large $q$ scaling with $n$. Furthermore, NTRU lattices (with $\Phi_0$) are constrained by 1. being *cyclic* lattices and 2. having an existing inverse of $f \in R_q$ and 3. having a fixed number $2d$ of non-zero coefficients in the vector corresponding to the secret key $(\sigma(\boldsymbol{f})^T, \boldsymbol{g}^T)^T \in L$,

which on the one hand make it not immediately clear if they would be sufficiently random for the Gaussian heuristic to hold, and on the other hand already present short vectors of length $\leq O(\sqrt{d})$. These points have been addressed in refs. [55, 16], where the authors show the following statement.

**Corollary 2** ([55, 16, Corollary 3]). *If $d = \lfloor n/3 \rfloor$, then with probability greater than $1-2^{-0.1n}$ the shortest vector in a random NTRU lattice has length greater than $\sqrt{0.28n}$.*

This statement gives us confidence to claim that random NTRU lattice based GKP codes as constructed above can be expected to be *good* when the parameters are chosen properly, as summarized by the following.

**Proposition 1** (Good codes from NTRU lattices). *A GKP code with $\mathcal{L} = \sqrt{(2/q)}L$, where $L$ is the NTRU lattice over $\Phi_0$ specified in the basis eq. (59) with $d = \lfloor n/3 \rfloor$ encodes*

$$k = n \tag{64}$$

*qubits and has with probability greater than $1-2^{-0.1n}$ a distance given by*

$$\Delta = \min\left\{\sqrt{\frac{0.14n}{q}}, \sqrt{\frac{q}{2}}\right\}. \tag{65}$$

*For sufficiently large constant $q$ and $n \leq q^2/0.28$ this defines a randomized family of good GKP codes.*

*Proof.* Follows immediately from corollary 2 and the GKP-code construction laid out in the main text. □

### 4.3 Numerical results

In fig. 3, we have computed the shortest vector lengths for $N_{\text{sample}} = 100$ randomly sampled NTRU lattices for varying $q$ and $n$ with $p = 3$. We compare samples over NTRU-like random cyclic lattices, where $h$ is sampled randomly from $R_q$ in row $a$) with NTRU lattices over $\Phi = x^n - 1$ with $f$ invertible in $R_q$ and bounded non-zero entries $d = \lfloor n/3 \rfloor$ (in row $b$)). We also compare the average length of shortest vectors for even more constrained NTRU lattices where we also required the public key $h$ to be invertible in $R_q$ in row $c$. In this case we obtain $g$ from the amended distribution $g \sim pD(d+1, d)$ since otherwise $g$ – and thus $h$ – would have a trivial root $g(1) = 0$ rendering the polynomial non-invertible. Finally, in row $d$), we perform the experiment using the setup of ref. [17], where the quotient $\Phi = x^n + 1$ is chosen to be irreducible and $n$ is a power of 2.

In our statistics we observe that random cyclic lattices (row $a$) appear to agree well with the Gaussian heuristic, while the growth of the shortest vector length of the NTRU lattices in row $b$) and $c$) degrades with increasing $q$, consistent with the bound given in Corollary 2. Based on our numerics, we also conjecture the following.

**Conjecture 1** (Good GKP codes). *A GKP code with $\mathcal{L} = \sqrt{\lambda/q}L$, where $L$ is specified by the basis in (59) and $h$ is selected at random from $R_q = \mathbb{Z}_q[x]/\langle x^n - 1\rangle$, is likely a good code with $k = n$ and*

$$\Delta \geq \min\left\{\sqrt{\frac{n}{\lambda\pi e}}, \sqrt{\frac{q}{\lambda}}\right\}. \tag{66}$$

Finally, in row $d$) we observe a good agreement of the shortest vector lengths with the scaling proposed by the Gaussian heuristic. In ref. [17] a probabilistic lower bound on the smallest infinity norm $\lambda_1^\infty(L)$ has been proven, which we include in the figure. As we will discuss later in the manuscript, GKP codes derived from this particular NTRU setup is is of cryptographic relevance. Based on our numerical observations we hence also conjecture that such GKP codes are likely to be good.

**Conjecture 2** (Good GKP codes). *A GKP code with $\mathcal{L} = \sqrt{\lambda/q}L$, where $L$ with $\det L = q^n$ is equivalent to NTRU lattice specified by the basis in (59) and $h = g/f \leftarrow f, g$ are sampled at random from a Gaussian distribution with variance $\sigma^2 = q$ in $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, $q \geq \texttt{poly}(n)$ and $n \geq 8$ a power of 2 is likely a good code with $k = n$ and*

$$\Delta \geq \sqrt{\frac{n}{\lambda\pi e}}. \tag{67}$$

In contrast to the previous statement in proposition 1, these distance bounds do not suffer from choosing larger modulus $q$, but we can pick it arbitrarily large to obtain high distances.

The trivial sub-lattice $L_q = q\mathbb{Z}^{2n} \subseteq L$ which enforces the $q$ modularity in the cryptographic setup is analogue to the structure of concatenated (hypercubic) GKP codes $\mathcal{L}_{\text{triv}} = \sqrt{\lambda q}\mathbb{Z}^{2n} \subseteq \mathcal{L}$, such that the lattices $\mathcal{L}$ defined above may be interpreted as a concatenated (qudit) GKP code where $\mathcal{L}_{\text{triv}}$ defines the underlying single mode qudit-code with $D = \lambda q$. It is interesting that this class of NTRU-GKP codes thus shares characteristics of both *scaled-* as well as *concatenated* GKP codes.

## 5 Decoding GKP codes from NTRU lattices

A code state that (either through a natural error process or by deliberate modification) undergoes a displacement by

$$\boldsymbol{e} = \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{y} \end{pmatrix} \tag{68}$$

gives rise to trivial syndrome

$$\boldsymbol{s}_{\text{triv}} = \sqrt{\lambda q}\boldsymbol{e} \mod 1. \tag{69}$$

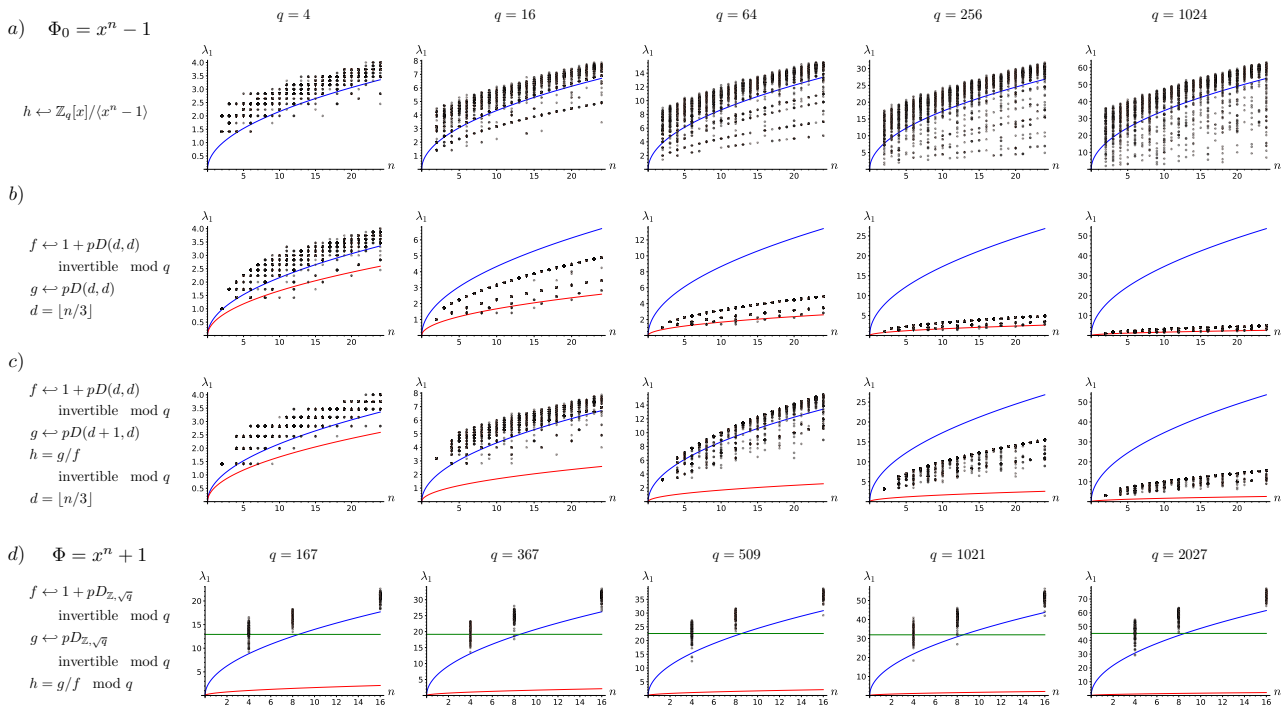



Figure 3: Shortest vector lengths computed via full HKZ reduction of $a)$ random cyclic ($\Phi_0 = x^n - 1$) lattices as generated by the hard lattice generator in sagemath, $b)$ random NTRU lattices with $p = 3$ and $d = \lfloor n/3 \rfloor$ and $c)$ random NTRU lattices where $h$ is invertible in $R_q$ for varying $q = 2, \ldots, 2048$. In $d)$ we sample NTRU lattices generated with the irreducible quotient $\Phi = x^n + 1$, where $n$ is a power of 2. For each $n \in [2, 24]$ we sample 100 NTRU lattices and compute the shortest vector by computing the HKZ reduced lattice basis. For reference, we plot the expected shortest vector length from the Gaussian heuristic $\lambda(n) = \sqrt{nq/\pi e}$ in blue and the expected lower bound $\lambda_0(n) = \sqrt{0.28n}$ in red. In panel $d)$, we have also included a green line at $\sqrt{q}$, which is the standard deviation of the discrete Gaussian distribution $f, g$ are sampled from and is related to a probabilistic lower bound for $n \geq 8$ a power of 2 on the shortest infinity norm $\lambda_1^\infty(L)$ derived in ref. [17]. The sagemath [56] code as well as all numerical data presented here is available under ref. [57]. The sagemath functionalities to construct NTRU lattices are partially adapted from ref. [58].

Due to the simple orthogonal structure of $\mathcal{L}_{\text{triv}}$ a first step of the correction is easily carried out by applying the correction $\boldsymbol{\eta} = -\boldsymbol{s}_{\text{triv}}/\sqrt{\lambda q}$. After correcting for the trivial syndrome (associated to the underlying hypercubic GKP code) the remaining error is the unknown, but likely short, vector

$$\boldsymbol{e}' = \frac{1}{\sqrt{\lambda q}} \begin{pmatrix} \boldsymbol{u} \\ \boldsymbol{v} \end{pmatrix} \in \mathcal{L}_{\text{triv}}^{\perp},\ \boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}^n. \tag{70}$$

The residual error can be considered as living on the scaled $q$-ary lattice

$$\mathcal{L}_q = \frac{1}{\sqrt{\lambda q}} \mathbb{Z}_q^{2n} \tag{71}$$

dual to the trivial stabilizer lattice and has a probability distribution induced by the trivial syndrome and correction

$$P(\boldsymbol{e}') \propto \sum_{\boldsymbol{t} \in \mathcal{L}_{\text{triv}}} e^{-\frac{(\boldsymbol{e}' + \boldsymbol{s}_{\text{triv}} + \boldsymbol{t})^2}{2\bar{\sigma}^2}}. \tag{72}$$

The remaining syndrome is

$$\begin{aligned} \boldsymbol{s} &= MJ\boldsymbol{e}' \mod 1 \\ &= \frac{1}{q} \begin{pmatrix} \boldsymbol{v} - A(h)\,\boldsymbol{u} \mod q \\ 0 \mod 1 \end{pmatrix}. \end{aligned} \tag{73}$$

In the first block of the syndrome $q\boldsymbol{s}_1 = \boldsymbol{v} - A(h)\,\boldsymbol{u} \mod q$ we recognize the structure of the NTRU ciphertext. The position of the message is taken by $\boldsymbol{m} = \boldsymbol{v}$ and the random vector is replaced by $\boldsymbol{r} = -\sigma(\boldsymbol{u})$. Following the standard NTRU decryption process now allows to obtain $\boldsymbol{v} \mod q \mod p$ as well as

$$\boldsymbol{u} = qA^{\sigma}\left(h^{-1}\right)(\boldsymbol{v} - q\boldsymbol{s}_1) \mod q \tag{74}$$

when $h$ is also chosen to by invertible in $R_q$ with inverse $h^{-1}$. When $p$ is not prime, we can instead obtain $\boldsymbol{u} \mod q \mod p_i$ for each prime factor $p_i$ of $p$ and estimate $\boldsymbol{u} \mod q$ via the Chinese remainder theorem. We refer to this decoding routine as `NTRUDecode` and provide some small scale numerical tests in appendix C.

Alternatively, we can decompose the remaining syndrome as

$$q\boldsymbol{s} = \begin{pmatrix} \boldsymbol{v} \\ -\boldsymbol{u} \end{pmatrix} + \underbrace{\begin{pmatrix} -A(h)\,\boldsymbol{u} \\ \boldsymbol{u} \end{pmatrix}}_{\in \mathcal{L}_{\text{cs}}^{J}}, \tag{75}$$

where the vector on the RHS is element of the flipped NTRU lattice generated by the public basis

$$H^J = \begin{pmatrix} qI & 0 \\ -A(h) & I \end{pmatrix}. \tag{76}$$

Equation (75) shows that a likely, i.e., small, error vector $\begin{pmatrix} \boldsymbol{v} \\ -\boldsymbol{u} \end{pmatrix}$ can indeed be obtained by solving CVP $\left(\mathcal{L}^J, q\boldsymbol{s}\right)$. In appendix C, we implement an approximation of this CVP instance using Babai's nearest plane algorithm with the HKZ reduced flipped public basis as `BabaiDecode` again only for small parameters $n$.

We recognize that the solving CVP or BDD on the respective NTRU lattices provides a viable route to decoding. To analyze how well decoding can be carried out efficiently when provided only the public- vs. the secret basis, we analyze the radius $\epsilon$, up to which $\texttt{BDD}_\epsilon$ can be implemented given the respective bases.

## 5.1 Bounding $\texttt{BDD}_\epsilon$

The maximum $\texttt{BDD}_\epsilon$-radius achieved by using Babai's nearest plane algorithm using this basis $B = \left(\boldsymbol{b}_1^T \ldots \boldsymbol{b}_{2n}^T\right)^T$ is given by

$$\epsilon = \frac{1}{2} \min_i \|\tilde{\boldsymbol{b}}_i\|, \tag{77}$$

where we write $\tilde{B} = (\tilde{\boldsymbol{b}}_1^T, \ldots, \tilde{\boldsymbol{b}}_{2n}^{*T})^T$ for the Gram-Schmidt orthogonalization of $B$.

The secret key pair $(f, g)$ can be extended to a full rank secret basis [59, 60, 17]

$$B_R = \begin{pmatrix} f & g \\ F & G \end{pmatrix} \in R^{2\times 2} \tag{78}$$

$$\mapsto B_{\mathbb{Z}} = \begin{pmatrix} C_\Phi(f) & C_\Phi(g) \\ C_\Phi(F) & C_\Phi(G) \end{pmatrix} \in \mathbb{Z}^{2n\times 2n}, \tag{79}$$

which constitutes an equivalent lattice basis in $R^2$ if $F, G \in R$ are such that $fG - gF = q \in R$, that is if

$$\begin{aligned} B_R J B_R^T &= \begin{pmatrix} f & g \\ F & G \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} f & F \\ g & G \end{pmatrix} \\ &= \begin{pmatrix} 0 & fG - gF \\ gF - fG & 0 \end{pmatrix} = qJ \end{aligned} \tag{80}$$

is symplectic in $R^2$. The vector $(F, G) \in R^2$ is typically chosen to be the minimal representative modulo multiples of $(f, g)$ in $R$ and can be approximated efficiently using Babai's algorithm [59, 60, 17]. By applying the circulant homomorphism, this secret basis is mapped to a secret basis for the lattice in $\mathbb{Z}^{2n}$ on which the GKP-NTRU lattice is defined – note that the symplectic basis obtained from the public key, eq. (59) is obtained from this by a rotation and change of basis using $\sigma_\Phi$. Due to this simple relationship, we perform the following analysis in the non-rotated basis w.l.o.g. .

By leveraging symplecticity, we can derive lower bounds on the `BDD`-radius achieved using this secret basis. By comparing this to solving `BDD` when the input public basis is $\delta$-LLL reduced, we obtain an almost exponential separation between the BDD radius provided by the public and private basis.

**Proposition 2.** *Let $q \geq n$. Using the secret basis*

$$B = \begin{pmatrix} C_\Phi(f) & C_\Phi(g) \\ C_\Phi(F) & C_\Phi(G) \end{pmatrix}, \tag{81}$$

*Babai's algorithm solves* $\texttt{BDD}_\epsilon$ *with*

$$\epsilon_B \geq q \left(2 \max \left\{ \| \left(\boldsymbol{f}, \boldsymbol{g}\right) \|, \| \left(\boldsymbol{F}, \boldsymbol{G}\right) \| \right\}\right)^{-1}, \tag{82}$$

*which is at worst on a scale of* $O\left(1/\texttt{poly}(n)\right)$*, while using the* $\delta$*-LLL reduced public basis obtained from*

$$H = \begin{pmatrix} I & C_\Phi(h) \\ 0 & qI \end{pmatrix}, \tag{83}$$

*we have*

$$\epsilon_H \leq \frac{\lambda_1\left(L\right)}{2} e^{-\sqrt{n \ln\left(q\right) \ln\left(1/\delta\right)}}, \tag{84}$$

*which is on a scale of* $o(e^{-\sqrt{n \ln n \ln\left(1/\delta\right)}})$.

*Proof.* We define the conjugation of polynomials $R \mapsto R:\ f \mapsto \overline{f} \Leftrightarrow \boldsymbol{f} \mapsto \sigma_\Phi \boldsymbol{f}$ such that $C_\Phi(\overline{f}) = C_\Phi(f)^T$. Using the homomorphism to circulants we have that

$$B_{\mathbb{Z}} = \begin{pmatrix} C_\Phi(f) & C_\Phi(g) \\ C_\Phi(F) & C_\Phi(G) \end{pmatrix}, \tag{85}$$

$$\overline{B}_{\mathbb{Z}} = \begin{pmatrix} C_\Phi(\overline{f}) & C_\Phi(\overline{g}) \\ C_\Phi(\overline{F}) & C_\Phi(\overline{G}) \end{pmatrix}, \tag{86}$$

$$B_{\mathbb{Z}} J \left(\frac{1}{q} \overline{B}_{\mathbb{Z}}\right)^T = J, \tag{87}$$

$$\left(\frac{1}{q} J^T \overline{B}_{\mathbb{Z}}\right) J B_{\mathbb{Z}}^T = I, \tag{88}$$

where the last line is obtained using the defining operation $fG - gF = q \in R$. We will from now on omit the subscript $_{\mathbb{Z}}$. This equation identifies the canonical symplectic dual of the basis $B_{\mathbb{Z}}$ as

$$B^\perp = \frac{1}{q} J^T \overline{B}, \tag{89}$$

which is related to the canonical euclidean dual by a $J-$rotation [12]

$$B^* = B^\perp J = \frac{1}{q} J^T \overline{B} J. \tag{90}$$

Let $\tilde{B} = \texttt{GS}\left(B\right)$ the Gram-Schmidt diagonalization of $B$ and

$$\hat{B}^* = R_{2n}^T \texttt{GS}\left(R_{2n} B^*\right) = \frac{1}{q} R_{2n}^T \texttt{GS}\left(R_{2n} J^T \overline{B}\right) J, \tag{91}$$

the Gram-Schmidt diagonalization of the canonical euclidean dual $B^*$ in reverse order, where $R_{i,j} = \delta_{n-i,j}$ and $R_{2n} = R \oplus R$. We have that

$$\|\tilde{\boldsymbol{b}}_i\| \|\hat{\boldsymbol{b}^*}_i\| = 1 \, \forall i, \tag{92}$$

such that

$$\min_i \|\tilde{\boldsymbol{b}}_i\| = \frac{1}{\max_i \|\hat{\boldsymbol{b}^*}_i\|}. \tag{93}$$

The Gram-Schmidt norm is trivially upper bounded by

$$\|\hat{B}^*\|_{\text{GS}} = \max_i \|\hat{\boldsymbol{b}^*}_i\| \leq \max \left\{ \| \left(\boldsymbol{f}, \boldsymbol{g}\right) \|, \| \left(\boldsymbol{F}, \boldsymbol{G}\right) \| \right\} / q, \tag{94}$$

such that we obtain

$$\min_i \|\tilde{\boldsymbol{b}}_i\| \geq 1/\|\hat{B}^*\|_{\text{GS}} = q / \max \left\{ \| \left(\boldsymbol{f}, \boldsymbol{g}\right) \|, \| \left(\boldsymbol{F}, \boldsymbol{G}\right) \| \right\}. \tag{95}$$

This lower bound on the Gram-Schmidt norm of the secret basis is large, when the secret key pairs $(f, g), (F, G)$, with length on a scale of $\Omega\left(\sqrt{n}\right)$ are short relative to $q \geq n$, which is expected to be the case by construction of the cryptosystem. More concretely, for $\Phi = x^n + 1$, the NTRUSign construction in [17, Lemma 4.6] asserts that $(F, G)$ can be found such that $\|(F, G)\| \leq \sigma n$, where $\sigma \approx n^c \sqrt{q}$ is the standard deviation of the discrete Gaussian distribution used to sample the discrete Gaussians. This bound yields a BDD radius not smaller than $\epsilon_B \sim O\left(1/\texttt{poly}(n)\right)$.

We compare this to the bound obtained from the public basis, when the input basis $H$ is $\delta$-LLL reduced [61]. Building on an argument by Eldar and Hallgreen, Ducas and van Woerden [62, 63] have shown that for a $q$-ary lattice (for $q = c^n$), Babai's algorithm can solve BDD up to

$$\epsilon_H = \frac{\lambda_1\left(L\right)}{2} e^{-\sqrt{n \ln\left(q\right) \ln\left(1/\delta\right)}}, \tag{96}$$

which has also been extended to general $q$ in ref. [64]. □

## 5.2 Quantum public key communication from NTRU-GKP codes

In addition to its usual use as a QECC, the fact that the NTRU-GKP codes have the additional property that *decoding* for a stochastic displacement noise model is tightly related to *decrypting* the NTRU cryptosystem suggests that the NTRU-GKP codes presented here may be used for both, quantum error correction and a new kind of quantum public key communication scheme at the same time. One may interpret NTRU-GKP codes as *trapdoor decodable quantum error correcting codes*. That is, while stabilizer measurements can be performed and code states prepared using only access to the public key $h$, knowledge of the corresponding secret keys $(f, g)$ of the NTRU cryptosystem is necessary for reliable and efficient decoding.

In the following, we outline how instances of the NTRU-GKP code can be used to set up a *private quantum channel* [65] with quantum information being sent from Bob to Alice, in that quantum information is transmitted in a fashion that is oblivious

to an eavesdropper with limited computational power who has access to the physical quantum channel used for transmission. This setup is based on the observation that an attacker capable of decoding instances of the NTRU-GKP code by solving CVP on the related lattice also allows her successfully retrieve the message from the ciphertext of the corresponding NTRU cryptosystem.

The workings of the here proposed cryptosystem is similar to that of a *one time pad* (OTP), where every OTP instance corresponds to a random displacement error applied to an NTRU-GKP code instance such that the syndrome of the random displacement error encodes a ciphertext of the NTRU scheme. The security of this scheme under the assumption that decoding a quantum error correcting code – i.e., finding small errors that are consistent with the syndrome – is *necessary* to retrieve its logical content is then immediately inherited from the corresponding classical NTRU cryptosystem. While we have carried out most of our exposition with the only heuristically secure version of the NTRU cryptosystem originally presented in ref. [15] with quotient $\Phi_0 = x^n - 1$ and secret key sampling from the uniform binary distributions $D(d_1, d_2) \subseteq \{-1, 0, +1\}^n$, we have also shown that NTRU-GKP codes can be constructed using irreducible quotients $\Phi = x^n + 1$, $n$ a power of 2, and $q \geq \text{poly}(n)$ while secret key pairs are sampled from discrete Gaussian distributions. This is the setting chosen for a provably secure version of the NTRU cryptosystem discussed in ref. [17], where the public key is shown to be pseudorandom and security is inherited from the (average-case) hardness of the ring based $\mathtt{R}-\mathtt{SIS}$ and $\mathtt{R}-\mathtt{LWE}$ problem.

The public key protocol, also described in fig. 4 is sketched as follows:

1. Alice samples a secret key pair $(f, g)$ and computes the public key $h$, which is communicated to Bob.

2. Bob produces a code state described by the GKP code using the basis $\sqrt{(\lambda/q)}H(h)$ and samples an error corresponding to a random message $\boldsymbol{e}_0 = (-\boldsymbol{r}, \boldsymbol{m})/\sqrt{\lambda q}$, according to the specifications of the NTRU cryptosystem, by which he displaces the state. He transmits the state to Alice.

3. Alice measures the stabilizers and decodes the state, e.g., via the NTRU decryption routine or by employing Babai's algorithm as outlined before using the secret key pair $(f, g)$. She has hence received the to her unknown state from Bob through the error corrected private quantum channel.

To our knowledge, this setup presents a new paradigm of quantum cryptographic protocols. We summarize points in support of its security.

**Necessity to decode.** In order to unambiguously obtain the logical code state, it is necessary to find a correction $\boldsymbol{e}'$ consistent with the syndrome such that $\|\boldsymbol{e}_0 + \boldsymbol{e}'\| \leq \Delta/2$. Since $\|\boldsymbol{e}_0\|_\infty \leq 1/\sqrt{\lambda q}$ and the smallest element in $\mathcal{L}^\perp$ is of length $\Delta$, this amounts to decrypting the NTRU ciphertext in the syndrome to identify $\boldsymbol{e}_0$. Towards a first cryptanalysis, we examine to which degree an adversary is able to distinguish a quantum ciphertext. Let $|\overline{\psi}\rangle$ be a logical code state vector specified by a GKP-NTRU code with lattice $\mathcal{L}$. We examine the eigenvalue of logical Pauli observables obtained when the initial code state is encrypted by applying the random displacement $D(\boldsymbol{e}_0)$, a syndrome $\boldsymbol{s}(e_0) = MJ\boldsymbol{e}_0 \mod 1$ is obtained and a generic correction via $\boldsymbol{\eta} = (MJ)^{-1}\boldsymbol{s}(\boldsymbol{e}_0)$ is applied. With

$$M^{-1} = \frac{1}{\sqrt{\lambda q}} \begin{pmatrix} qI & -A_\Phi(h) \\ 0 & I \end{pmatrix}, \tag{97}$$

this yields a generic correction

$$\boldsymbol{\eta} = \frac{1}{\sqrt{\lambda q}} \begin{pmatrix} 0 \\ \boldsymbol{c}, \end{pmatrix} \tag{98}$$

where $\boldsymbol{c} = \boldsymbol{m} + A_\Phi(h)\boldsymbol{r} \mod q$ is the associated NTRU ciphertext. The total remaining error after correction thus is

$$\boldsymbol{e}_0 - \boldsymbol{\eta} = \frac{-1}{\sqrt{\lambda q}} \begin{pmatrix} \boldsymbol{r} \\ \boldsymbol{c} - \boldsymbol{m} \end{pmatrix} = \begin{pmatrix} \boldsymbol{r} \\ A_\Phi(h)\boldsymbol{r} \mod q \end{pmatrix}. \tag{99}$$

We compute

$$M^\perp J(\boldsymbol{e}_0 - \boldsymbol{\eta}) = \frac{1}{\lambda} \begin{pmatrix} 0 \\ \boldsymbol{r} \end{pmatrix} \mod q/\lambda, \tag{100}$$

which shows that for an input code state vector $|\overline{\psi}\rangle$, after encoding and generic correction, the eigenvalues of logical Pauli operators corresponding to rows $i = n+1, \ldots, 2n$ in $M^\perp$ obtain a random phase $e^{i\frac{2\pi}{\lambda}r_{i-n}}$. This observation suggests that, for $\lambda = 2$, without access to the random string $\boldsymbol{r}$ embedded in the NTRU ciphertext in every instance, the quantum state is effectively projected onto a state that is diagonal in the logical Pauli-$Z$ basis and quantum superpositions are washed out. This situation is similar to that of half a quantum OTP, where only one type (either $X$ or $Z$) of Pauli operators is used in the encryption.

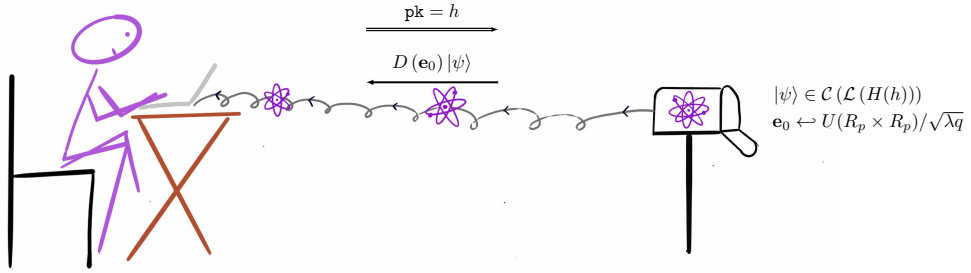
**Orthogonality.** For a fixed quantum state vector $|\overline{\psi}\rangle$, different error realizations $D(\boldsymbol{e}_0)$ where $\|\boldsymbol{e}_0\| < \Delta/2$ map the state to mutually orthogonal states (sectors of the QECC). This is guaranteed by the quantum error correction conditions. Without applying suitable corrections, separate encodings of the same logical quantum state vector $D(\boldsymbol{e}_i)|\overline{\psi}\rangle$ are expected to appear uncorrelated.

Alice

- Sample secret key $\mathtt{sk} = (f, g)$.
- Compute public key $\mathtt{pk} = h = g/f \mod q$.

Bob

- Produce code state stabilized by NTRU-GKP code with public key $\mathtt{pk} = h$.
- Apply random displacement $\mathbf{e}_0 \hookleftarrow U(R_p \times R_p)/\sqrt{\lambda q}$.
- Send state to Alice.




- Measure stabilizers in basis $M = H(h)$.
- Error correct state and decode using secret key $\mathtt{sk} = (f, g)$.

Figure 4: Outline of the private quantum channel established using the NTRU-GKP code as described in the main text.

We leave a further study of the degree of quantum security of this scheme as challenge for future work. It is important to stress that the security of this scheme is not based on information theoretic arguments, but on computational limitations of an eavesdropper, giving rise to a new situation in quantum cryptography. For a practical security analysis it would be furthermore meaningful to study how potential security claims can sustain when also considering the finite squeezing error present in physical GKP states [7, 66].

In addition to the possibility of obtaining a classical public key private quantum channel by this construction, this scheme is also expected to be tolerant against additional errors imposed by the channel. Additional displacement errors would effectively change the "quantum encoded" NTRU ciphertext as encoded in the syndrome, but as long as the additional error together with the initial random displacement implemented by Bob are sufficiently smaller than the euclidean code distance, the transmitted logical quantum state is still expected to be decoded correctly.

As computation and transmission of quantum information encoded in GKP codes using photonics and integrated optics is becoming technologically ever more developed, this setup is interesting for the reason that to transmit quantum information one would potentially use a (bosonic) quantum error correcting codes anyways. Our construction highlights that this can be done with in-built security options without explicitly concatenating the encoded qubits into a separate cryptographic protocol.

## 6 Conclusion and outlook

In this work, we have introduced the randomized construction of *good* GKP codes using the NTRU cryptosystem and discussed how a decoder for these codes can be obtained from variations of the NTRU decryption process.

We have discussed the use of these codes in a public key quantum communication scheme where we expect to inherit a conditional security guarantee from the original cryptosystem. This defines a *trapdoor decodable quantum error correcting code* for which the core idea is that we can provide "bad" bases for suitably chosen GKP codes that allow an agent to prepare code states and measure stabilizers but – without access to a "good" secret basis – require exponential overhead to decode the syndrome. We leave as open challenge to either prove or disprove the quantum security of our scheme. More broadly, this idea also opens the door to potential client-server schemes where a client requests a server – capable of preparing GKP states and carry out Gaussian operations – to carry out computations on client-specified GKP codes and measure stabilizer syndromes without giving the server the power to decode efficiently to apply logical corrections.

It is also worth mentioning that the NTRU cryptosystem has multi-key homomorphic properties with respect to adding and multiplying the message- and random bit-strings [67]. Beyond the scope of this work, we expect it to be possible to leverage these homomorphic properties to design more advanced NTRU-GKP codes for the secure and error corrected transmission of quantum states. Effective NTRU-lattices derived from products of public/secret keys correspond to non-principal ideals of the underlying ring, which makes for an interesting generalization of our setting. Alternatively, it would also be interesting to examine symplecticity for higher rank module lattices. Higher rank module lattices over polynomial rings have previously found application in quantum error correction, e.g., in the work of Pantaleev and

Kalachev [26] to construct high distance quantum LDPC codes, who consider binary polynomial rings with quotient $\Phi_0 = x^l - 1$ and where the element-wise homomorphism of basis elements of the $R$-module basis to circulants is termed *lift*.

On the *hardware level*, we also expect that the cyclic structure of these codes can be helpful in the design of modular stabilizer-measurement architectures with a fixed stabilizer-measurement gadget that is coupled to the data modes with shifted mode-index and at alternating delay. The short length of the corresponding displacements when the stabilizers generators are measured in the secret basis implies a reduced overhead in required interaction time/strength when the required connectivity is present and further highlights a *physical* advantage in having access to the secret basis for several meaningful physical platforms.

For future work, it would be interesting to improve on the decoders, such as adapting our proposition of `BabaiDecode` by adapting Babai's nearest plane algorithm to include information about the biased input error distribution eq. (72), to design a better approximation to MLD decoding NTRU-GKP codes and provide numerical studies for large $n$.

We have highlighted the complexity of decoding GKP codes as an interesting subject to study and we expect that, using concatenation, computational complexity questions on the GKP-lattice level can be put into tighter relationships with corresponding problems in qubit-codes and equivalent questions in classical error correction. It would further be interesting to identify other ideal lattices that can be used to construct GKP codes.

Finally, it is worth mentioning that the relationship between GKP quantum error correction and cryptography runs even deeper. Physical, i.e., normalizable, realizations of GKP states obey a phase-space probability distribution very similar to that of a discrete lattice Gaussian distribution. Quantum states as such, and the ability to produce and sample from them, play a central role in the quantum reduction from SVP to the learning with errors problem [68]. Given the ability to efficiently prepare approximate GKP-state by measuring its stabilizers, we leave as final open question in how far it is possible to sample from discrete lattice Gaussian distributions using physically preparable GKP states.

## Acknowledgements

We thank Victor V. Albert, Yusuf Alnawakhtha, Francesco Arzani, Nikolas P. Breuckmann, Steven T. Flammia, Cica Gustiani, Florian Hirsch, John Preskill, Manasi Shingane, Vincent Ulitzsch, and Daochen Wang for many helpful and inspiring discussions. We thank Henning Seidler for constructive feedback on parts of an early version of the manuscript and Nathan Walk for many helpful comments on a later version. JC thanks the Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland for their kind hospitality during the final preparation stages of this project and many stimulating discussions. During preparation of this manuscript JC was also temporarily affiliated with the AWS CQC and Caltech, which he also thanks for their hospitality.

We gratefully acknowledge support from the BMBF (RealistiQ, MUNIQC-Atoms, PhoQuant, QPIC-1, and QSolid, 6G-RIC, Q-Fiber, Q-net-Q), the DFG (CRC 183, project B04, on entangled states of matter), the Quantum Flagship (Millenion, PasQuans2), the Munich Quantum Valley (K-8), the ERC (DebuQC), the EU (Q-net-Q) as well as the Einstein Research Unit on quantum devices, for which this is an inter-node joint project as well as Berlin Quantum.

## References

[1] D. Gottesman, A. Kitaev, and J. Preskill. "Encoding a qubit in an oscillator". Phys. Rev. A **64**, 012310 (2001).

[2] J. E. Bourassa, R. N. Alexander, M. Vasmer, A. Patil, I. Tzitrin, T. Matsuura, D. Su, B. Q. Baragiola, S. Guha, G. Dauphinais, and et al. "Blueprint for a scalable photonic fault-tolerant quantum computer". Quantum **5**, 392 (2021).

[3] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph, and C. Sparrow. "Fusion-based quantum computation". Nature Comm. **14**, 912 (2021).

[4] A. L. Grimsmo and S. Puri. "Quantum error correction with the Gottesman-Kitaev-Preskill code". PRX Quantum **2**, 020101 (2021).

[5] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. T. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, B. M. Terhal, and L. Jiang. "Performance and structure of single-mode bosonic codes". Phys. Rev. A**97** (2018).

[6] K. Noh, V. V. Albert, and L. Jiang. "Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes". IEEE Trans. Inf. Th. **65**, 2563–2582 (2019).

[7] B. M. Terhal, J. Conrad, and C. Vuillot. "Towards scalable bosonic quantum error correction". Quant. Sc. Tech. **5**, 043001 (2020).

[8] J. Hastrup and U. L. Andersen. "Analysis of loss correction with the Gottesman-Kitaev-Preskill code" (2021). arXiv:2112.01425.

[9] C. Vuillot, H. Asasi, Y. Wang, L. P. Pryadko, and B. M. Terhal. "Quantum error correction

with the toric Gottesman-Kitaev-Preskill code". Phys. Rev. A **99**, 032344 (2019).

[10] K. Noh, S. M. Girvin, and L. Jiang. "Encoding an oscillator into many oscillators". Phys. Rev. Lett. **125**, 080503 (2020).

[11] J. W. Harrington. "Analysis of quantum error-correcting codes: Symplectic lattice codes and toric codes". PhD thesis. California Institute of Technology. (2004).

[12] J. Conrad, J. Eisert, and F. Arzani. "Gottesman-Kitaev-Preskill codes: A lattice perspective". Quantum **6**, 648 (2022).

[13] B. Royer, S. Singh, and S. M. Girvin. "Encoding qubits in multimode grid states". PRX Quantum **3**, 010335 (2022).

[14] F. Schmidt and P. van Loock. "Quantum error correction with higher Gottesman-Kitaev-Preskill codes: Minimal measurements and linear optics". Phys. Rev. A **105**, 042427 (2022).

[15] J. Hoffstein, J. Pipher, and J. H. Silverman. "NTRU: A ring-based public key cryptosystem". In J. P. Buhler, editor, Algorithmic Number Theory. Page 267–288. Lecture Notes in Computer ScienceBerlin (1998). Springer.

[16] J. Bi and Q. Cheng. "Lower bounds of shortest vector lengths in random NTRU lattices". Th. Comp. Sc. **560**, 121–130 (2014).

[17] D. Stehlé and R. Steinfeld. "Making ntru as secure as worst-case problems over ideal lattices". In K. G. Paterson, editor, Advances in Cryptology – EUROCRYPT 2011. Pages 27–47. Berlin, Heidelberg (2011). Springer Berlin Heidelberg.

[18] J. Harrington and J. Preskill. "Achievable rates for the Gaussian quantum channel". Phys. Rev. A **64**, 062301 (2001).

[19] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. "Topological quantum memory". J. Math. Phys. **43**, 4452–4505 (2002).

[20] L. Babai. "On Lovász' lattice reduction and the nearest lattice point problem". Combinatorica **6**, 1–13 (1986).

[21] D. Micciancio. "CSE 206A: Lattice algorithms and applications". url: `http://cseweb.ucsd.edu/classes/wi10/cse206a/`.

[22] J. Preskill. "Lecture notes in quantum error correction". `http://theory.caltech.edu/~preskill/ph229/notes/chap7.pdf` (2009).

[23] A. R. Calderbank and P.W. Shor. "Good quantum error-correcting codes exist". Phys. Rev. A **54**, 1098–1105 (1996).

[24] D. Bacon, S.T. Flammia, A. W. Harrow, and J. Shi. "Sparse quantum codes from quantum circuits". In Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing. Page 327–334. STOC '15New York, NY, USA (2015). Association for Computing Machinery.

[25] P. Panteleev and G. Kalachev. "Asymptotically good quantum and locally testable classical ldpc codes" (2021).

[26] P. Panteleev and G. Kalachev. "Quantum LDPC codes with almost linear minimum distance". IEEE Trans. Inf. Th. **68**, 213–229 (2022).

[27] N. P. Breuckmann and J. N. Eberhardt. "Balanced product quantum codes". IEEE Trans. Inf. Th. **67**, 6653–6674 (2021).

[28] P. Sarnak and P. Buser. "On the period matrix of a Riemann surface of large genus (with an Appendix by J. H. Conway and N. J. A. Sloane)". Invent. Math. **117**, 27–56 (1994).

[29] S. Lang. "Algebra". Graduate Texts in Mathematics. Springer New York. (2005).

[30] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen. "Symplectic lattice reduction and NTRU". In Serge Vaudenay, editor, Advances in Cryptology - Eurocrypt 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Volume 4004 of Lecture Notes in Computer Science, pages 233–253. Springer (2006).

[31] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci. "All-Gaussian universality and fault tolerance with the Gottesman-Kitaev-Preskill code". Phys. Rev. Lett. **123**, 200502 (2019).

[32] J. Conway and N. Sloane. "Sphere packings, lattices and groups". Volume 290. Springer, New York. (1988).

[33] J. Conway and N. Sloane. "On the Voronoi regions of certain lattices". SIAM J. Alg. Dis. Meth.**5** (1984).

[34] Y. Wang. "Quantum error correction with the GKP code and concatenation with stabilizer codes" (2019). arXiv:1908.00147.

[35] K. Fukui, A. Tomita, and A. Okamoto. "Analog quantum error correction with encoding a qubit into an oscillator". Phys. Rev. Lett. **119**, 180507 (2017).

[36] K. Noh and C. Chamberland. "Fault-tolerant bosonic quantum error correction with the surface–Gottesman-Kitaev-Preskill code". Phys. Rev. A **101**, 012316 (2020).

[37] N. Raveendran, N. Rengaswamy, F. Rozpedek, A. Raina, L. Jiang, and Vasic B. "Finite rate QLDPC-GKP coding scheme that surpasses the CSS Hamming bound" (2021). arXiv:2111.07029.

[38] M. Lin, C. Chamberland, and K. Noh. "Closest lattice point decoding for multimode Gottesman-Kitaev-Preskill codes". PRX Quantum**4** (2023).

[39] O. Regev. "Lecture Notes: Lattices in Computer Science". https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/. Online; accessed 05 December 2022.

[40] E. Berlekamp, R. McEliece, and H. van Tilborg. "On the inherent intractability of certain coding problems (corresp.)". IEEE Trans. Inf. Th. **24**, 384–386 (1978).

[41] A. Vardy. "The intractability of computing the minimum distance of a code". IEEE Trans. Inf. Th. **43**, 1757–1766 (1997).

[42] M.-H. Hsieh and F. Le Gall. "NP-hardness of decoding quantum error-correction codes". Phys. Rev. A **83**, 052331 (2011).

[43] P. Iyer and D. Poulin. "Hardness of decoding quantum stabilizer codes". IEEE Trans. Inf. Theor. **61**, 5209–5223 (2015).

[44] M. Ajtai. "Generating hard instances of lattice problems (extended abstract)". In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. Page 99–108. STOC '96New York, NY, USA (1996). Association for Computing Machinery.

[45] J. Silverman. "Lecture notes: An introduction to lattices, lattice reduction, and lattice-based cryptography". https://www.ias.edu/sites/default/files/Silverman_PCMI_Note_DistributionVersion_220705.pdf. Online; accessed 05 December 2022.

[46] Y. Aono, Espitau T., , and Q. Ngyuen P. "Random lattices: Theory and practice". https://espitau.github.io/bin/random_lattice.pdf.

[47] A. M. Macbeath and C. A. Rogers. "A modified form of Siegel's mean value theorem. II". Math. Proc. Cambr. Phil. Soc. **54**, 322–326 (1958).

[48] D. Coppersmith and A. Shamir. "Lattice attacks on NTRU". In Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding. Volume 1233 of Lecture Notes in Computer Science, pages 52–61. Springer (1997).

[49] A. May. "Auf Polynomgleichungen basierende Public-Key-Kryptosysteme" (1999).

[50] A. May. "Cryptanalysis of NTRU" (1999). preprint.

[51] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. "Mixed-state entanglement and quantum error correction". Phys. Rev. A **54**, 3824–3851 (1996).

[52] D. J. Bernstein, J. Buchmann, and Dahmen E. "Post-quantum cryptography". Springer Berlin Heidelberg. Berlin, Heidelberg (2009).

[53] S. Halevi and T. Malkin. "Lecture Notes: Lattices and homomorphic encryption, Spring 2013". https://www.cs.columbia.edu/~tal/6261/SP13/. Online; accessed 04 December 2022.

[54] V. Lyubashevsky and D. Micciancio. "Generalized compact knapsacks are collision resistant". In Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II. Page 144–155. ICALP'06Berlin, Heidelberg (2006). Springer-Verlag.

[55] J. Bi and Q. Cheng. "Lower bounds of shortest vector lengths in random knapsack lattices and random NTRU lattices". Cryptology ePrint Archive, Paper 2011/153 (2011). https://eprint.iacr.org/2011/153.

[56] The Sage Developers, W. Stein, D. Joyner, D. Kohel, J. Cremona, and B. Eröcal. "Sagemath, version 9.6". http://www.sagemath.org (2022).

[57] https://github.com/JonCYeh/NTRUGKP.git.

[58] D. J. Bernstein, N. Heninger, and T. Lange. "LatticeHacks". https://latticehacks.cr.yp.to/ntru.html.

[59] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. "NTRUSign: Digital signatures using the NTRU lattice". In M. Joye, editor, Topics in Cryptology — CT-RSA 2003. Pages 122–140. Berlin, Heidelberg (2003). Springer Berlin Heidelberg.

[60] L. Ducas, V. Lyubashevsky, and T. Prest. "Efficient identity-based encryption over NTRU lattices". In P. Sarkar and T. Iwata, editors, Advances in Cryptology – ASIACRYPT 2014. Pages 22–41. Berlin, Heidelberg (2014). Springer Berlin Heidelberg.

[61] A. Lenstra, H. Lenstra, and L. Lovász. "Factoring polynomials with rational coefficients". Math. Ann. **261**, 515–534 (1982).

[62] Lior Eldar and Sean Hallgren. "An efficient quantum algorithm for lattice problems achieving subexponential approximation factor" (2022). arXiv:2201.13450.

[63] L. Ducas and W. van Woerden. "A note on a claim of eldar & hallgren: Lll already solves it". Cryptology ePrint Archive, Paper 2021/1391 (2021). https://eprint.iacr.org/2021/1391.

[64] R. Allen, R. E. Berker, S. Casacuberta, and M. Gul. "Quantum and classical algorithms for bounded distance decoding". Cryptology

ePrint Archive, Paper 2022/195 (2022). https://eprint.iacr.org/2022/195.

[65] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. "Private quantum channels". IEEE Symp. Found. Comp. Sc.Page 547–553 (2000).

[66] I. Tzitrin, J. E. Bourassa, N. C. Menicucci, and K. K. Sabapathy. "Progress towards practical qubit computation using approximate gottesman-kitaev-preskill codes". Phys. Rev. A **101**, 032315 (2020).

[67] A. López-Alt, E. Tromer, and V. Vaikuntanathan. "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption". In Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing. Page 1219–1234. STOC '12New York, NY, USA (2012). Association for Computing Machinery.

[68] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. Page 84–93. STOC '05New York, NY, USA (2005). Association for Computing Machinery.

[69] D. E. Gottesman. "Stabilizer codes and quantum error correction". PhD thesis. California Institute of Technology. (1997).

[70] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn. "Quantum error detection ii: Bounds" (1999). arXiv:quant-ph/9906131.

[71] A. Ashikhmin and E. Knill. "Nonbinary quantum stabilizer codes" (2000). arXiv:quant-ph/0005008.

## A $\lambda_1 = \Omega\left(\sqrt{n}\right)$ scaling for NTRU-like lattices with random symmetric $H$.

In this section we discuss a strategy towards proving conjecture 1 and 2. Following the proof strategy laid out in ref. [28], we show that a certain distribution over symplectic lattices with NTRU lattice-like generating matrix implement the "design property" of eq. (31), which, following the derivation in the main text, suffices to establish the scaling provided by the Gaussian heuristic and thus establish goodness of the associated GKP codes. By viewing the considered GKP codes as concatenated codes with a $\mathcal{L}_\square \propto q\mathbb{Z}^{2n}$ sublattice, the following statement also establishes the existence of "good" qudit-based quantum error correcting codes when the local dimension $q \to \infty$ is large and yields an alternative proof of the existence of good qudit-based stabilizer codes as similarly obtained from the quantum Gilbert-Varshamov bound [69, 70, 71]. The proof presented here also yields a simple constructive way to sample GKP- or qudit-based stabilizer codes that are expected to be good. A canonical basis for an NTRU lattice is given by the rows of the $\mathbb{Z}^{2n\times 2n}$ matrix

$$M\left[X\right] = \begin{pmatrix} I & X \\ 0 & qI_n \end{pmatrix}, \tag{101}$$

where $X = H(h) \in \mathbb{F}_q^{n\times n}$ has a special cyclic structure. The top block can be interpreted as the reduced row-echelon form $(I\ H\left(h\right))$ of a classical linear $q-$ary code in $\mathbb{F}_q^{2n}$. For $X = X^T$ symmetric, we have that $M\left[X\right]$ is $q-$ symplectic. We will denote $M_{\text{sp}}\left[X\right] = M\left[X\right]/\sqrt{q}$ its rescaling to a symplectic matrix. Following the technique used in ref. [28], we first show the subsequent statement.

**Proposition 3.** *Let*

$$U_q := \left\{ X = X^T \in \left\{ -\frac{q}{2}, \ldots, \frac{q}{2} \right\}^{n\times n} \right\} \tag{102}$$

*be the set of symmetric matrices in $\mathbb{Z}_q$ and let $f : \mathbb{R}^{2n} \to \mathbb{R}$ be a function with compact support. We have*

$$\lim_{q\to\infty} \left\langle \sum_{\boldsymbol{k}\in\mathbb{Z}^{2n}-\{0\}} f\left(M_{\text{sp}}^T\left[X\right]\boldsymbol{k}\right) \right\rangle_{X\in U_q} = \int_{\mathbb{R}^{2n}} f\left(\boldsymbol{x}\right) d\boldsymbol{x}, \tag{103}$$

*where the expectation value on the LHS is taken uniformly over $U_q$.*

*Proof.* We start from the definition

$$\begin{aligned} \lim_{q\to\infty} \left\langle F(X) \right\rangle_{X\in U_q} &= \lim_{q\to\infty} q^{-1} \sum_{X_{1,1}=-q/2}^{q/2} q^{-1} \sum_{X_{1,2}=-q/2}^{q/2} \ldots F(X) \\ &= \int_{-1/2}^{1/2} dX_{1,1} dX_{1,2} dX_{1,3} \ldots F(qX). \end{aligned} \tag{104}$$

We have for $\boldsymbol{k} = \boldsymbol{m} \oplus \boldsymbol{n}$

$$M_{\text{sp}}^T\left[X\right]\boldsymbol{k} = q^{-\frac{1}{2}} \begin{pmatrix} \boldsymbol{m} \\ qX\boldsymbol{m} + q\boldsymbol{n} \end{pmatrix},$$

such that we can compute analogously to the argument presented in ref. [28]

$$I(q) = \int_{-1/2}^{1/2} dX_{1,1} dX_{1,2} dX_{1,3} \ldots \sum_{\boldsymbol{m},\boldsymbol{n}\in\mathbb{Z}^n-\{0\}} f\left( q^{-\frac{1}{2}} \begin{pmatrix} \boldsymbol{m} \\ qX\boldsymbol{m} + q\boldsymbol{n} \end{pmatrix} \right) \tag{105}$$

$$= \int_{-1/2}^{1/2} dX_{1,1} dX_{1,2} dX_{1,3} \ldots \left\{ \sum_{\substack{\boldsymbol{m}\in Z^n, \\ m_1\neq 0}} + \sum_{\substack{\boldsymbol{m}\in Z^n, \\ m_1=0 \\ m_2\neq 0}} + \sum_{\substack{\boldsymbol{m}\in Z^n, \\ m_1=0 \\ m_2=0 \\ m_3\neq 0}} + \ldots \right\} \sum_{\boldsymbol{n}\in\mathbb{Z}^n} f\left( q^{-\frac{1}{2}} \begin{pmatrix} \boldsymbol{m} \\ qX\boldsymbol{m} + q\boldsymbol{n} \end{pmatrix} \right) \tag{106}$$

$$+ \sum_{\boldsymbol{n}\in\mathbb{Z}^n} f\left( \begin{pmatrix} \boldsymbol{0} \\ \sqrt{q}\boldsymbol{n} \end{pmatrix} \right). \tag{107}$$

In eq. (106), we consider each summation over $\boldsymbol{m}$ separately. In the first term with the constraint $m_1 \neq 0$ we rewrite

$$qX\boldsymbol{m} + q\boldsymbol{n} = \begin{pmatrix} qm_1 \left( X_{1,1} + \frac{n_1}{m_1} + m_1^{-1} \sum_{k>1} X_{1,k} m_k \right) \\ qm_1 \left( X_{2,1} + \frac{n_2}{m_1} + m_1^{-1} \sum_{k>1} X_{2,k} m_k \right) \\ qm_1 \left( X_{3,1} + \frac{n_3}{m_1} + m_1^{-1} \sum_{k>1} X_{3,k} m_k \right) \\ \vdots \end{pmatrix}. \tag{108}$$

We write for each $n_i = \lfloor \frac{n_i}{m_1} \rfloor m_1 + (n_i \mod m_1)$ and split the summation

$$\sum_{n_i \in \mathbb{Z}} g\left(\frac{n_i}{m_1}\right) = \sum_{j_i \in \mathbb{Z}} \sum_{n_i \in \mathbb{Z}_{m_1}} g\left(j_i + \frac{n_i}{m_1}\right). \tag{109}$$

This way, each summation over the integer divisors of $n_i$ with $m_1$ can be combined with the integral over $X_{i,1} \in [-1/2, 1/2]$ to an integral of $X_{i,1} \in \mathbb{R}$ over the real numbers. To perform this trick, start with $X_{1,1} + j_1$ in the first row of eq. (108) and realize that all subsequent rows are independent of $X_{1,1}$. After converting the integration in the first row, all remaining summand of that row can be absorbed into a shift of the $X_{1,1}$ integral. Now the first row is also independent of $X_{2,1} = X_{1,2}$, such that we can repeat this trick, converting the integral over $X_{2,1}$ and summation over $j_2$ into integration of $X_{2,1}$ over $\mathbb{R}$ which again gets rid of the dependency on $X_{k,2}, k > 1$ in this row. Similarly, the summations over the terms $\frac{n_i}{m_1}$ also becomes trivial and provides a factor of $m_1$. In total, after substitution $t_i = qm_1 X_{i,1}$

$$\begin{aligned} &\int_{-1/2}^{1/2} dX_{1,1} dX_{1,2} dX_{1,3} \ldots \sum_{\substack{\boldsymbol{m} \in Z^n, \\ m_1 \neq 0}} \sum_{\boldsymbol{n} \in \mathbb{Z}^n} f\left( q^{-\frac{1}{2}} \begin{pmatrix} \boldsymbol{m} \\ qX\boldsymbol{m} + q\boldsymbol{n} \end{pmatrix} \right) \\ &= \sum_{\substack{\boldsymbol{m} \in Z^n, \\ m_1 \neq 0}} \int_{-\infty}^{\infty} d\boldsymbol{t}\, q^{-n} f\left( q^{-\frac{1}{2}} \begin{pmatrix} \boldsymbol{m} \\ \boldsymbol{t} \end{pmatrix} \right) \\ &= q^{-n/2} \sum_{\substack{\boldsymbol{m} \in Z^n, \\ m_1 \neq 0}} \int_{-\infty}^{\infty} d\boldsymbol{t}\, f\left( \begin{pmatrix} q^{-\frac{1}{2}} \boldsymbol{m} \\ \boldsymbol{t} \end{pmatrix} \right). \end{aligned} \tag{110}$$

In the second term with constraint $m_1 = 0$, $m_2 \neq 0$ we repeat the above procedure by pulling out a factor of $qm_2$, $qX\boldsymbol{m} + q\boldsymbol{n} = qm_2(qX\boldsymbol{m}/m_2 + \boldsymbol{n}/m_2)$. Begin with the integration over $X_{2,2}$, together with the sum over $n_2$ this again extends the domain of integration of $X_{2,2}$ to $\mathbb{R}$. Substituting the remaining summands in the corresponding row renders the rest of $qX\boldsymbol{m} + q\boldsymbol{n}$ independent of independent of $X_{2,i}, i > 2$ such that in each other row we can combine the $X_{2,i}$ integration with the sum over $n_i$ to extend the domains of integration. Repeat this procedure using each $m_i \neq 0$ in eq. (106) and finally use that $f$ has compact support, such that in the limit $q \to \infty$ eq. (105) becomes

$$\lim_{q\to\infty} I(q) = \lim_{q\to\infty} q^{-n/2} \sum_{\boldsymbol{m} \in Z^n - \{0\}} \int_{-\infty}^{\infty} d\boldsymbol{t}\, f\left( \begin{pmatrix} q^{-\frac{1}{2}} \boldsymbol{m} \\ \boldsymbol{t} \end{pmatrix} \right). \tag{111}$$

In the limit, we again use the definition of the Riemann integral to finally obtain

$$\lim_{q\to\infty} I(q) = \int_{\mathbb{R}^{2n}} f(\boldsymbol{x})\, d\boldsymbol{x}. \tag{112}$$

□

We make the observation that for this proof strategy to work, it was important that each row/column of $X$ contained one entry that was independent of all the other rows. This is manifestly not the case for the (quasi) cyclic matrices $H(h)$ provided by the NTRU cryptosystem. To show goodness for NTRU-GKP codes for random public key $h$ and thus establish conjecture 1, it would further be necessary to understand how the distribution over cyclic matrices $H(h)$ approximates that of the random symmetric matrices considered above. We leave this as interesting open problem to examine in future work.

## B Thresholds of GKP codes

In this section, we sketch how the existence and value of a threshold for a GKP code family can be analyzed using the lattice theta function. For simplicity, assume a zero syndrome $\boldsymbol{s} = 0$ on a lattice $\mathcal{L}_n$ that is part of a family of lattices scaling with $n$. The probability for the state to be in the $\boldsymbol{\xi}_n^\perp = 0$ coset is given by $P([\boldsymbol{\xi}_n^\perp]|0) = \Theta_{\mathcal{L}_n}(z)/\Theta_{\mathcal{L}_n^\perp}(z)$, where

$$\Theta_{\mathcal{L}_n^\perp}(z) = \sum_{\boldsymbol{\xi}_n^\perp \in \mathcal{L}_n^\perp/\mathcal{L}_n} \Theta_{\mathcal{L}_n + \boldsymbol{\xi}_n^\perp}(z) \tag{113}$$

denotes the probability to be in any logical coset and $z = i/(2\pi\sigma^2)$. A necessary condition for a GKP code family to exhibit a threshold is satisfied if there exists $z^* \in i\mathbb{R}$ such that for any $|z| > |z^*|$, $z \in i\mathbb{R}$, it holds that

$$0 = \lim_{n\to\infty} \Theta_{\mathcal{L}_n^\perp}(z) - \Theta_{\mathcal{L}_n}(z) = \lim_{n\to\infty} \sum_{\boldsymbol{\xi}_n^\perp \in \mathcal{L}_n^\perp \setminus \mathcal{L}_n} \Theta_{\mathcal{L}_n + \boldsymbol{\xi}_n^\perp}(z). \tag{114}$$

We write

$$\begin{aligned} \Theta_{\mathcal{L}_n + \boldsymbol{\xi}_n^\perp}(z) &= \sum_{\delta \in \mathcal{D}_n} N_\delta(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp) q^\delta \\ &= \sum_{\delta \in \mathcal{D}_n} \exp\left\{\delta\left(\delta^{-1}\ln(N_\delta(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)) - |\ln(q)|\right)\right\}, \end{aligned} \tag{115}$$

where we have $\mathcal{D}_n := \{\|\boldsymbol{x}\|^2,\ \boldsymbol{x} \in \mathcal{L}_n + \boldsymbol{\xi}_n^\perp)\}$ and $N_\delta(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp) = \#\{\boldsymbol{x} \in \mathcal{L}_n + \boldsymbol{\xi}_n^\perp : \|\boldsymbol{x}\|^2 = \delta\}$. We have that $\lambda_1\left(\mathcal{L}_n + \boldsymbol{\xi}_n^\perp\right)$ corresponds to a shortest representative of the logical coset given by $\xi_n^\perp$, such that the threshold condition becomes

$$\begin{aligned} 0 &= \lim_{n\to\infty} \sum_{\xi_n^\perp \in \mathcal{L}_n^\perp \setminus \mathcal{L}_n} \sum_{\delta \in \mathcal{D}_n} \exp\left\{\delta\left(\delta^{-1}\ln(N_\delta(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)) - |\ln(q)|\right)\right\} \\ &= \lim_{n\to\infty} \exp\left\{\Delta^2\left(\Delta^{-2}\ln(N_{\Delta^2}(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)) - |\ln(q)|\right)\right\} + \ldots, \end{aligned} \tag{116}$$

where $\Delta$ is the Euclidean code distance of the code $\mathcal{L}_n$ as defined in previous sections that we assume to grow with increasing $n$. Since each term in the sum is positive, a necessary condition for asymptotic error suppression becomes

$$\begin{aligned} &|\ln(q)| > \Delta^{-2}\ln(N_{\Delta^2}(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)) \\ &\Leftrightarrow 2\sigma^2 < \Delta^2 \ln^{-1}(N_{\Delta^2}(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)). \end{aligned} \tag{117}$$

Hence, under negligence of all higher order terms we can upper bound the threshold as

$$2\sigma^{*\,2} < \min_{\boldsymbol{\xi}_n^\perp \in \mathcal{L}_n^\perp/\mathcal{L}_n} \frac{\Delta^2}{\ln\left(N_{\Delta^2}(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)\right)}, \tag{118}$$

which shows the impact of the entropic contribution $N_{\Delta^2}(\mathcal{L}_n, \boldsymbol{\xi}_n^\perp)$ on the potential threshold.

## C Numerical results on decoding NTRU-HPS

In this section we report some small scale numerical experiments we have conducted on decoding the NTRU-GKP code (with $\Phi_0 = x^n - 1$) in the small $n$ regime, where numerical experiments where feasible within the scope of this work. The following codes are obtained as the NTRU lattice with the largest shortest vector length amongst 100 samples of NTRU key pairs $(f, g)$, where each instance of the SVP problem is solved by full HKZ reduction. We aim at correcting errors up to a standard deviation $\overline{\sigma}^* = \sigma^*/\sqrt{2\pi}$ with physical standard deviation of $\sigma^* = 0.1$. By solving for $n, q$ in $\Delta/2 \geq \sqrt{2n\overline{\sigma}^2}$ using the bound in proposition 1, we trial $q = 8$ as a reasonable parameter.

The parameters of the codes we obtained are summarized in fig. 5. For comparison, notice that a standard square GKP code concatenated with a small $[\![n, 1, 3]\!]$ qubit code has distance $\Delta = \sqrt{3/2} = 1.22$ using typically $n = 5$ to 9 qubits to encode a single logical qubit while here a similar distance is achieved while encoding $k = n$ logical qubits.

| $n, d, q, p$ | $\lambda_1\,(L_{\text{cs}})$ | $\Delta$ |
|---|---|---|
| $7, 2, 8, 3$ | 4 | 1 |
| $11, 3, 8, 3$ | 4.69 | 1.17 |
| $17, 5, 8, 3$ | 4.9 | 1.23 |
| $23, 7, 8, 3$ | 5.48 | 1.37 |

Figure 5: Parameters of sampled NTRU lattices.

Using these codes we simulate the error correction process on $N_{\text{samples}} = 10^5$ Gaussian distributed errors with physical variance $\sigma^2 = 2\pi\bar{\sigma}^2$. The data displayed in fig. 6 shows $\sigma^2 = 2\pi\bar{\sigma}^2$ on the x-axis denoting the *physical* variance of Gaussian displacements and $p_{\text{err}}$ as the logical error rate conditioned on successful decoding in the sense that the decoder successfully undid the syndrome. We also plot $p_{\text{check}}$, denoting the rate of decoding failures, i.e., the rate by which the decoder fails to output an error with the correct syndrome that is input to the decoder. The standard deviation on the estimates for $p$ given by $\epsilon_p = \sqrt{p_{\text{err}}(1-p_{\text{err}})/N_{\text{sample}}}$ is included in the plots but due to the sample number of $N_{\text{sample}} = 10^5$ is of negligible size. For comparison, we also plot in black

$$p(n, q, \sigma) = 1 - \left[\int_{-\frac{\tilde{\Delta}}{2}}^{\frac{\tilde{\Delta}}{2}} \frac{e^{-\frac{x^2}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}} dx\right]^{2n} \tag{119}$$

$$= 1 - \left[\text{erf}\left(\frac{\tilde{\Delta}}{2\sqrt{2}\sigma}\right)\right]^{2n},$$

$$\tilde{\Delta} = \sqrt{\frac{2\pi}{2q}}, \tag{120}$$

which denotes the logical error probability of $n$ qudits with $d = 2q$ encoded into the trivial sub-lattice $\mathcal{L}_{\text{triv}} = \sqrt{2q}\mathbb{Z}^{2n}$ corresponding to a hypercubic GKP code as well as in grey $p(n, 1, \sigma)$, corresponding to the logical error probability of $n$ square GKP codes each encoding a single logical qubit. We further provide results for simulations of NTRU-GKP codes separately sampled from distributions $b$) and $c$) as denoted in fig. 3. The parameters listed below in fig. 7 reflect the codes simulated in figs. 8, 9, 10. In total, we make the following observations.

- `BabaiDecode` has a rate of decoding failures matching $p(n, q, \sigma)$, suggesting that decoding fails whenever the original error lies outside of the Voronoi Cell of $\mathcal{L}_{\text{triv}}^{\perp} = \mathbb{Z}/\sqrt{2q}$. When decoding is successful, the logical error rate is negligible.

- `NTRUDecode` consistently corrects successfully, i.e., returns the state to code space, and has a conditional logical error rate that is smaller than $p(n, q, \sigma)$. The logical error rate is however consistently larger than that of $n$ square GKP codes, which is negligible in this parameter range. For $\sigma \approx 1.13$ we observe a "threshold"-like behaviour in the transition between the sampled $n = 17$ and $n = 23$ code.

- There appears to be no significant difference which $p$ we choose.

The performance of these codes appears to be relatively poor when compared to more conventional multi-mode codes, such as the *toric-GKP code* [9], which we expect to be mainly the case due to the extremely small $n, q$ parameter regime we have simulated.

Further contributing factors to this observation may be that by decoding via essentially `MED` decoders, we ignore a significant entropic contribution to the optimal `MLD` problem. We have a number of minimal logical shifts $N_{\Delta^2} \geq n$ since the lattice $\mathcal{L}$ is invariant under the cyclic shift $T : T^n = I$, which is expected to be a relevant factor in the full `MLD` decoding problem. Another factor is that the NTRU decryption process used in `NTRUDecode` is in fact not tailored to a Gaussian distribution of random bits, but rather is originally set up to decrypt a message hidden away using random strings $\boldsymbol{r}$ sampled from an uniform distribution. `BabaiDecode` improves upon this fact in spirit by employing the *nearest plane algorithm* in the decryption process, but ignores the biasing of the error distribution, eq. (72), from the first step of the decoding routine which is a necessary step in order to interpret the decryption process as a `CVP`.

It is interesting to observe that `BabaiDecode` consistently displays a negligible logical error rate but quickly rises to high decoding failure rate, which worsens as the code is scaled up and that for `NTRUDecode` we do observe a parameter range where the decoder displays a lower logical error rate than $p(n, q, \sigma)$. This shows that

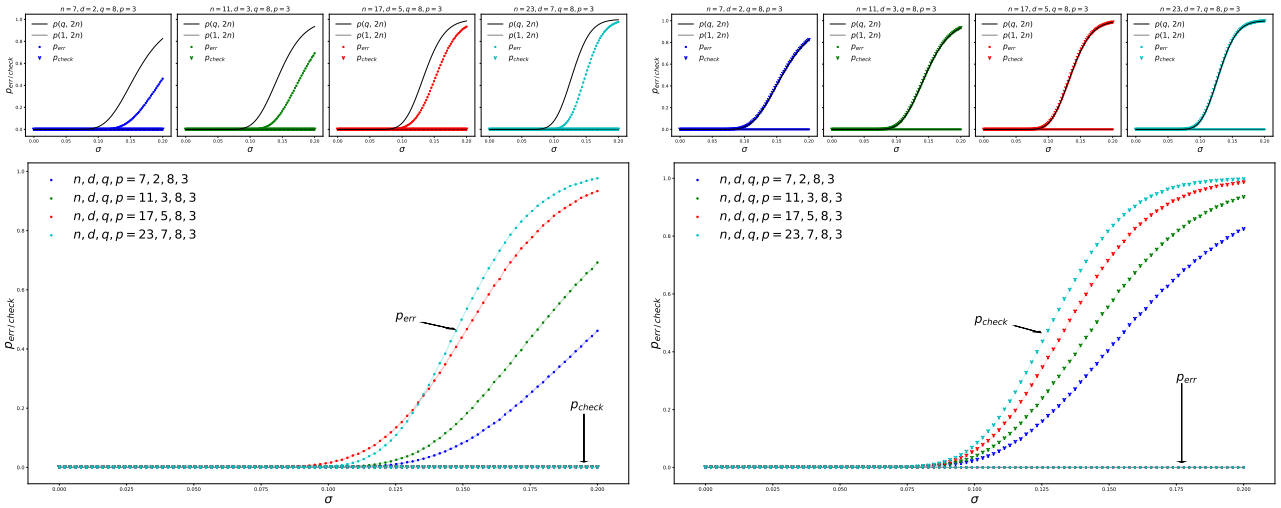



Figure 6: Numerical results for the NTRU-GKP codes using the NTRU decryption routine `NTRUDecode` (left) and `BabaiDecode` (right) for NTRU-GKP lattices where $h$ is invertible. Here, the parameters $q = 8$ and $p = 3$ are fixed. $p_{\mathrm{err}}$ (dots) denotes the the logical error rate conditioned on successful decoding and $p_{\mathrm{check}}$ (stars) denotes the rate of decoding failures.

| $n, d, q, p$ | $\lambda_1\,(L_{\mathrm{cs}})$ | $\Delta$ |
|---|---|---|
| $7, 2, 4, 3$ | 2.65 | 0.94 |
| $11, 3, 8, 5$ | 3.32 | 0.83 |
| $17, 5, 16, 7$ | 4.12 | 0.74 |
| $7, 2, 4, 3$ | 2.65 | 0.94 |
| $11, 3, 8, 3$ | 3.32 | 0.83 |
| $17, 5, 16, 3$ | 4.12 | 0.74 |

| $n, d, q, p$ | $\lambda_1\,(L_{\mathrm{cs}})$ | $\Delta$ |
|---|---|---|
| $7, 2, 4, 3$ | 2.83 | 1 |
| $11, 3, 8, 5$ | 4.24 | 1.06 |
| $17, 5, 16, 7$ | 7.07 | 1.24 |
| $7, 2, 4, 3$ | 2.83 | 1 |
| $11, 3, 8, 3$ | 4.24 | 1.06 |
| $17, 5, 16, 3$ | 6.93 | 1.23 |

Figure 7: Lattice parameters for random NTRU lattices. The table on the right summarizes the results when additionally $h$ is required to be invertible.

the decoder indeed non-trivially decodes errors. Overall, it appears necessary to perform larger scale numerical studies at large $n, q$ to examine the possibility of a threshold. The `sagemath` [56] and `python` code as well as all numerical data presented here is publicly available under ref. [57]. `sagemath` functionalities to construct NTRU lattices are partially adapted from ref. [58].

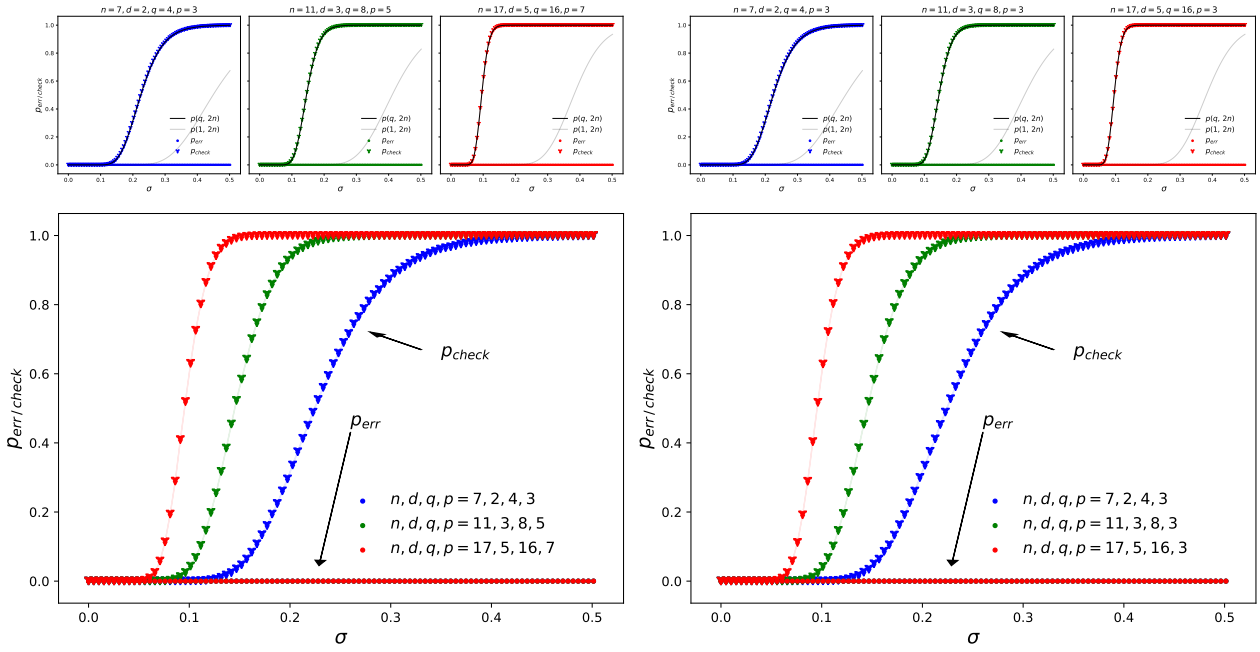



Figure 8: Numerical results for the NTRU-GKP codes using the NTRU decryption routine `BabaiDecode`. (left) $p = 3, 5, 7$ is running and (right) $p = 3$ is fixed.

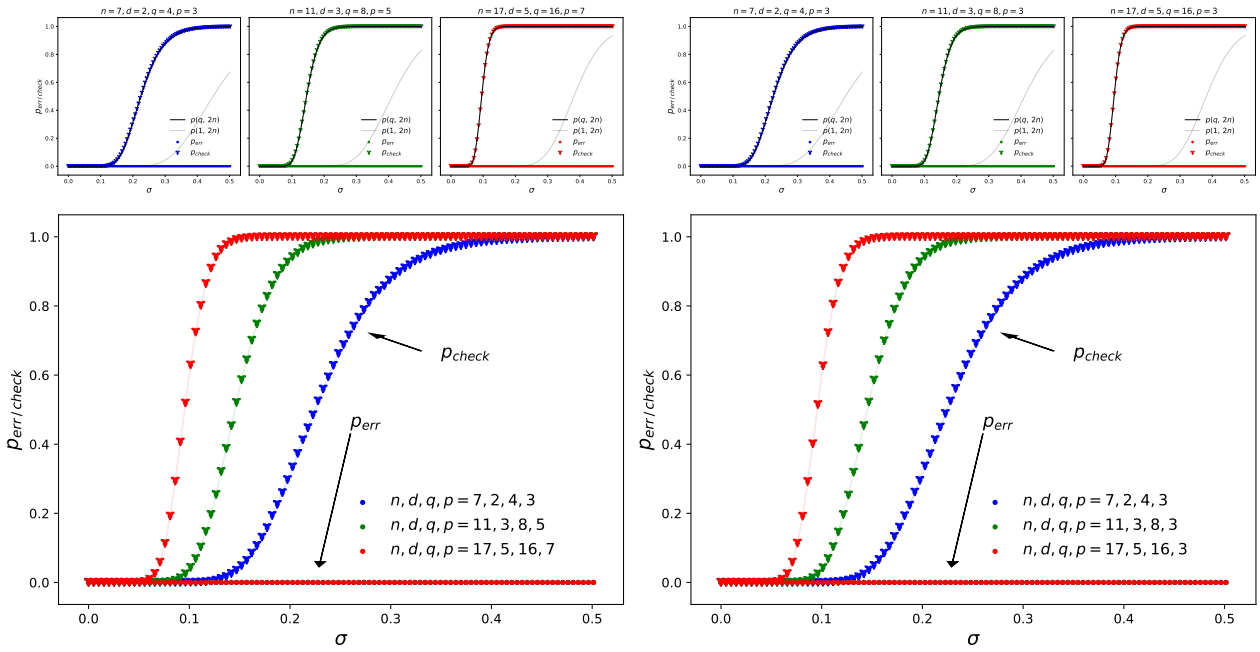



Figure 9: Numerical results for the NTRU-GKP codes using the NTRU decryption routine `BabaiDecode` for NTRU-GKP codes where $h$ is invertible. (left) $p = 3, 5, 7$ is running and (right) $p = 3$ is fixed.

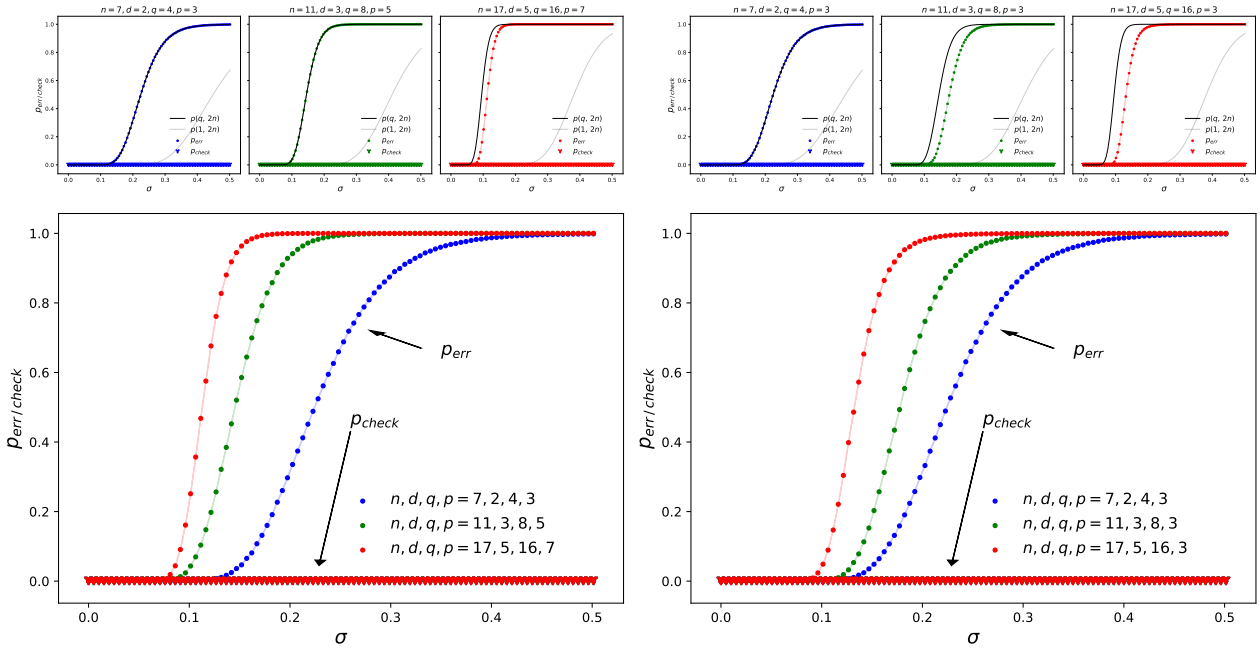



Figure 10: Numerical results for the NTRU-GKP codes using the NTRU decryption routine `NTRUDecode` for NTRU-GKP lattices where $h$ is invertible. (left) $p = 3, 5, 7$ is running and (right) $p = 3$ is fixed.