Reduction from Sparse LPN to LPN, Dual Attack 3.0

Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, Jean-Pierre Tillich

REDUCTION FROM SPARSE LPN TO LPN, DUAL ATTACK 3.0

KÉVIN CARRIER[1], THOMAS DEBRIS–ALAZARD[2,3], CHARLES MEYER-HILFIGER[4], AND JEAN-PIERRE TILLICH[4]

Abstract. The security of code-based cryptography relies primarily on the hardness of decoding generic linear codes. Until very recently, all the best algorithms for solving the decoding problem were information set decoders (ISD). However, recently a new algorithm called RLPN-decoding which relies on a completely different approach was introduced and it has been shown that RLPN outperforms significantly ISD decoders for a rather large range of rates. This RLPN decoder relies on two ingredients, first reducing decoding to some underlying LPN problem, and then computing efficiently many parity-checks of small weight when restricted to some positions. We revisit RLPN-decoding by noticing that, in this algorithm, decoding is in fact reduced to a sparse-LPN problem, namely with a secret whose Hamming weight is small. Our new approach consists this time in making an additional reduction from sparse-LPN to plain-LPN with a coding approach inspired by coded-BKW. It outperforms significantly the ISD's and RLPN for code rates smaller than 0.42. This algorithm can be viewed as the code-based cryptography cousin of recent dual attacks in lattice-based cryptography. We depart completely from the traditional analysis of this kind of algorithm which uses a certain number of independence assumptions that have been strongly questioned recently in the latter domain. We give instead a formula for the LPN noise relying on duality which allows to analyze the behavior of the algorithm by relying only on the analysis of a certain weight distribution. By using only a minimal assumption whose validity has been verified experimentally we are able to justify the correctness of our algorithm. This key tool, namely the duality formula, can be readily adapted to the lattice setting and is shown to give a simple explanation for some phenomena observed on dual attacks in lattices in [DP23b].

1. Introduction

1.1. Background.

Code-based Cryptography: Decoding and LPN Problems. Code-based cryptography relies on the hardness of decoding generic linear codes or sometimes also on a closely related problem, namely the LPN problem. The first one corresponds in the binary case to

Problem 1 (decoding a fixed error weight in a linear code)**.** *Let $\mathcal{C}$ be a binary linear code over $\mathbb{F}_2$ of dimension k and length n,* i.e. *a subspace of $\mathbb{F}_2^n$ of dimension k. We are given $\mathbf{y} \in \mathbb{F}_2^n$, an integer t and we want to find a codeword $\mathbf{c} \in \mathcal{C}$ and an error vector $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight $|\mathbf{e}| = t$ for which $\mathbf{y} = \mathbf{c} + \mathbf{e}$.*

Generally the linear code is specified by a *generator matrix*, namely a $k \times n$ binary matrix $\mathbf{G}$ whose rows span the vector space $\mathcal{C}$, in other words

$$\mathcal{C} = \{\mathbf{uG} : \mathbf{u} \in \mathbb{F}_2^k\}.$$

[1] Laboratoire ETIS, UMR 8051, CY Cergy-Paris Université, ENSEA, CNRS
[2] Project GRACE, Inria Saclay
[3] Laboratoire LIX, École Polytechnique, Institut Polytechnique de Paris, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau Cedex
[4] Project COSMIQ, Inria de Paris
E-mail addresses: kevin.carrier@ensea.fr, thomas.debris@inria.fr, charles.meyer-hilfiger@inria.fr, jean-pierre.tillich@inria.fr.

The work of KC, TDA and JPT was funded by the French Agence Nationale de la Recherche through ANR JCJC DECODE (ANR-22-CE39-0004-01) for KC, ANR JCJC COLA (ANR-21-CE39-0011) for TDA and ANR-22-PETQ-0008 PQ-TLS for JPT. The work of CMH was funded by the French Agence de l'innovation de défense and by Inria.

The second one is a version of this problem where the length n is basically unbounded; the code is randomly chosen and the error model is slightly modified to take into account that the length is not fixed.

Problem 2 (LPN problem)**.** *Let* $\mathbf{s}$ *be a secret chosen uniformly at random in* $\mathbb{F}_2^k$*. We have unbounded access to an oracle such that each query provides a pair* $(\mathbf{a}, b)$ *where* $\mathbf{a}$ *is chosen uniformly at random in* $\mathbb{F}_2^k$ *and* b *is a bit obtained as*

$$b = \langle \mathbf{s}, \mathbf{a} \rangle + e$$

where $e \in \mathbb{F}_2$ *is chosen at random and is equal to* 1 *with probability* p*. Quantity* $\langle \mathbf{s}, \mathbf{a} \rangle$ *stands for the inner product* $\sum_{i=1}^{k} s_i a_i$ *between* $\mathbf{s} = (s_i)_{1 \leqslant i \leqslant k}$ *and* $\mathbf{a} = (a_i)_{1 \leqslant i \leqslant k}$*. The aim is to output* $\mathbf{s}$ *after querying a certain number of times the oracle.*

Sometimes a variation of the LPN problem is considered, namely the *sparse* LPN problem where the only difference is the way $\mathbf{s}$ is chosen, say uniformly at random among the words of length n and Hamming weight t' small, or the entries like i.i.d. Bernoulli random variables of parameter p' small.

The Complexity of the Best Generic Decoding Algorithms and LPN-solvers. It is of fundamental importance to study the complexity of these problems, the best state of the art algorithms being those that are used to determine secure parameters of code-based cryptosystems. The regime of parameters which is relevant for code-based cryptography depends on the type of primitive, but a large range of parameters is relevant here. For some code-based cryptosystems, t is sublinear in n, [McE78, AAB+21a, AAB+21b, BCL+19, AAB+21b], for some Stern like signatures schemes [Ste93, Vér96, CVA10, AGS11, GPS22, FJR22] it is precisely decoding at the Gilbert-Varshamov distance that is relevant. It is at this distance that the decoding problem is expected to be the hardest. Recall that the Gilbert-Varshamov distance $d_{\mathrm{GV}}(n, k)$ is given by $d_{\mathrm{GV}}(n, k) \stackrel{\text{def}}{=} n\, h^{-1}(1 - R)$, where $R \stackrel{\text{def}}{=} \frac{k}{n}$ is the code rate, h is the binary entropy function $h(x) \stackrel{\text{def}}{=} -x \log_2 x - (1 - x) \log_2(1 - x)$ and $h^{-1}(x)$ its inverse ranging over $\left(0, \frac{1}{2}\right)$. Above this bound, the number of solutions becomes exponential and this helps to devise more efficient decoders.

Concerning now the LPN problem, it has long been recognized that having an unbounded number of queries or codelength while having a fixed error probability p per bit as in LPN makes the problem really simpler. The best algorithms for solving this problem, are BKW type algorithms [BKW03, EKM17] and are of subexponential complexity $2^{\mathcal{O}(k/\log k)}$. However, this is not true anymore if the number of queries is fixed and the error rate p is chosen such that the problem is the hardest, namely when $h(p) = 1 - k/n$. In this case, the best algorithms behave exponentially in $\min(k, n-k)$ despite many efforts on this issue [Pra62, Ste88, Dum91, BLP11, MMT11, BJMM12, MO15, BM17, BM18, CDMT22].

Reduction from Decoding to an LPN Problem. Note that until very recently, all the best algorithms for solving the decoding problem or the LPN problem when it is the hardest have been ISD algorithms. They all rely crucially on the Prange bet, namely that we have finally found after many trials a subset of positions of size $\approx n - k$ which contains almost all the errors. This was the situation since 1962 [Pra62]. There was at some point, just one exception [Dum86] which relied instead on a collision technique and gave only a slight improvement in a very tiny rate range $R \in (0.98, 1)$, but it was soon found out how to incorporate this technique in ISD algorithms [Ste88, Dum89] to improve them. However in 2022, a new algorithm called RLPN-decoding was introduced in [CDMT22]. It relies on a completely different approach following an old idea called "statistical decoding" due to Al Jabri [Jab01]. The new approach consists in reducing decoding to LPN. For the first time in sixty years a strong competitor for ISD techniques was found: it outperforms ISD techniques in the low rate regime, say $R \in (0, 0.3)$ and the improvement is quite significant in the range $R \in (0, 0.2)$ say. To explain the idea, assume we are given an instance of the decoding problem $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in \mathcal{C}$ and $|\mathbf{e}| = t$. As in statistical decoding, decoding relies on low weight parity-check equations, namely vectors $\mathbf{h}$ such that $\langle \mathbf{h}, \mathbf{c} \rangle = 0$ for any $\mathbf{c} \in \mathcal{C}$ (in other words, such $\mathbf{h}$'s belong to the dual code $\mathcal{C}^{\perp}$). However, in the new approach these parity-check equations are required to be of low weight only on a subset $\mathscr{N}$ of positions. The rest of the

positions $\mathscr{P}$ correspond to the entries of $\mathbf{e}$ we aim to recover and is the secret in the LPN problem. The point of the whole approach is that

$$\langle \mathbf{y}, \mathbf{h} \rangle = \langle \mathbf{e}, \mathbf{h} \rangle = \sum_{j \in \mathscr{P}} h_j e_j + \sum_{j \in \mathscr{N}} h_j e_j = \underbrace{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} \rangle}_{\text{lin. comb.}} + \underbrace{\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle}_{\text{LPN noise}}.$$

Here the notation $\mathbf{e}_{\mathscr{P}}$ means the restriction of $\mathbf{e}$ to the positions in $\mathscr{P}$: $\mathbf{e}_{\mathscr{P}} = (e_i)_{i \in \mathscr{P}}$. Vector $\mathbf{e}_{\mathscr{P}}$ is interpreted as the LPN secret $\mathbf{s}$, *i.e.* $\mathbf{s} \stackrel{\text{def}}{=} \mathbf{e}_{\mathscr{P}}$ and $\mathbf{h}_{\mathscr{P}}$ as the linear combination vector $\mathbf{a}$ while $\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$ is the LPN noise. Therefore, by computing $(\mathbf{h}, \langle \mathbf{y}, \mathbf{h} \rangle)$ we really have access to the LPN sample

$$\underbrace{\mathbf{a}}_{\mathbf{h}_{\mathscr{P}}}, \overbrace{\underbrace{\langle \mathbf{s}, \mathbf{a} \rangle}_{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} \rangle} + \underbrace{e}_{\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle}}^{= \langle \mathbf{y}, \mathbf{h} \rangle}.$$

The point of choosing low weight vectors $\mathbf{h}$ on $\mathscr{N}$, is that it is readily verified that this translates into the fact that the binary random variable $\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$ is biased, say $\mathbb{P}(\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle = 1) = \frac{1-\varepsilon}{2}$ with a bias ε which gets bigger when the Hamming weight $|\mathbf{h}_{\mathscr{N}}|$ of $\mathbf{h}$ on $\mathscr{N}$ gets smaller.

Recovering $\mathbf{e}_{\mathscr{P}}$ is then performed by producing enough parity-check equations to have enough information on $\mathbf{e}_{\mathscr{P}}$ (we need about $N \approx 1/\varepsilon^2$ parity-check equations) and amounts to solve the LPN problem. This is done by the Fast Fourier Transform (FFT) and costs about $s2^s$ where $s \stackrel{\text{def}}{=} |\mathscr{P}|$. We cannot afford more sophisticated techniques like the BKW algorithm which would give a sub-exponential algorithm, because we are very far away from the constant error probability regime. Here the bias ε is exponentially small in the codelength, so we are really in the extreme noise regime, where on top of that we have hardly more LPN samples than the number we need to recover the secret. In other words, we are in a situation where we can only use very basic algorithms, and the FFT which saves a factor N when compared to plain exhaustive search over all possible LPN secrets comes in handy here. The low weight parity-check equations are found by using collision techniques which are borrowed from advanced ISD techniques [Dum89, BJMM12].

The improvement upon statistical decoding given by RLPN is really due to this splitting in two parts. Recall that plain statistical decoding uses parity-checks which are low weight on the *whole support*. In both cases, $\frac{1}{\varepsilon^2}$ of such parity-checks are needed, however in RLPN decoding the bias ε is way bigger because the weight we have on $\mathscr{N}$ is way smaller for our parity-checks.

Dual Attacks, Some Negative Results and a New Analysis. Statistical decoding [Jab01] or its variant, namely RLPN decoding, both fall into the category of *dual attacks* meaning a decoding algorithm that computes in a first step low weight codewords in the dual code and then computes the inner products of the received word $\mathbf{y}$ with those parity-checks to infer some information about the error $\mathbf{e}$. These methods can be viewed as the coding theoretic analogue of the dual attacks in lattice-based cryptography [MR09]. Similarly to what happened in code-based cryptography, they were shown after a sequence of improvements [Alb17, EJK20, GJ21, MAT22, CST22] to be able of being competitive with primal attacks, and the crucial improvement came from similar techniques, namely by a splitting strategy. Like in RLPN decoding, the point is that this splitting in two parts really allows to find dual vectors that are of smaller weight/norm on the restricted subset. Note that this idea was already put forward for statistical decoding (but not exploited there) in [DT17a, §8, p.33] or [DT17b, p. 21].

However, the analysis in both settings relies on various independence assumptions, see for instance [MAT22, Ass. 4.4, Ass. 5.8] for dual attacks in lattices or [CDMT22, Ass. 3.7] for dual attacks for codes. In lattice-based cryptography, the dual attacks were strongly questioned recently in [DP23b] by showing that these independence assumptions made for analyzing dual attacks were in contradiction with some theorems in certain regimes or with well-tested heuristics in some other regimes. Note that it was already noticed in [CDMT22, §3.4] that the i.i.d. Bernoulli model implied by the LPN model for the $\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$'s is not always accurate, but it was conjectured there that the discrepancy between this ideal model and experiments does not impact the asymptotic analysis of the decoding based on this model. This was proved to be wrong in [MT23] where it was shown that the number of candidates passing the validity test of the RLPN decoder given in [CDMT22]

is actually exponentially large for the parameters considered there, whereas there should be only one candidate passing the test if the algorithm was correct. However, this paper gave at the same time an approach for analyzing rigorously dual attacks in coding theory by bringing in a duality equation [MT23, Prop. 1.3] which relates the fundamental quantity manipulated by the decoder and the weight distribution of translates of a shortened version of the code to be decoded. By studying this weight distribution together with an assumption whose validity has been verified experimentally, a slightly modified RLPN decoder was introduced there and shown to attain the complexity exponent claimed in [CDMT22].

1.2. Our Contribution.

(*i*) improving RLPN-decoding by a reduction from sparse LPN to plain LPN,

(*ii*) a rigorous analysis of the decoding algorithm based on a simple assumption verified experimentally.

Reduction from Sparse LPN to Plain LPN. Notice that the LPN problem we have to solve is actually a *sparse* LPN problem: $\mathbf{e}_{\mathscr{P}}$ is not uniformly distributed among $\mathbb{F}_2^s$ since it is of low weight. Indeed, it is the restriction to $\mathscr{P}$ of a vector which is itself of low weight. Unfortunately, the FFT algorithm used for recovering $\mathbf{e}_{\mathscr{P}}$ is unable to exploit this fact. In a sense, what we need here to improve RLPN decoding is an algorithm for solving sparse secret LPN in the very noisy regime (but with an exponential number of samples). This can be done by using a coded-BKW technique that was introduced in [GJL14]. There it was not used as a technique for solving sparse LPN but as a technique to improve the reduction steps of the BKW algorithm [BKW03] that put together pairs of vectors $\mathbf{a}$ and $\mathbf{a}'$ which are equal on a block of positions and add the corresponding LPN samples to get an LPN sample $(\mathbf{a}+\mathbf{a}', \langle \mathbf{a}+\mathbf{a}', \mathbf{s}\rangle + e + e')$ which is more noisy but with vectors $\mathbf{a}$ which become sparser and sparser as the number of blocks increases. Asking exact collisions on the block needs a lot of LPN samples and this can be relaxed by the coded-BKW technique. It basically uses a code of the same length as the block of positions we are considering during the BKW step and asks only an approximate collision on the block meaning that the closest codewords $\mathbf{c}$ and $\mathbf{c}'$ to $\mathbf{a}$ and $\mathbf{a}'$ restricted to this block should be the same.

To explain what we have in mind here, consider an LPN sample which is of the following form $(\mathbf{h}_{\mathscr{P}}, \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}}\rangle + e)$. Choose now a linear code $\mathcal{C}_{\mathrm{aux}}$ of length s and dimension k_{aux} (*i.e.* a subspace of $\mathbb{F}_2^s$) which we know how to decode for any possible entry, meaning here that we can produce for any entry $\mathbf{y} \in \mathbb{F}_2^s$ a codeword $\mathbf{c}_{\mathrm{aux}} \in \mathcal{C}_{\mathrm{aux}}$ which is close *enough* to $\mathbf{y}$. Codes with this property are known under the name of *lossy source codes* in information theory. In [GJL14] it was proposed to use for instance a product of small codes. There are almost optimal codes (producing for a given dimension k_{aux} almost optimal near codewords) using a low complexity decoder. Basically, the best that can be done is to produce codewords at distance $d_{\mathrm{GV}}(s, k_{\mathrm{aux}})$. For instance polar codes are asymptotically optimal [KU10], they attain asymptotically this Gilbert-Varshamov distance by using only a decoding algorithm of quasi-linear complexity $\mathcal{O}(s \log s)$.

Consider now a parity-check $\mathbf{h}$ of small weight w on $\mathscr{N}$ that we use for RLPN-decoding and decode $\mathbf{h}_{\mathscr{P}}$ with the lossy source code $\mathcal{C}_{\mathrm{aux}}$: $\mathbf{h}_{\mathscr{P}} = \mathbf{c}_{\mathrm{aux}} + \mathbf{e}_{\mathrm{aux}}$ where $\mathbf{c}_{\mathrm{aux}} \in \mathcal{C}_{\mathrm{aux}}$ and $|\mathbf{e}_{\mathrm{aux}}|$ is small. Consider a generator matrix $\mathbf{G}_{\mathrm{aux}}$ of $\mathcal{C}_{\mathrm{aux}}$, namely a $k_{\mathrm{aux}} \times s$ matrix such that $\mathcal{C}_{\mathrm{aux}} = \{\mathbf{u}\mathbf{G}_{\mathrm{aux}} : \mathbf{u} \in \mathbb{F}_2^{k_{\mathrm{aux}}}\}$ (*i.e.* the rows of $\mathbf{G}_{\mathrm{aux}}$ generate $\mathcal{C}_{\mathrm{aux}}$). Notice now that

$$\begin{aligned}\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}}\rangle &= \langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\mathrm{aux}} + \mathbf{e}_{\mathrm{aux}}\rangle = \langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\mathrm{aux}}\rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\mathrm{aux}}\rangle \\ &= \langle \mathbf{e}_{\mathscr{P}}, \mathbf{u}\mathbf{G}_{\mathrm{aux}}\rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\mathrm{aux}}\rangle \quad (\text{where } \mathbf{u} \in \mathbb{F}_2^{k_{\mathrm{aux}}}) \\ &= \langle \mathbf{e}_{\mathscr{P}}\mathbf{G}_{\mathrm{aux}}^{\intercal}, \mathbf{u}\rangle + \underbrace{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\mathrm{aux}}\rangle}_{\text{biased}}.\end{aligned}$$

If we plug this expression in the original LPN sample $(\mathbf{h}_{\mathscr{P}}, \langle \mathbf{h}, \mathbf{y}\rangle = \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle)$ we obtain

$$\langle \mathbf{h}, \mathbf{y}\rangle = \langle \mathbf{e}_{\mathscr{P}}\mathbf{G}_{\mathrm{aux}}^{\intercal}, \mathbf{u}\rangle + \underbrace{\langle \mathbf{e}, \mathbf{e}_{\mathrm{aux}}\rangle}_{\text{noise 1}} + \underbrace{\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle}_{\text{noise 2}}.$$

In other words, we have a new LPN problem where

$$\underbrace{\mathbf{a}}_{\mathbf{u}}, \overbrace{\underbrace{\langle \mathbf{s}, \mathbf{a} \rangle}_{\langle \mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^{\intercal}, \mathbf{u} \rangle} + \underbrace{e}_{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle}}^{\langle \mathbf{y}, \mathbf{h} \rangle}. \tag{1}$$

The new secret is not anymore a part $\mathbf{e}_{\mathscr{P}}$ of the error but a linear combination $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ of it and the LPN noise has increased somehow. However, now the secret is way smaller, it belongs to $\mathbb{F}_2^{k_{\text{aux}}}$. The situation is changed significantly by this. Before, basically the optimal parameters for RLPN-decoding were such that the cost of FFT decoding the LPN secret, namely $\mathcal{O}(s2^s)$ is of the same order as $1/\varepsilon^2$ the number of parity-check equations we need. Here ε is defined by

$$\mathbb{P}(e = 1) = \frac{1 - \varepsilon}{2}.$$

Recall that ε is basically a decreasing function of the weight w of the parity-check equations we are able to produce. Here since we do not pay anymore $\mathcal{O}(s2^s)$ for FFT decoding the new LPN secret but $\mathcal{O}\big(k_{\text{aux}}2^{k_{\text{aux}}}\big)$ we can take larger values for s which themselves give a smaller support $\mathscr{N}$ resulting in much smaller weight w on $\mathscr{N}$ and thus the bias term coming from $\langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$ is much smaller. Of course there is an additional noise term now which is $\langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\text{aux}} \rangle$. However, all in all, the gain we have by being able to use a much larger s outweighs the additional noise term. It can also be observed that we do not recover $\mathbf{e}_{\mathscr{P}}$ but k_{aux} linear combinations of bits of $\mathbf{e}_{\mathscr{P}}$. This is easy to fix by running a few times more this algorithm with other lossy source codes $\mathcal{C}_{\text{aux}}$ until getting enough linear combinations to be able to recover $\mathbf{e}_{\mathscr{P}}$.

We call this new algorithm double-RLPN-decoding, since it is based on two successive reductions: first we reduce the problem to sparse-LPN, then we reduce the sparse-LPN to a plain-LPN problem as explained above.

double-RLPN-Decoding and its Analysis. It turns out that the LPN problem given in Equation (1) is more structured than a standard LPN problem and like what happened in the RLPN algorithm [CDMT22], producing the most likely candidate for the LPN problem does not necessarily produce the right candidate $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ even if we have enough samples for ensuring that in the ideal i.i.d model of the LPN problem the most likely candidate would indeed be the right solution. Again, the i.i.d. model is not accurate. We have to use the whole information given by the FFT and output for L big enough the L most likely solutions to have a chance to have $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ in the list. However, verifying whether a candidate $\mathbf{s}$ for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ is indeed valid is relatively straightforward:

- (a) we can as in the RLPN algorithm make a bet on the weight $|\mathbf{e}_{\mathscr{P}}|$, say $|\mathbf{e}_{\mathscr{P}}| = t'$ (and run enough double-RLPN decoding steps until finding a partition $\mathscr{P} \cup \mathscr{N}$ for which this bet is valid),
- (b) recover $\mathbf{e}_{\mathscr{P}}$ by solving the decoding problem (in its syndrome form) $\mathbf{s} = \mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ and $|\mathbf{e}_{\mathscr{P}}| = t'$,
- (c) check whether the putative candidate $\mathbf{v}$ for $\mathbf{e}_{\mathscr{P}}$ we get can be extended to a complete solution by solving the decoding problem $\mathbf{y} = \mathbf{c} + \mathbf{e}$, $\mathbf{e}_{\mathscr{P}} = \mathbf{v}$, $\mathbf{c} \in \mathcal{C}$ and $|\mathbf{e}| = t$ which is much easier to solve than the original decoding problem due to the partial knowledge about $\mathbf{e}$, *i.e.* $\mathbf{e}_{\mathscr{P}} = \mathbf{v}$.

The whole problem we face here for analyzing the problem is the same as the one that was faced to analyze the RLPN algorithm, the i.i.d. LPN model is not valid and we really have to get rid of the independence assumptions. Part of this work is achieved by adapting one of the fundamental tools used for analyzing RLPN decoding, namely [CDMT22, Proposition 3.1] which gives a formula of the bias ε in terms of Krawtchouk polynomials. We will obtain a generalization of this proposition adapted to the double-RLPN decoder, namely Proposition 2 in §3. Note that Proposition 2 does not rely on unproven assumptions contrarily to what is done in dual attacks in lattice-based cryptography where the corresponding result is achieved through independence assumptions.

Estimating the number L of candidates for the LPN problem given in Equation (1) we have to keep for being sure to have $\mathbf{e}_{\mathscr{J}}\mathbf{G}_{\text{aux}}^{\intercal}$ is even more delicate. It requires a careful adaptation to our setting of [MT23] that analyzed the RLPN decoder. Here, we will not be able to avoid completely assumptions for performing the analysis (but this was also the case in [MT23]). However, again we will not resort to independence assumptions which seem in our context not only to be wrong strictly speaking, but also to be unable to be good enough for capturing the size of L. We will namely develop some tools analogous to what has been achieved in [MT23]:

(i) a duality result, namely Proposition 4 of §5.3, which expresses the FFT value of a candidate as a weighted sum of the product of evaluations of Krawtchouk polynomials where the weights come from a certain weight distributions of codes related to $\mathcal{C}$ and $\mathcal{C}_{\text{aux}}$. This is an adaptation of [MT23, Prop. 3.2] to our setting and is the key for estimating L as explained in §5.2,

(ii) an estimation of this sum with probabilistic considerations. These probabilistic considerations are rigorous for the part of the sum which is most certainly the dominating term. However for the part of the sum which is very likely to be negligible, we lack accurate tail bounds for the number of codewords of a given weight in a random linear code and in this case we just conjecture that the part of the sum which seems negligible and for which we have only partial control with the probabilistic tool at hand, is indeed negligible. This conjecture has been verified experimentally and we even used a very crude approximation of this weighted sum with the help of independent Poisson variables which captures the size of L obtained in our experiments and which implies our conjecture.

All in all with the help of a conjecture that we verified experimentally, we are able to capture the size of L and to obtain a formula for the complexity of double-RLPN decoding. The key tool for performing this analysis, namely the duality result, can be readily adapted to lattices (see §8). It turns out that even a crude use of this duality result gives a good explanation of the part of the experimental curve departing from the theoretical curve based on the standard independence assumption found in [DP23b, Fig. 3]. This substantiates the claim made in [MT23, §6] that the code duality result of [MT23] carries over to the lattice setting and can be used to predict dual attacks without using the independence assumption.

The Results Obtained by this New Approach. This new approach results in a very significant gain compared to RLPN decoding. Our most advanced version of double-RLPN-decoding algorithm performs better than the current state of the art ISD algorithm for all rates $R \leqslant 0.42$ as shown in Figure 1.

Concurrent/related work. Very recently, we became aware that the prediction we have made on the score function for lattices by using our duality result and crude estimates of the relevant sum (see §8) has also been obtained by using as we do here Bessel functions and related tools in [DP23a]. This paper provides a much more in depth study as we do here.

2. Notation and Coding Theory Background

Basic Notation. Vectors and matrices are respectively denoted in bold letters and bold capital letters such as $\mathbf{a}$ and $\mathbf{A}$. The entry at index i of the vector $\mathbf{x}$ is denoted by x_i or $x(i)$. The canonical inner product $\sum_{i=1}^{n} x_i y_i$ between two vectors $\mathbf{x}$ and $\mathbf{y}$ of $\mathbb{F}_2^n$ is denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$ where $\mathbb{F}_2$ denotes the binary field. Let $\mathscr{I}$ be a list of indexes. We denote by $\mathbf{x}_{\mathscr{I}}$ the vector $(x_i)_{i \in \mathscr{I}}$. In the same way, we denote by $\mathbf{A}_{\mathscr{I}}$ the sub-matrix made of the columns of $\mathbf{A}$ which are indexed by $\mathscr{I}$. We denote by $\mathbf{0}_n \in \mathbb{F}_2^{n \times n}$ and $\mathbf{Id}_n \in \mathbb{F}_2^{n \times n}$ the null matrix and the identity matrix of size n respectively. The concatenation of two vectors $\mathbf{x}$ and $\mathbf{y}$ is denoted by $\mathbf{x}||\mathbf{y}$. The Hamming weight of a vector $\mathbf{x}$ and the cardinality of a finite set $\mathscr{A}$ are denoted in the same way by $|\mathbf{x}|$ and $|\mathscr{A}|$ respectively. There will be no confusion since they apply to different objects. Notation $[\![a, b]\!]$ stands for the set of the integers between a and b, both included. Furthermore, we let $\mathcal{S}_w^n$ denote the Hamming sphere of $\mathbb{F}_2^n$ with radius w and centered at $\mathbf{0}$, namely

$$\mathcal{S}_w^n \stackrel{\text{def}}{=} \{\mathbf{x} \in \mathbb{F}_2^n \ : |\mathbf{x}| = w\}.$$

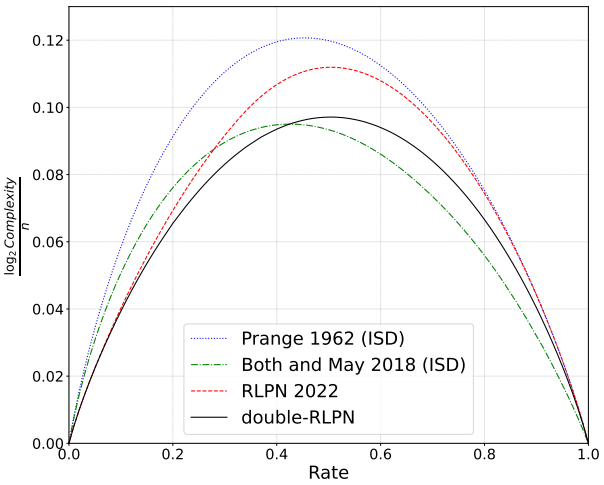

FIGURE 1. Asymptotic complexity exponent of some decoding algorithms: our new double-RLPN decoder, the RLPN decoder, Both and May algorithm [BM18] (with the correction of [CDMT22, Ess22]) which is the state-of-the-art of ISD decoders and the Prange decoder [Pra62].

Probabilistic Notation. For a finite set $\mathscr{S}$, we write $X \xleftarrow{\$} \mathscr{S}$ when X is an element of $\mathscr{S}$ drawn uniformly at random in it. For a Bernoulli random variable X, denote by $\mathrm{bias}(X)$ the quantity

$$\mathrm{bias}(X) \stackrel{\text{def}}{=} \mathbb{P}(X=0) - \mathbb{P}(X=1).$$

For a Bernoulli random variable X of parameter $p = \frac{1-\varepsilon}{2}$, *i.e.* $\mathbb{P}(X=1) = \frac{1-\varepsilon}{2}$, we have $\mathrm{bias}(X) = \varepsilon$.

Fourier Transform. Let $f : \mathbb{F}_2^n \to \mathbb{R}$ be a function. We define its Fourier transform $\widehat{f} : \mathbb{F}_2^n \to \mathbb{R}$ as

$$\widehat{f}(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{F}_2^n} f(\mathbf{u}) (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle}. \tag{2}$$

Soft-O Notation. For real valued functions defined over $\mathbb{R}$ or $\mathbb{N}$ we define $o()$, $\mathcal{O}()$, $\Omega()$, $\Theta()$, in the usual way and also use the less common notation $\widetilde{\mathcal{O}}()$ and $\widetilde{\Omega}()$, where $f = \widetilde{\mathcal{O}}(g)$ means that $f(x) = \mathcal{O}\left(g(x) \log^k g(x)\right)$ and $f = \widetilde{\Omega}(g)$ means that $f(x) = \Omega\left(g(x) \log^k g(x)\right)$ for some k. We will use this for functions which have an exponential behavior, say $g(x) = e^{\alpha x}$, in which case $f(x) = \widetilde{\mathcal{O}}(g(x))$ means that $f(x) = \mathcal{O}(P(x)g(x))$ where P is a polynomial in x. We also use $f = \omega(g)$ when f dominates g asymptotically; that is when $\lim_{x \to \infty} \frac{|f(x)|}{g(x)} = \infty$.

Coding Theory. A binary linear code $\mathcal{C}$ of length n and dimension k is a subspace of $\mathbb{F}_2^n$ of dimension k. We say that it has parameters $[n,k]$ or that it is an $[n,k]$-code. Its *rate* R is defined as $R \stackrel{\text{def}}{=} \frac{k}{n}$. A generator matrix $\mathbf{G}$ for $\mathcal{C}$ is a full rank $k \times n$ matrix over $\mathbb{F}_2$ such that

$$\mathcal{C} = \left\{ \mathbf{uG} : \mathbf{u} \in \mathbb{F}_2^k \right\}.$$

A parity-check matrix $\mathbf{H}$ for $\mathcal{C}$ is a full-rank $(n-k) \times n$ matrix over $\mathbb{F}_2$ such that

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_2^n : \mathbf{Hc}^\intercal = \mathbf{0} \right\}.$$

In other words, $\mathcal{C}$ is the null space of $\mathbf{H}$. The dimension of the code is given by $\dim(\mathcal{C}) \stackrel{\text{def}}{=} k$. The code whose generator matrix is the parity-check matrix of $\mathcal{C}$ is called the dual code of $\mathcal{C}$. It might be seen as the subspace of parity-checks of $\mathcal{C}$ and is defined equivalently as

Definition 1 (Dual Code)**.** *The* dual code $\mathcal{C}^{\perp}$ *of an* $[n,k]$*-code* $\mathcal{C}$ *is an* $[n,n-k]$*-code which is defined by*

$$\mathcal{C}^{\perp} \stackrel{def}{=} \{\mathbf{h} \in \mathbb{F}_2^n : \forall \mathbf{c} \in \mathcal{C},\ \langle \mathbf{c}, \mathbf{h} \rangle = 0\}.$$

Sometimes it is considered in the literature the following equivalent version of the decoding problem (see Problem 3 as defined in the introduction) by using instead the parity-check matrix and syndrome point of view

Problem 3 (Decoding a fixed error weight via syndromes)**.** *Let* $\mathcal{C}$ *be an* $[n,k]$*-code with parity-check matrix* $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$*. We are given a syndrome* $\mathbf{s} \in \mathbb{F}_2^{n-k}$*, an integer* t *and we want to find an error vector* $\mathbf{e} \in \mathbb{F}_2^n$ *of Hamming weight* $|\mathbf{e}| = t$ *for which* $\mathbf{H}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$*.*

It is readily seen that both Problems 1 and 3 are equivalent: given $\mathcal{C}$ with parity-check matrix $\mathbf{H}$, then decoding $\mathbf{c}+\mathbf{e}$ with a codeword $\mathbf{c} \in \mathcal{C}$ and $\mathbf{e} \in \mathcal{S}_t^n$ amounts to recover $\mathbf{e}$ from $\mathbf{H}\mathbf{y}^{\intercal} = \mathbf{H}\mathbf{e}^{\intercal}$ as by definition $\mathbf{H}\mathbf{c}^{\intercal} = \mathbf{0}$.

When $\mathcal{C}$ is an $[n,k]$-code and $\mathbf{x} \in \mathbb{F}_2^n$ we let

$$\mathcal{C} + \mathbf{x} \stackrel{\text{def}}{=} \{\mathbf{c} + \mathbf{x}\,, \mathbf{c} \in \mathcal{C}\}$$

denote a coset of $\mathcal{C}$ and we denote by $N_i(\mathcal{C}+\mathbf{x})$ the number of words of hamming weight i in the coset $\mathcal{C}+\mathbf{x}$, namely

$$N_i(\mathcal{C}+\mathbf{x}) \stackrel{\text{def}}{=} |\mathcal{C} + \mathbf{x} \cap \mathcal{S}_i^n|\,.$$

An important quantity is the *Gilbert-Varshamov* distance which is defined as

Definition 2 (Gilbert-Varshamov distance)**.** *The Gilbert-Varshamov distance* $d_{\mathrm{GV}}(n,k)$ *associated to a length* n *and dimension* k *is defined as the largest integer* d *such that*

$$2^k |\mathscr{B}_d| < 2^n$$

where $\mathscr{B}_d$ *is the Hamming ball centered at* $\mathbf{0}$ *in* $\mathbb{F}_2^n$ *and radius* d*, that is* $\mathscr{B}_d \stackrel{def}{=} \{\mathbf{x} \in \mathbb{F}_2^n :\ |\mathbf{x}| \leqslant d\}$*.*

This quantity has two different interpretations. On one hand, it corresponds up to a constant term to the *typical minimum distance* of a linear code of length n and dimension k, but it is also related to the expected number of solutions of the decoding problem for a random linear $[n,k]$-code which is defined as follows.

Problem 4 ((n,k,t) Decoding Problem - $\mathsf{DP}(n,k,t)$)**.**

- Given: $(\mathbf{G}, \mathbf{y} \stackrel{def}{=} \mathbf{m}\mathbf{G} + \mathbf{x})$ *where* $\mathbf{m}, \mathbf{G}$ *and* $\mathbf{x}$ *are respectively picked uniformly at random over* $\mathbb{F}_2^k$*,* $\mathbb{F}_2^{k\times n}$ *and* $\mathcal{S}_t^n$*.*
- Aim: *an error* $\mathbf{e} \in \mathbb{F}_2^n$ *of Hamming weight* t *such that* $\mathbf{y} - \mathbf{e} = \mathbf{z}\mathbf{G}$ *for some* $\mathbf{z} \in \mathbb{F}_2^k$*.*

This problem really corresponds to decoding at distance t the $[n,k]$-code admitting $\mathbf{G}$ as generator matrix. The largest weight t for which we might hope for having a single solution (strictly speaking when we look for solutions of weight $\leqslant t$ and not exactly t, but the difference between these two notions is generally irrelevant) is given by the Gilbert-Varshamov distance $d_{\mathrm{GV}}(n,k)$. At this distance, the expected number of solutions is readily seen to be $\Theta(1)$ whether we look at codewords at distance exactly t from the received word $\mathbf{y}$ or at distance $\leqslant t$.

It will also be very convenient to consider the operation of puncturing a code, *i.e.* keeping only a subset of entries in a codeword.

Definition 3 (Punctured Code)**.** *For a code* $\mathcal{C}$ *and a subset* $\mathscr{I}$ *of code positions, we denote by* $\mathcal{C}_{\mathscr{I}}$ *the punctured code obtained from* $\mathcal{C}$ *by keeping only the positions in* $\mathscr{I}$*,* i.e.

$$\mathcal{C}_{\mathscr{I}} = \{\mathbf{c}_{\mathscr{I}} : \mathbf{c} \in \mathcal{C}\}.$$

Definition 4 (Shortened Code)**.** *For a code $\mathcal{C}$ and a subset $\mathscr{I}$ of code positions, we denote by $\mathcal{C}^{\mathscr{I}}$ the shortened code is defined by*

$$\mathcal{C}^{\mathscr{I}} = \{\mathbf{c}_{\mathscr{I}} : \mathbf{c} \in \mathcal{C} \text{ and } \mathbf{c}_{[\![1,n]\!]\setminus\mathscr{I}} = \mathbf{0}\}.$$

It is readily seen that we have

$$\left(\mathcal{C}^{\mathscr{I}}\right)^{\perp} = \left(\mathcal{C}^{\perp}\right)_{\mathscr{I}} \quad \text{and} \quad \left(\mathcal{C}_{\mathscr{I}}\right)^{\perp} = \left(\mathcal{C}^{\perp}\right)^{\mathscr{I}}. \tag{3}$$

Krawtchouk Polynomial. We recall here some properties about Krawtchouk polynomial that will be useful in the article. Many useful properties can be found in [KS21, §2.2]

Definition 5. *(Krawtchouk polynomial) We define the Krawtchouk polynomial $K_w^{(n)}$ of degree w and of order n as*

$$K_w^{(n)}(X) \stackrel{def}{=} \sum_{j=0}^{w} (-1)^j \binom{X}{j}\binom{n-X}{w-j}.$$

The following fact is well known: it gives an alternate expression of the Krawtchouk polynomial (see for instance [vL99, Lemma 5.3.1]).

Fact 1. *For any $\mathbf{x} \in \mathbb{F}_2^n$,*

$$K_w^{(n)}(|\mathbf{x}|) = \widehat{\mathbb{1}_w}(\mathbf{x}) = \sum_{\mathbf{y}\in\mathbb{F}_2^n : |\mathbf{y}|=w} (-1)^{\langle \mathbf{x},\mathbf{y}\rangle}. \tag{4}$$

where $\mathbb{1}_w$ is the characteristic function of the Hamming sphere $\mathcal{S}_w^n$ of radius w.

We recall here the summary of some known results about Krawtchouk polynomials made in [CDMT22].

Proposition 1. [CDMT22, Prop. 3.5, Prop. 3.6]

(1) **Value at 0.** *For all $0 \leqslant w \leqslant n$, $K_w^{(n)}(0) = \binom{n}{w}$.*

(2) **Reciprocity.** *For all $0 \leqslant t, w \leqslant n$, $\binom{n}{t}K_w^{(n)}(t) = \binom{n}{w}K_t^{(n)}(w)$.*

(3) **Roots.** *The polynomials $K_w^{(n)}$'s have w distinct roots which lie in the interval $[\![n/2 - \sqrt{w(n-w)}, n/2 + \sqrt{w(n-w)}]\!]$. The distance between roots is at least 2 and at most $o(n)$.*

(4) **Magnitude in and out the root region.** *Let τ and ω be two reals in $[0,1]$. Let $\omega^{\perp} \stackrel{def}{=} \frac{1}{2} - \sqrt{\omega(1-\omega)}$, and let $z \stackrel{def}{=} \frac{1-2\tau-\sqrt{D}}{2(1-\omega)}$ where $D \stackrel{def}{=} (1-2\tau)^2 - 4\omega(1-\omega)$.*

Define $\widetilde{\kappa}(\tau,\omega) \stackrel{def}{=} \begin{cases} \tau\log_2(1-z) + (1-\tau)\log_2(1+z) - \omega\log_2 z & \text{if } \tau \in [0,\omega^{\perp}], \\ \frac{1-h(\tau)+h(\omega)}{2} & \text{otherwise.} \end{cases}$

- *4.1. If $\tau \leqslant \frac{1}{2} - \sqrt{\omega(1-\omega)}$, then for all t and w such that $\lim_{n\to\infty}\frac{t}{n} = \tau$ and $\lim_{n\to\infty}\frac{w}{n} = \omega$ we have $K_w^{(n)}(t) = 2^{n(\widetilde{\kappa}(\tau,\omega)+o(1))}$.*
- *4.2. If $\tau > \frac{1}{2} - \sqrt{\omega(1-\omega)}$, then there exists $t(n)$ and $w(n)$ such that $\lim_{n\to\infty}\frac{t}{n} = \tau$, $\lim_{n\to\infty}\frac{w}{n} = \omega$ and $\left|K_w^{(n)}(t)\right| = 2^{n(\widetilde{\kappa}(\tau,\omega)+o(1))}$.*

3. Reduction from Sparse to Plain LPN

The purpose of this section is to explain in detail the reduction from sparse to plain LPN and to give an important result about the bias of the resulting RLPN samples. We assume from now on that we are given and $[n,k]$-code $\mathcal{C}$ and a $\mathbf{y} \in \mathbb{F}_2^n$ such that

$$\mathbf{y} \stackrel{\text{def}}{=} \mathbf{c} + \mathbf{e}, \quad \mathbf{c} \in \mathcal{C},\ |\mathbf{e}| = t,$$

and we want to find $\mathbf{c}$ and $\mathbf{e}$.

3.1. **The Approach.** First, we randomly select a subset $\mathscr{P} \subseteq [\![1, n]\!]$ of s positions, where s is a parameter that will be chosen later. Let $\mathscr{N} \stackrel{\text{def}}{=} [\![1, n]\!] \setminus \mathscr{P}$ be the complementary set of $\mathscr{P}$. Here $\mathscr{P}$ corresponds to the entries of $\mathbf{e}$ we aim to recover. As explained in the introduction, the basic step of the decoding algorithm is to compute a large set $\mathscr{W}$ of parity-check equations of low weight w on $\mathscr{N}$ and to compute all the $\langle \mathbf{y}, \mathbf{h} \rangle$ with $\mathbf{h}$ ranging over $\mathscr{W}$. In RLPN decoding, the approach is to exploit directly that we have a number $|\mathscr{W}|$ of LPN samples $(\mathbf{h}_{\mathscr{P}}, \langle \mathbf{h}, \mathbf{y} \rangle)$ which can be viewed as an LPN sample $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$ by letting $\mathbf{a} \stackrel{\text{def}}{=} \mathbf{h}_{\mathscr{P}}$, $\mathbf{s} \stackrel{\text{def}}{=} \mathbf{e}_{\mathscr{P}}$, $e \stackrel{\text{def}}{=} \langle \mathbf{h}_{\mathscr{N}}, \mathbf{e}_{\mathscr{N}} \rangle$. Indeed,

$$\langle \mathbf{h}, \mathbf{y} \rangle = \langle \mathbf{h}, \mathbf{c} + \mathbf{e} \rangle = \underbrace{\langle \mathbf{h}, \mathbf{c} \rangle}_{=0} + \langle \mathbf{h}, \mathbf{e} \rangle = \underbrace{\langle \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}} \rangle}_{=\langle \mathbf{a}, \mathbf{s} \rangle} + \underbrace{\langle \mathbf{h}_{\mathscr{N}}, \mathbf{e}_{\mathscr{N}} \rangle}_{\text{LPN noise } e}.$$

Notice that we really have a sparse LPN problem because of the sparseness of the secret $\mathbf{e}_{\mathscr{P}}$ which is not exploited in [CDMT22] and only exploited to verify the solution in the corrected RLPN algorithm of [MT23]. The point of this article is to exploit the sparseness of $\mathbf{e}_{\mathscr{P}} \in \mathbb{F}_2^s$ right away in order to reduce the dimension s of the secret. This is obtained by introducing an auxiliary code $\mathcal{C}_{\text{aux}}$ of length s and dimension k_{aux} which will be instrumental for reducing the dimension s of the secret down to k_{aux}. This is obtained as follows. We will assume that $\mathcal{C}_{\text{aux}}$ is chosen as a code with an *efficient list-decoding procedure* at distance t_{aux}.

Definition 6 (Efficiently list decodable code)**.** *A code $\mathcal{C}$ of length n is said to be efficiently decodable code at distance t if it outputs for any $\mathbf{y} \in \mathbb{F}_2^n$ a non empty list of codewords of $\mathcal{C}$ at distance t in time $2^{o(n)}$.*

Moreover from now on, we assume that

Notation 1. *$\mathcal{C}_{\text{aux}}$ is an $[s, k_{\text{aux}}]$ efficiently list decodable for some distance t_{aux}. We denote by $\mathcal{D}\text{ec}(\mathbf{z})$ the set of all codewords of $\mathcal{C}_{\text{aux}}$ at distance t_{aux} from $\mathbf{z} \in \mathbb{F}_2^s$, namely*

$$\mathcal{D}\text{ec}(\mathbf{z}) = \{\mathbf{c}_{\text{aux}} \in \mathcal{C}_{\text{aux}} \ : \ |\mathbf{c}_{\text{aux}} + \mathbf{z}| = t_{\text{aux}}\}.$$

Remark 1. *In our instantiation, t_{aux} is chosen such that $t_{\text{aux}} \approx d_{\text{GV}}(s, k_{\text{aux}})$, thus we typically have $|\mathcal{D}\text{ec}(\mathbf{h}_{\mathscr{P}})| = \Theta(1)$.*

Now, let us consider $\mathbf{c}_{\text{aux}} \in \mathcal{D}\text{ec}(\mathbf{h}_{\mathscr{P}})$, a codeword of $\mathcal{C}_{\text{aux}}$ at distance t_{aux} of $\mathbf{h}_{\mathscr{P}}$. It is readily seen that $\langle \mathbf{y}, \mathbf{h} \rangle$ decomposes as:

$$\langle \mathbf{y}, \mathbf{h} \rangle = \underbrace{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}} \rangle}_{\text{linear comb.}} + \underbrace{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle}_{\text{“new” LPN noise}}.$$

Let us start by defining $\mathcal{C}_{\text{aux}}$ with a generator matrix $\mathbf{G}_{\text{aux}} \in \mathbb{F}_2^{s \times k_{\text{aux}}}$. Then, knowing $\mathbf{c}_{\text{aux}} \in \mathcal{C}_{\text{aux}}$ is equivalent to know $\mathbf{m}_{\text{aux}} \in \mathbb{F}_2^{k_{\text{aux}}}$ such that

$$\mathbf{c}_{\text{aux}} = \mathbf{m}_{\text{aux}} \mathbf{G}_{\text{aux}}.$$

We can therefore rewrite $\langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}} \rangle$ as

$$\langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}} \rangle = \langle \mathbf{e}_{\mathscr{P}}, \mathbf{m}_{\text{aux}} \mathbf{G}_{\text{aux}} \rangle = \langle \mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^{\intercal}, \mathbf{m}_{\text{aux}} \rangle.$$

We have therefore for each parity-check equation $\mathbf{h}$ of weight w on $\mathscr{N}$ that we have computed (*i.e.* for all $\mathbf{h} \in \mathscr{W}$) and each codeword $\mathbf{m}_{\text{aux}} \mathbf{G}_{\text{aux}}$ of $\mathcal{C}_{\text{aux}}$ at distance t_{aux} from $\mathbf{h}_{\mathscr{P}}$, an LPN sample $(\mathbf{m}_{\text{aux}}, \langle \mathbf{y}, \mathbf{h} \rangle)$ which can be viewed as such by noticing that it is indeed equal to

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \quad \text{with} \quad \begin{cases} \mathbf{a} \stackrel{\text{def}}{=} \mathbf{m}_{\text{aux}} \\ \mathbf{s} \stackrel{\text{def}}{=} \mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^{\intercal} \\ e \stackrel{\text{def}}{=} \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle \end{cases} \tag{5}$$

Notice here that, if $\mathcal{D}\text{ec}(\mathbf{h}_{\mathscr{P}})$ contains more than one element, we can compute such LPN samples for each different $\mathbf{c}_{\text{aux}} \in \mathcal{D}\text{ec}(\mathbf{h}_{\mathscr{P}})$. The secret in the above LPN sample is no longer given by $\mathbf{e}_{\mathscr{P}}$ that we want to recover (contrarily to RLPN-decoding [CDMT22]), but is given by $\mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^{\intercal} \in \mathbb{F}_2^{k_{\text{aux}}}$ which are $k_{\text{aux}} < s$ linear equations involving the $s = |\mathscr{P}|$ bits of the vector $\mathbf{e}$ we are looking for.

The main advantage of our new technique is that we end up with an LPN problem whose dimension of the secret has decreased from s to k_{aux}. However, the noise has increased; let us describe how it behaves in the following paragraph.

3.2. **Estimating the New Noise.** The error e in Equation (5) is biased toward zero and its bias is a function of n, s, t and u, w, t_{aux} which are respectively

$$u \stackrel{\text{def}}{=} |\mathbf{e}_{\mathscr{N}}|, \quad w \stackrel{\text{def}}{=} |\mathbf{h}_{\mathscr{N}}| \quad \text{and} \quad t_{\text{aux}} \stackrel{\text{def}}{=} |\mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}}|.$$

In the following statement we compute the bias of e over all the possible LPN samples, that is we compute

$$\operatorname*{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}} (\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\text{aux}} + \mathbf{c}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle) = \frac{1}{\left|\widetilde{\mathscr{H}}\right|} \sum_{(\mathbf{h},\mathbf{c}_{\text{aux}}) \in \widetilde{\mathscr{H}}} (-1)^{\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle}$$

where $\widetilde{\mathscr{H}}$ is defined by

Definition 7.

$$\widetilde{\mathscr{H}} \stackrel{def}{=} \{(\mathbf{h}, \mathbf{c}_{\text{aux}}) \in \mathcal{C}^{\perp} \times \mathcal{C}_{\text{aux}} \ : \ |\mathbf{h}_{\mathscr{N}}| = w \text{ and } |\mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}}| = t_{\text{aux}}\}. \tag{6}$$

It is tempting to conjecture that this bias is well approximated by the bias of a Bernoulli variable $X \stackrel{\text{def}}{=} \langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{w} \rangle$ where $\mathbf{e}_{\text{aux}}$ and $\mathbf{w}$ are respectively drawn uniformly at random in the Hamming spheres $\mathcal{S}^s_{t_{\text{aux}}}$ and $\mathcal{S}^{n-s}_w$. The sum $\langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{w} \rangle$ is performed over $\mathbb{F}_2$ and all the vectors are independent random variables. Because of the independence of the random variables, from the straightforward fact that $\operatorname{bias}(X_1 + X_2) = \operatorname{bias}(X_1) \operatorname{bias}(X_2)$ when X_1 and X_2 are independent Bernoulli variables (and the addition is performed modulo 2). Therefore,

$$\begin{aligned} \operatorname{bias}(X) &= \operatorname{bias}\left(\langle \mathbf{e}_{\mathscr{P}}, \mathbf{e}_{\text{aux}} \rangle\right) \operatorname{bias}\left(\langle \mathbf{e}_{\mathscr{N}}, \mathbf{w} \rangle\right) \\ &= \frac{K^{(s)}_{t_{\text{aux}}}(t-u)}{\binom{s}{t_{\text{aux}}}} \frac{K^{(n-s)}_w(u)}{\binom{n-s}{w}} \qquad \text{(by Fact 1)}. \end{aligned}$$

This kind of approximation was done in the early days of statistical decoding [Jab01, Ove06, DT17c], until [CDMT22, Prop. 3.1] which has shown that under certain conditions, *i.e.* when there are enough available parity-check equations of weight w (essentially when the number is of order $\omega(1/\delta^2)$ where δ is the bias), then this approximation can indeed be shown to hold with overwhelming probability. It turns out that [CDMT22, Prop. 3.1] can be adapted to our setting with some additional technicalities and conditions. It can be shown that with overwhelming probability we indeed have

$$\operatorname*{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}} (\langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle) = (1 + o(1)) \operatorname{bias}(X).$$

This is in essence what the following proposition shows.

Proposition 2. *Suppose that the parameters are such that for some constant $\alpha > 0$*

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} = \omega\left(\frac{n^{\alpha}}{\delta^2}\right) \qquad \text{where} \qquad \delta \stackrel{def}{=} \frac{K^{(n-s)}_w(u)\, K^{(s)}_{t_{\text{aux}}}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}. \tag{7}$$

Moreover suppose that

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^k} = \mathcal{O}(n^{\alpha}) \quad \text{and} \quad \frac{\binom{s}{t_{\text{aux}}}}{2^{s-k_{\text{aux}}}} = \mathcal{O}(n^{\alpha}). \tag{8}$$

Let $\mathscr{N}$ be a set of $n-s$ positions in $[\![1,n]\!]$ and $\mathscr{P} \stackrel{def}{=} [\![1,n]\!] \backslash \mathscr{N}$. Let $\mathbf{e}$ be a vector of weight u on $\mathscr{N}$ and $t-u$ on $\mathscr{P}$. Let $\mathcal{C}$ and $\mathcal{C}_{\text{aux}}$ be $[n,k]$ and $[s,k_{\text{aux}}]$ linear codes respectively. Let us choose $(\mathbf{c}_{\text{aux}}, \mathbf{h})$ uniformly at random in

$$\widetilde{\mathscr{H}} = \{(\mathbf{h}, \mathbf{c}_{\text{aux}}) \in \mathcal{C}^{\perp} \times \mathcal{C}_{\text{aux}} \ : \ |\mathbf{h}_{\mathscr{N}}| = w \text{ and } |\mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}}| = t_{\text{aux}}\}.$$

Then for a proportion $1-o(1)$ *of codes* $\mathcal{C}_{\text{aux}}$ *and* $\mathcal{C}$ *we have that*

$$\operatorname*{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}(\langle \mathbf{c}_{\text{aux}}+\mathbf{h}_{\mathscr{P}},\mathbf{e}_{\mathscr{P}}\rangle+\langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle)=\delta(1+o(1)).$$

Proof. See Appendix §A . □

4. The double-RLPN Algorithm

We first going to explain the four main ingredients of the double-RLPN algorithm:

- computing suitable LPN samples,
- FFT decoding,
- recovering $\mathbf{e}_{\mathscr{P}}$,
- the bet ensuring that there are u errors on $\mathscr{N}$ at some point.

Let us detail each of these ingredients (or steps of the algorithm).

Computing the LPN Samples. First, our algorithm computes a certain number of LPN samples by computing a set $\mathscr{W}$ of elements of $\mathcal{C}^{\perp}$ of weight w on $\mathscr{N}$ by using a procedure `ParityCheckEquations`$(w,\mathscr{N},\mathcal{C})$ that uses low-weight codewords search techniques to produce a bunch of parity-check equations of $\mathcal{C}$ of weight w on $\mathscr{N}$. Then a random code $\mathcal{C}_{\text{aux}}$ is chosen in a family of codes over $\mathbb{F}_2^{|\mathscr{P}|}$ and dimension k_{aux} that we know how to decode efficiently at distance t_{aux}. For an element $\mathbf{h}$ in $\mathscr{W}$, each $\mathbf{h}_{\mathscr{P}}$ is decoded at distance t_{aux} to finally compute the set $\mathscr{H}$ containing pairs $(\mathbf{h},\mathbf{c}_{\text{aux}})$ in $\mathscr{W}\times\mathcal{C}_{\text{aux}}$ satisfying $|\mathbf{h}_{\mathscr{N}}|=w$ and $|\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\text{aux}}|=t_{\text{aux}}$. Algorithm 1 gives the pseudo-code of the procedure.

Algorithm 1 The function computing the LPN samples associated to $\mathscr{N}$

function LPN-Samples$(\mathcal{C},\mathscr{N})$
  $\mathscr{P}\leftarrow[\![1,n]\!]\setminus\mathscr{N}$
  $\mathscr{W}\leftarrow$ ParityCheckEquations$(w,\mathscr{N},\mathcal{C})$ ▷ returns a set of parity-check equations of $\mathcal{C}$ of weight w on $\mathscr{N}$
  $\mathcal{C}_{\text{aux}}\xleftarrow{\$}\mathscr{F}(\mathscr{P},k_{\text{aux}},t_{\text{aux}})$ ▷ returns a code $\mathcal{C}_{\text{aux}}$ in a family of codes $\mathscr{F}$ over $\mathbb{F}_2^{|\mathscr{P}|}$ and dimension k_{aux} that we know how to decode efficiently at distance t_{aux}
  $\mathscr{H}\leftarrow\emptyset$
  for all $\mathbf{h}\in\mathscr{H}$ **do**
    $\mathscr{H}\leftarrow\mathscr{H}\cup\{\mathbf{h}\}\times$ Decode$(\mathbf{h}_{\mathscr{P}},\mathcal{C}_{\text{aux}},t_{\text{aux}})$ ▷ Decode$(\mathbf{h}_{\mathscr{P}},\mathcal{C}_{\text{aux}},t_{\text{aux}})$ outputs a set of codewords of $\mathcal{C}_{\text{aux}}$ at distance t_{aux} of $\mathbf{h}_{\mathscr{P}}$
  end for
  $\mathbf{G}_{\text{aux}}\leftarrow$ generating matrix of $\mathcal{C}_{\text{aux}}$
return $(\mathscr{H},\mathbf{G}_{\text{aux}})$
end function

FFT Decoding. Computing $\mathscr{H}$ gives a number $|\mathscr{H}|$ of LPN samples, which from the interpretation given in Equation (5), leads us to think that the right choice $\mathbf{x}\in\mathbb{F}_2^{k_{\text{aux}}}$ for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ is the one for which

$$\operatorname*{bias}_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\xleftarrow{\$}\mathscr{H}}(\langle \mathbf{y},\mathbf{h}\rangle+\langle \mathbf{x},\mathbf{m}_{\text{aux}}\rangle)$$

would be given by Proposition 2. It should namely be of order δ which is defined in this proposition. Natural candidates for being equal to $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ are those for which this bias is say $\geqslant\delta/2$. This leads to compute all those biases. This can be done rather efficiently by factoring the common computations made for computing all those biases for $\mathbf{x}\in\mathbb{F}_2^{k_{\text{aux}}}$ by an FFT trick which is standard in the LPN context. It dates back in this context to [LF06], but it can be traced back to decoding the first-order Reed-Muller code (which is another way to view the decoding task in case of the LPN problem) which was already suggested in [Gre66]. The link between the bias of the

random variables we are interested in and the Fourier transform is based on the following simple observation that follows right away from the very definition of the Fourier transform. Before we give this observation, let us bring in a notation that will be helpful for describing it and which will be used throughout the paper from now on.

Notation 2. *For any* $\mathbf{y} \in \mathbb{F}_2^n$, $\mathscr{H} \subseteq \mathcal{C}^\perp \times \mathcal{C}_{\text{aux}}$ *and a generator matrix* $\mathbf{G}_{\text{aux}}$ *of* $\mathcal{C}_{\text{aux}}$ *we define the function* $f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}$ *on* $\mathbb{F}_2^{k_{\text{aux}}}$ *by*

$$\begin{aligned} f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}} : \mathbb{F}_2^{k_{\text{aux}}} &\to \mathbb{R} \\ \mathbf{u} &\mapsto \begin{cases} \sum_{\mathbf{h}:(\mathbf{h},\mathbf{u}\mathbf{G}_{\text{aux}})\in\mathscr{H}} (-1)^{\langle \mathbf{y},\mathbf{h}\rangle} & \text{if this sum is not empty,} \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{9}$$

With this notation at hand, the link between the biases and the Fourier transform of this function is given by the following lemma.

Lemma 1. *We have for any* $\mathbf{u} \in \mathbb{F}_2^{k_{\text{aux}}}$ *and any* $\mathbf{x} \in \mathbb{F}_2^s$ *such that* $\mathbf{x}\mathbf{G}_{\text{aux}}^\intercal = \mathbf{u}$

$$\begin{aligned} \widehat{f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}}(\mathbf{u}) &= |\mathscr{H}| \operatorname*{bias}_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\xleftarrow{\$}\mathscr{H}} (\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{u},\mathbf{m}_{\text{aux}}\rangle) \\ &= |\mathscr{H}| \operatorname*{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\mathscr{H}} (\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{c}_{\text{aux}}\rangle). \end{aligned}$$

Proof. We have the following computation,

$$\begin{aligned} \widehat{f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}}(\mathbf{u}) &= \sum_{\mathbf{v}\in\mathbb{F}_2^{k_{\text{aux}}}} (-1)^{\langle \mathbf{u},\mathbf{v}\rangle} f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}(\mathbf{v}) \\ &= \sum_{(\mathbf{h},\mathbf{v})\in\mathcal{C}^\perp\times\mathbb{F}_2^{k_{\text{aux}}}:(\mathbf{h},\mathbf{v}\mathbf{G}_{\text{aux}})\in\mathscr{H}} (-1)^{\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{u},\mathbf{v}\rangle} \qquad \text{(Equations (2) and (9))} \\ &= \sum_{(\mathbf{h},\mathbf{v})\in\mathcal{C}^\perp\times\mathbb{F}_2^{k_{\text{aux}}}:(\mathbf{h},\mathbf{v}\mathbf{G}_{\text{aux}})\in\mathscr{H}} (-1)^{\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x}\mathbf{G}_{\text{aux}}^\intercal,\mathbf{v}\rangle} \\ &= \sum_{(\mathbf{h},\mathbf{v})\in\mathcal{C}^\perp\times\mathbb{F}_2^{k_{\text{aux}}}:(\mathbf{h},\mathbf{v}\mathbf{G}_{\text{aux}})\in\mathscr{H}} (-1)^{\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{v}\mathbf{G}_{\text{aux}}\rangle} \\ &= \sum_{(\mathbf{h},\mathbf{c}_{\text{aux}})\in\mathscr{H}} (-1)^{\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{c}_{\text{aux}}\rangle} \end{aligned}$$

which concludes the proof by definition of the bias. □

Remark 2. *The probabilistic notation hides the fact that computing all these Fourier coefficients and taking the maximum of them allows to decode in a certain code. Indeed let,*

$$\mathcal{D} \stackrel{def}{=} \left\{ (\langle \mathbf{u},\mathbf{m}_{\text{aux}}\rangle)_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\in\mathscr{H}} : \mathbf{u} \in \mathbb{F}_2^{k_{\text{aux}}} \right\}$$

which is under very mild assumptions a linear code of dimension k_{aux} *and length* $|\mathscr{H}|$*. If we let* $c(\mathbf{u}) \stackrel{def}{=} (\langle \mathbf{u},\mathbf{m}_{\text{aux}}\rangle)_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\in\mathscr{H}}$ *be the codeword associated to* $\mathbf{u}$ *and* $\mathbf{v} = (\langle \mathbf{y},\mathbf{h}\rangle)_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\in\mathscr{H}}$ *then since*

$$|\mathscr{H}| \operatorname*{bias}_{(\mathbf{h},\mathbf{m}_{\text{aux}}\mathbf{G}_{\text{aux}})\xleftarrow{\$}\mathscr{H}} (\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{u},\mathbf{m}_{\text{aux}}\rangle) = |\mathscr{H}| - 2|\mathbf{v} + c(\mathbf{u})|,$$

it follows from Lemma 1 that $c(\mathbf{u}_0)$ *is the codeword of* $\mathcal{D}$ *which is the closest to* $\mathbf{v}$*, where* $\mathbf{u}_0 = \arg\max \widehat{f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}}(\mathbf{u})$*. Therefore, vector* $\mathbf{u}_0$ *is here a likely candidate for being equal to* $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^\intercal$ *when* $\mathscr{H}$ *is big enough.*

We give the pseudo-code of the FFT decoding algorithm producing a list $\mathscr{S}$ of putative candidates for being equal to $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^\intercal$ in Algorithm 2.

The point of using the FFT for computing all these biases is that its complexity is of order $\mathcal{O}\big(k_{\text{aux}}2^{k_{\text{aux}}}F\big)$ where F is the complexity of computing $f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}$ which can be bounded by

Algorithm 2 FFT algorithm producing a list of candidates for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$

Input: $\mathscr{H}$, $\mathbf{G}_{\text{aux}}$
Output: $\mathscr{S}$ a list of candidates for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$

1: **function** FFT-DECODE($\mathscr{H}$, $\mathbf{G}_{\text{aux}}$)
2: $\quad \widehat{f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}} \leftarrow \text{FFT}(f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}})$
3: $\quad \mathscr{S} \leftarrow \left\{\mathbf{u} \in \mathbb{F}_2^{k_{\text{aux}}} \ : \widehat{f_{\mathbf{y},\mathscr{H},\mathbf{G}_{\text{aux}}}}(\mathbf{u}) > \frac{\delta}{2}\,|\mathscr{H}|\right\}$ $\quad \triangleright\ \delta \stackrel{\text{def}}{=} \frac{K_w^{(n-s)}(u)K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}$
4: $\quad$ **return** $\mathscr{S}$
5: **end function**

$\mathcal{O}\left(\max\left(1, \frac{|\mathscr{H}|}{2^{k_{\text{aux}}}}\right)\right)$. On the other hand, if we had computed directly all those biases we would have a much bigger complexity of $\mathcal{O}\left(|\mathscr{H}|\,2^{k_{\text{aux}}}\right)$ because $\mathscr{H}$ is of exponential size for the problem at hand.

Recovering $\mathbf{e}_{\mathscr{P}}$ and then $\mathbf{e}$. If we have a candidate $\mathbf{s}$ for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$, then since we expect $|\mathbf{e}_{\mathscr{P}}| = t-u$, recovering $\mathbf{e}_{\mathscr{P}}$ from the equality $\mathbf{s} = \mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ is nothing but solving a decoding problem, namely to decode $t-u$ errors in the code of parity-check matrix $\mathbf{G}_{\text{aux}}$, *i.e.* $\mathcal{C}_{\text{aux}}^{\perp}$. In other words, we have to solve $\mathsf{DP}(s, s-k_{\text{aux}}, t-u)$. This approach can be generalized by taking N_{aux} different sets of LPN samples associated respectively to the codes $\mathcal{C}_{\text{aux}}^{(1)}, \cdots, \mathcal{C}_{\text{aux}}^{(N_{\text{aux}})}$. For i in $[\![1, N_{\text{aux}}]\!]$, let $\mathbf{G}_{\text{aux}}^{(i)}$ be the generating matrix which is chosen for $\mathcal{C}_{\text{aux}}^{(i)}$. Then each of these sets of LPN samples brings candidates for $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$. By choosing an N_{aux}-tuple of candidates $(\mathbf{s}^{(1)}, \cdots, \mathbf{s}^{(N_{\text{aux}})})$, where $\mathbf{s}^{(i)}$ is a candidate for $\mathbf{G}_{\text{aux}}^{(i)}\mathbf{e}_{\mathscr{P}}^{\intercal}$ (we have taken the transpose to have a more readable form) given by the i-th LPN samples set, we get to solve the set of simultaneous equations

$$(\mathbf{s}^{(1)})^{\intercal} = \mathbf{G}_{\text{aux}}^{(1)}\mathbf{e}_{\mathscr{P}}^{\intercal}, \cdots, \ (\mathbf{s}^{(N_{\text{aux}})})^{\intercal} = \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})}\mathbf{e}_{\mathscr{P}}^{\intercal}$$

with the constraint $|\mathbf{e}_{\mathscr{P}}| = t-u$. In other words if we set

$$\mathbf{H}^{\intercal} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbf{G}_{\text{aux}}^{(1)\,\intercal} & \cdots & \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})\intercal} \end{pmatrix} \quad \text{and} \quad \mathbf{s} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbf{s}^{(1)} & \cdots & \mathbf{s}^{(N_{\text{aux}})} \end{pmatrix}$$

then we have to solve the decoding problem $\mathbf{H}\mathbf{e}_{\mathscr{P}}^{\intercal} = \mathbf{s}^{\intercal}$ with $|\mathbf{e}_{\mathscr{P}}| = t-u$, in other words we have to solve $\mathsf{DP}\,(s, s-N_{\text{aux}}k_{\text{aux}}, t-u)$. We are going to choose a simple ISD algorithm to solve this problem, namely Dumer's algorithm [Dum89] which is a good compromise between efficiency and simple formula for its complexity. We denote by DECODE-DUMER$(\mathbf{H}, \mathbf{s}, t)$ the call to Dumer's algorithm to decode the syndrome $\mathbf{s}$ of an error of weight t associated to the parity-check matrix $\mathbf{H}$. We assume here that this call produces *all* solutions to this decoding problem.

Once we have recovered $\mathbf{e}_{\mathscr{P}}$, say we know that it is equal to some $\mathbf{v}$ of weight $t-u$ in $\mathbb{F}_2^s$, we face a much simpler problem. We namely have to solve the problem

$$\mathbf{y} = \mathbf{c} + \mathbf{e},\ \mathbf{c} \in \mathcal{C},\ \mathbf{e}_{\mathscr{P}} = \mathbf{v},\ |\mathbf{e}_{\mathscr{N}}| = u.$$

This is nothing but $\mathsf{DP}(n-s, k-s, u)$ which is much simpler. Here we might just use algorithm DECODE-DUMER on it. Let us call SOLVE-SUBPROBLEM$(\mathcal{C}, \mathscr{N}, \mathbf{y}, \mathbf{v}, u)$ the routine which performs this task and which returns a candidate for $\mathbf{e}_{\mathscr{N}}$ and returns $\perp$ otherwise. If this problem has no solution we have of course a false candidate for $\mathbf{e}_{\mathscr{P}}$ and if we have a solution, then we have solved our decoding problem. To verify that we have indeed such a decoding problem, suppose without loss of generality that $\mathscr{P} = [\![1, s]\!]$ and $\mathscr{N} = [\![s+1, n]\!]$. We can also assume that $\mathcal{C}_{\mathscr{P}}$ is of full rank dimension s (this holds with overwhelming probability). We can compute $\mathbf{G}$ a generator matrix of $\mathcal{C}$ of the form $\mathbf{G} = \begin{pmatrix} \mathbf{Id}_s & \mathbf{R} \\ \mathbf{0}_{k-s} & \mathbf{R}' \end{pmatrix}$ by applying partial Gaussian elimination on a generator matrix of $\mathcal{C}$. Then SOLVE-SUBPROBLEM$(\mathcal{C}, \mathscr{N}, \mathbf{y}, \mathbf{x}, u)$ decodes at distance u the word $\mathbf{y}' \stackrel{\text{def}}{=} \mathbf{y}_{\mathscr{N}} - (\mathbf{y}_{\mathscr{P}} - \mathbf{x})\mathbf{R}$ onto the code $\mathcal{C}^{\mathscr{N}}$ of generator matrix $\mathbf{R}'$.

With this notation at hand, the pseudo-code describing the algorithm for recovering $\mathbf{e}_{\mathscr{P}}$ and then returning $\mathbf{e}$ if a suitable solution is found, is given in Algorithm 3.

Algorithm 3 algorithm recovering $\mathbf{e}_{\mathscr{P}}$ and then $\mathbf{e}$

Input: $\mathscr{S}^{(1)}, \cdots, \mathscr{S}^{(N_{\text{aux}})} \subset \mathbb{F}_2^{k_{\text{aux}}}$, $\mathbf{G}_{\text{aux}}^{(1)}, \cdots, \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})} \in \mathbb{F}_2^{k_{\text{aux}} \times s}$

function RECOVER-$\mathbf{e}(\mathscr{S}^{(1)}, \cdots, \mathscr{S}^{(N_{\text{aux}})}, \mathbf{G}_{\text{aux}}^{(1)}, \cdots, \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})})$
  $\mathbf{H}^\intercal \leftarrow \left(\mathbf{G}_{\text{aux}}^{(1)\,\intercal} \quad \cdots \quad \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})\intercal}\right)$
  for $\left(\mathbf{s}^{(1)}, ..., \mathbf{s}^{(N_{\text{aux}})}\right) \in \prod_{j=1}^{N_{\text{aux}}} \mathcal{S}^{(j)}$ **do**
    $\mathbf{s} \leftarrow \left(\mathbf{s}^{(1)} \quad \ldots \quad \mathbf{s}^{(N_{\text{aux}})}\right)$
    for all $\mathbf{v} \in$ DECODE-DUMER$(\mathbf{H}, \mathbf{s}, t)$ **do**
      $\mathbf{e}' \leftarrow$ SOLVE-SUBPROBLEM$(\mathcal{C}, \mathscr{N}, \mathbf{y}, \mathbf{v}, u)$
      if $\mathbf{e}' \neq \perp$ **then**
        return $\mathbf{e}$ such that $\mathbf{e}_{\mathscr{P}} = \mathbf{x}$ and $\mathbf{e}_{\mathscr{N}} = \mathbf{e}'$
      end if
    end for
  end for
end function

Testing Enough Candidates $\mathscr{N}$. Now, it may also happen that when choosing $\mathscr{N}$, we might not have that $|\mathbf{e}_{\mathscr{N}}| = u$. For this, we have to check enough candidates. The probability that a set $\mathscr{N}$ of size $n - s$ satisfies this property is given by

$$P_{\text{succ}} \stackrel{\text{def}}{=} \frac{\binom{t}{u}\binom{n-t}{n-u-s}}{\binom{n}{n-s}}.$$

Performing a number N_{iter} of trials for $\mathscr{N}$ which is of order $\Theta\left(1/P_{\text{succ}}\right)$ will succeed with constant probability. Putting all these ingredients together leads to the whole double-RLPN algorithm given in Algorithm 4.

Algorithm 4 double-RLPN decoder

Input: $\mathbf{y}$, t, $\mathcal{C}$ an $[n, k]$-code

Parameters: $s, u, k_{\text{aux}}, t_{\text{aux}}, N, \left(\mathcal{C}_{\text{aux}}^{(j)}\right)_{j \in \mathcal{F}}$

Output: $\mathbf{e}$ such that $|\mathbf{e}| = t$ and $\mathbf{y} - \mathbf{e} \in \mathcal{C}$.

function double-RLPN$(\mathbf{y}, \mathcal{C}, t)$
  for i from 1 to N_{iter} **do** ▷ N_{iter} such that w.o.p one iteration is s.t $|\mathbf{e}_{\mathscr{N}}| = u$
    $\mathscr{N} \xleftarrow{\$} \{\mathscr{I} \subseteq [\![1, n]\!] \ : \ |\mathscr{I}| = n - s\}$ ▷ Hope that $|\mathbf{e}_{\mathscr{N}}| = u$
    for $j = 1, \ldots, N_{\text{aux}}$ **do**
      $(\mathscr{H}^{(j)}, \mathbf{G}_{\text{aux}}^{(j)}) \leftarrow$ LPN-SAMPLES$(\mathcal{C}, \mathscr{N})$
      $\mathcal{S}^{(j)} \leftarrow$ FFT-DECODE$(\mathscr{H}^{(j)}, \mathbf{G}_{\text{aux}}^{(j)})$
    end for
    RECOVER-$\mathbf{e}(\mathscr{S}^{(1)}, \cdots, \mathscr{S}^{(N_{\text{aux}})}, \mathbf{G}_{\text{aux}}^{(1)}, \cdots, \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})})$
  end for
end function

Complexity of the Algorithm. It is sufficient to take $N_{\text{aux}} = \mathcal{O}(1)$ for the parameters we are interested in which will correspond to a choice of k_{aux} of the form $k_{\text{aux}} = \Omega(s)$. With this choice we immediately get the following complexity for the double-RLPN algorithm

Proposition 3. *The complexity C of the* double-RLPN *algorithm is given by*

$$\begin{aligned} C &= \widetilde{\mathcal{O}}\left(\frac{1}{P_{\text{succ}}}\left(T_{\text{eq}} + NT_{\text{dec}} + k_{\text{aux}}\max\left(2^{k_{\text{aux}}}, |\mathscr{H}|\right) + S^{N_{\text{aux}}}T_{\text{ISD}}\right)\right) \quad \textit{where} \\ P_{\text{succ}} &= \frac{\binom{t}{u}\binom{n-t}{n-u-s}}{\binom{n}{n-s}} \\ T_{\text{ISD}} &= T_{\text{Dumer}}(s, s - N_{\text{aux}}k_{\text{aux}}, t-u) + N_{\text{ISD}}T_{\text{Dumer}}(n-s, k-s, u) \end{aligned}$$

and T_{eq} is the time complexity of ParityCheckEquations, *N is the number of parity-check equations produced by this procedure, T_{dec} is the complexity of decoding $\mathcal{C}_{\text{aux}}$,* i.e. *it is the complexity of a call to* Decode(), *S is the size of a list output by* FFT-Decode(), *N_{ISD} is the number of solutions to the $(s, s-N_{\text{aux}}k_{\text{aux}}, t-u)$ decoding problem and $T_{\text{Dumer}}(n,k,t)$ stands for the complexity of solving the (n,k,t) decoding problem with Dumer's algorithm when we want to find all solutions to the problem.*

The asymptotic complexity formula for the double-RLPN algorithm, including also the constraints required on our parameters, is given in Appendix B Proposition 9 which was used to generate Figure 1.

5. Estimating the Number of False Candidates

The goal of this section is to introduce the main tool necessary to make a rigorous analysis of Algorithm 4 and to give a formula for the number of false candidates which is proved by making a certain conjecture whose validity has then been verified experimentally.

5.1. **Main Duality Tool.** The fundamental quantity when analyzing dual attacks is the bias of $\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{x}, \mathbf{c}_{\text{aux}}\rangle$ which tells us whether $\mathbf{x}\mathbf{G}_{\text{aux}}^{\intercal}$ has to be put in the list $\mathscr{S}$ of candidates output by Algorithm 2. While initially standard independence assumptions were made to analyze its distribution [CDMT22, Ass. 3.7] (which are very similar to analyze dual attacks in lattice based cryptography), recently [MT23] showed that these assumptions were erroneous and, gave for the first time a dual expression [MT23, Prop 1.] for this quantity which seems a key step to understand its behavior and gave with an additional assumption a rigorous analysis of the RLPN dual attack. The proposition given there to estimate the number of false candidates turns out to match accurately the experiments. The following proposition is a generalization of [MT23, Prop 1.] and gives a dual expression for the aforementioned bias.

Proposition 4. *Let $\mathscr{P}$ and $\mathscr{N}$ be two complementary subsets of $[\![1,n]\!]$ of size s and $n-s$ respectively. Let $\mathcal{C}$ be an $[n,k]$-code such that $\mathcal{C}_{\mathscr{P}}$ is of dimension s and let $\mathcal{C}_{\text{aux}}$ be an $[s, k_{\text{aux}}]$-code. We have for any $\mathbf{x} \in \mathbb{F}_2^s$*

$$\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{x}, \mathbf{c}_{\text{aux}}\rangle\right) = \frac{1}{2^{k-k_{\text{aux}}}}\frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{i=0}^{n-s}\sum_{j=0}^{s} N_{i,j}K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j) \tag{10}$$

where

$$\begin{aligned} N_{i,j} &\overset{def}{=} \left|\left\{\left(\mathbf{r}, \mathbf{c}^{\mathscr{N}}\right) \in \left(\mathbf{x} + \mathcal{C}_{\text{aux}}^{\perp}\right) \times \mathcal{C}^{\mathscr{N}} \,:\, |\mathbf{r}| = j \text{ and } \left|\left(\mathbf{r} + \mathbf{e}_{\mathscr{P}}\right)\mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathbf{c}^{\mathscr{N}}\right| = i\right\}\right|, \\ \widetilde{\mathscr{H}} &= \left\{(\mathbf{h}, \mathbf{c}_{\text{aux}}) \in \mathcal{C}^{\perp} \times \mathcal{C}_{\text{aux}} \,:\, |\mathbf{h}_{\mathscr{N}}| = w \text{ and } |\mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}}| = t_{\text{aux}}\right\} \end{aligned}$$

and where $\mathbf{R} \in \mathbb{F}_2^{s\times(n-s)}$ is such that for any $\mathbf{h} \in \mathcal{C}^{\perp}$ we have $\mathbf{h}_{\mathscr{P}} = \mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}$.

Proof. This proposition is proved in Appendix C. □

5.2. **Intuition on How this Formula Allows to Estimate $|\mathscr{S}|$.** As a preliminary remark, notice that $\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{x}, \mathbf{c}_{\text{aux}}\rangle\right)$ is the same for all $\mathbf{x}$ belonging to a same coset of

$\mathcal{C}_{\text{aux}}^{\perp}$ and therefore only possibly allows to distinguish the values $\mathbf{x}\mathbf{G}_{\text{aux}}^{\intercal}$. Second, observe that the expected value of $\left|\widetilde{\mathscr{H}}\right|$ is $\frac{\binom{n-s}{w}}{2^{k-s}}\frac{\binom{s}{t_{\text{aux}}}}{2^{s-k_{\text{aux}}}}$ so that we expect

$$\frac{1}{2^{k-k_{\text{aux}}}\left|\widetilde{\mathscr{H}}\right|} \approx \frac{1}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.$$

Third, observe that Proposition 2 means in essence that the bias corresponding to $\mathbf{e}_{\mathscr{P}}$, namely $\text{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}(\langle\mathbf{y},\mathbf{h}\rangle + \langle\mathbf{e}_{\mathscr{P}},\mathbf{c}_{\text{aux}}\rangle)$ should be $\approx \frac{K_w^{(n-s)}(u)K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}$, *i.e.* it corresponds roughly to the "first" pair (i,j) (where we range the values according to the product $K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)$) for which $N_{i,j}\neq 0$, namely $(i,j)=(u,t-u)$ where the pair $(\mathbf{e}_{\mathscr{P}},\mathbf{0})$ is likely to be the only pair $(\mathbf{r},\mathbf{c}^{\mathscr{N}})$ in $(\mathbf{e}_{\mathscr{P}}+\mathcal{C}_{\text{aux}}^{\perp})\times\mathcal{C}^{\mathscr{N}}$ such that $|\mathbf{r}|=t-u$ and $\left|(\mathbf{r}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathbf{c}^{\mathscr{N}}\right|=u$ (and therefore we likely have $N_{u,t-u}=1$). Therefore the behavior of the sum appearing in (10) is dominated by this first term $N_{i,j}$ which is non zero, namely $(i,j)=(u,t-u)$ since we really have in this case that the corresponding term in the sum is nothing but

$$\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.$$

This kind of phenomenon appears to be much more general than this: the $\mathbf{x}\in\mathbb{F}_2^s$ which give a high bias (and are therefore the ones we put in $\mathscr{S}$) are those for which there is an $N_{i,j}$ which is unexpectedly non zero (and therefore most likely equal to 1) in the low values of (i,j) for which the term $K_w^{n-s}(i)\,K_{t_{\text{aux}}}^{(s)}(j)$ can compete or even supersede the term dominating in the expression (10) of the bias of $\mathbf{e}_{\mathscr{P}}$, namely $K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)$ (we have ignored the common denominator $2^{k-k_{\text{aux}}}\left|\widetilde{\mathscr{H}}\right|$ appearing in both sums). Similarly we expect that the bias of those $\mathbf{x}$ is of order in this case

$$\frac{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.$$

This intuition is formalized by Conjecture 1 what we make later on.

5.3. **Main Proposition.** The key step of the analysis is to estimate the number of candidates, namely the size of $\mathscr{S}$ (Instruction 3 of Algorithm 4). Provided that the bet ($|\mathbf{e}_{\mathscr{N}}|=u$) on the error is valid we expect that the secret vector $\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}$ belongs to $\mathscr{S}$. But, as we will show in this section this set also contains some false positives, namely any element of $\mathscr{S}\setminus\{\mathbf{e}_{\mathscr{P}}\mathbf{G}_{\text{aux}}^{\intercal}\}$. Testing if an element of $\mathscr{S}$ is a false positive (Algorithm 3) will be of exponential cost. Estimating their number is therefore crucial to predict the complexity of our algorithm. The following proposition bounds the expected number of candidates in a typical iteration of Algorithm 4.

Proposition 5. *Using Distribution 1 for $\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{e}$ and $\mathbf{y}$ and given that our parameters verify Parameter Constraint 1, that the number of computed* LPN *samples is the total number of available* LPN *samples,* i.e. *$\mathscr{H}=\widetilde{\mathscr{H}}$ and under Conjecture 1 we have that the expected number of candidates per iteration is bounded by*

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(|\mathscr{S}|)=\widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}}\frac{\binom{s}{j}\binom{n-s}{i}}{2^{n-k}}\right)+1 \tag{11}$$

where

$$\mathcal{A}\overset{def}{=}\left\{(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!],\ \left|\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right|\leqslant n^{3.2}\right\}. \tag{12}$$

The set $\mathscr{S}$ of candidates is defined by

$$\mathscr{S}\overset{def}{=}\left\{\mathbf{s}\in\mathbb{F}_2^{k_{\text{aux}}}\ :\widehat{f_{\mathbf{y},\widetilde{\mathscr{H}},\mathbf{G}_{\text{aux}}}}(\mathbf{s})\geqslant\frac{\delta}{2}\,\widetilde{H}\right\}, \tag{13}$$

where

$$\widetilde{H} \stackrel{def}{=} \frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} \qquad \text{and} \qquad \delta \stackrel{def}{=} \frac{K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}. \tag{14}$$

Remark 3. *The additional constraint that $\mathscr{H} = \widetilde{\mathscr{H}}$ is only here to simplify the proof. One could make a similar proposition without this constraint. In our instantiation of Algorithm 4 and with our optimal parameters this constraint is de-facto verified. Note also that $\widetilde{H}$ appearing in the expression of the threshold is the expected number of available* LPN *samples, namely $\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(\left|\widetilde{\mathscr{H}}\right|\right)$.*

Distribution 1.

- *$\mathscr{P}$ and $\mathscr{N}$ are two fixed complementary subsets of $[\![1,n]\!]$ of size s and $n-s$ respectively.*
- *The code $\mathcal{C}$ of generator matrix $\mathbf{G}$ is chosen uniformly at random among $[n,k]$ linear codes which are such that $\mathcal{C}_{\mathscr{P}}$ is of dimension s.*
- *The code $\mathcal{C}_{\text{aux}}$ of generator matrix $\mathbf{G}_{\text{aux}} \in \mathbb{F}_2^{k_{\text{aux}}\times s}$ is chosen uniformly at random among the $[s,k_{\text{aux}}]$-codes.*
- *$\mathbf{e} \in \mathbb{F}_2^n$ is a fixed vector of $\mathcal{S}_t^n$, $\mathbf{c} \in \mathcal{C}$ is a random codeword of $\mathcal{C}$ and we define $\mathbf{y} \stackrel{def}{=} \mathbf{c}+\mathbf{e}$.*

Correctness of our algorithm is ensured by the following constraints.

Parameter Constraint 1. *We suppose that the parameters $n,k,t,s,k_{\text{aux}},t_{\text{aux}},w,u$ are such that there exists a constant $\alpha>0$ that is such that*

$$(i)\ \frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} = \omega\left(\frac{n^{\alpha+8}}{\delta^2}\right),\ (ii)\ \frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k}} = \mathcal{O}(n^{\alpha}),\ (iii)\ \frac{\binom{s}{t_{\text{aux}}}}{2^{s-k_{\text{aux}}}} = \mathcal{O}(n^{\alpha}). \tag{15}$$

where,

$$\delta \stackrel{def}{=} \frac{K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.$$

Remark 4. *Note that these constraints are in fact, up to a polynomial factor, the minimal constraints required for our algorithm to work. Indeed, there are precisely the constraints required in Proposition 2 which estimates the bias of the error of the* LPN *samples (5).*

The difficulty of proving Proposition 5 is similar to the difficulties encountered in analyzing the RLPN algorithm in [MT23], we know too little about the tails of the distribution of $N_{i,j}$. As such, we will make the following conjecture which formalizes the discussion in §5.2.

Conjecture 1. *Using Distribution 1, under Parameter Constraint 1,*

$$\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j)\, K_w^{(n-s)}(i)\, N_{i,j} \geqslant \frac{1}{2} K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)\right) = \widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}} \mathbb{P}\left(N_{i,j}\neq 0\right) + 2^{-n}\right)$$

where $\mathcal{A}$ is given in Equation (12) and $\mathbf{x}$ is taken uniformly at random in $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^{\perp} + \mathbf{e}_{\mathscr{P}}\}$.

Conjecture 1 is discussed in the following section where we give experimental evidences that our analysis holds. In Appendix F.1 we show that this conjecture is in fact a consequence of a more minimalistic conjecture.

6. Experimental Evidence for Our Analysis

The goal of this section is to provide experimental evidence supporting Proposition 5. We will propose a convenient probabilistic model for the $N_{i,j}$'s and show that this model does not change the output distribution of our algorithm. We will essentially use the same model as in [MT23,

Appendix D] and model the weight distribution of the coset of a random linear code as a Poisson distribution of the right expected value. Recall that $N_{i,j}$ can be written as

$$N_{i,j} = \sum_{u=0}^{N_j\left(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)} N_i\left(\left(\mathbf{r}^{(u)}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\right)$$

where $\mathbf{R} \in \mathbb{F}_2^{s\times(n-s)}$ is such that for any $\mathbf{h} \in \mathcal{C}^{\perp}$ we have $\mathbf{h}_{\mathscr{P}} = \mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}$, $\mathbf{r}^{(u)}$ is the u'th codeword of weight j of $\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}$ and $N_j(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x})$ counts the number of elements in $\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}$ of Hamming weight j. With our model, we first draw $N_j\left(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)$ according to a Poisson distribution of expected value $\frac{\binom{s}{j}}{2^{k_{\text{aux}}}}$ and then we draw each $N_i\left(\left(\mathbf{r}^{(u)}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\right)$ according to independent Poisson distributions of expected values $\frac{\binom{n-s}{i}}{2^{n-k}}$ (see appendix E, Lemma 9 where we compute $\mathbb{E}\left(N_j\left(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\right)$ and $\mathbb{E}\left(N_i\left(\left(\mathbf{r}^{(u)}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\right)\right)$ under Distribution 1). Finally, we get the following model for $N_{i,j}$ by using the fact that the sum of independent Poisson random variables is a Poisson random variable:

Model 1 (Poisson Model)**.** *Under Distribution 1 and when* $\mathbf{x}$ *is taken uniformly at random in* $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$ *we make the model that*

$$N_{i,j} \sim \text{Poisson}\left(N_j\,\frac{\binom{n-s}{i}}{2^{n-k}}\right),\ \textit{where}\ N_j \sim \text{Poisson}\left(\frac{\binom{s}{j}}{2^{k_{\text{aux}}}}\right).$$

Under Poisson Model 1, the following proposition proves Conjecture 1 and thus it shows that Proposition 5 holds.

Proposition 6. *Under the Poisson Model 1, Conjecture 1 holds.*

Proof. The proof is given Appendix F. □

In Figure 2 we computed the expected number of $\mathbf{x}$'s whose bias multiplied by $\left|\widetilde{H}\right|$ is bigger than some prescribed quantity T according to

- the standard independence model in dual attacks where the $\langle \mathbf{e}, \mathbf{h}\rangle$'s are supposed to be independent,
- some experiments,
- the case were we replace the right-hand term of $N_{i,j}$ (given in Equation (10)) by their Poisson model.

As it is shown by Figure 2, the Poisson model matches remarkably well with the experiments. This shows, as was the case in the analysis [MT23] of the RLPN algorithm, that the Poisson model allows to predict accurately the size of $\mathscr{S}$.

7. Instantiating the Auxiliary Code $\mathcal{C}_{\text{aux}}$ with an Efficient Decoder

In double-RLPN we need to choose an auxiliary code $\mathcal{C}_{\text{aux}}$ which is efficiently list-decodable (Definition 6) at the smallest as possible distance $t_{\text{aux}} = d_{\text{GV}}(s, k_{\text{aux}})$. We propose to use the following product of small random codes (other choices may be more suitable but they are harder to analyze, like polar codes [Arı09, KU10, Şaş11, TV12]),

$$\mathcal{C}_{\text{aux}} \stackrel{\text{def}}{=} \mathcal{C}_1 \times \cdots \times \mathcal{C}_b$$

where the $\mathcal{C}_i$'s are random $\left[\frac{s}{b}, \frac{k_{\text{aux}}}{b}\right]$-codes. Notice that

$$\mathcal{D}\text{ec}(\mathbf{z}) \stackrel{\text{def}}{=} \{\mathbf{c}_{\text{aux}} \in \mathcal{C}_{\text{aux}} \ :\ |\mathbf{c}_{\text{aux}}+\mathbf{z}| = t_{\text{aux}}\}$$

does not look exactly like how it should with a random code for which our analysis given in Propositions 2 and 5 hold. Furthermore, we will compute

$$\mathscr{H} \subseteq \left\{(\mathbf{h}, \mathbf{c}_{\text{aux}}) \in \mathcal{C}^{\perp} \times \mathcal{C}_{\text{aux}} \ :\ \forall i \in [\![1, b]\!],\ |\mathbf{h}_{\mathscr{N}}(i)| = \tfrac{w}{b} \text{ and } |\mathbf{h}_{\mathscr{P}}(i) + \mathbf{c}_i| = \tfrac{t_{\text{aux}}}{b}\right\}$$

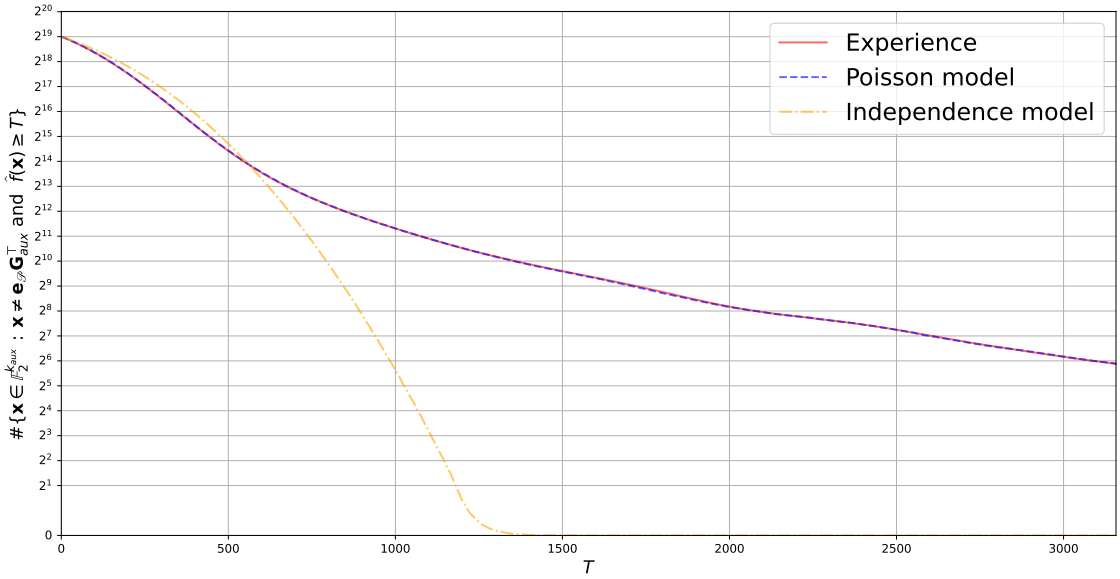

FIGURE 2. Size of the set $\{\mathbf{x} \in \mathbb{F}_2^{k_{\text{aux}}} \setminus \{\mathbf{e}_{\mathscr{D}}\mathbf{G}_{\text{aux}}\} \ : \widehat{f_{\mathbf{y},\mathscr{H}}}(\mathbf{x}) \geqslant T\}$ as a function of T when $[w, t_{\text{aux}}, k_{\text{aux}}, s, k, n, u, t] = [5, 2, 20, 28, 30, 60, 8, 8]$, number of LPN samples $N = 65536$. Here the curve "Independence model" has been replaced when modelling the $\langle \mathbf{y}, \mathbf{h} \rangle$'s by i.i.d Bernouilli random variables of parameter $\frac{1}{2}$ (standard independence model in dual attacks).

in Instruction 1 of Algorithm 1. To this aim we will perform exhausting search on the random codes. By choosing the number b of blocs as,

$$b = \Theta(\log n) \tag{16}$$

the above decoding algorithm costs for any parity-check equation $O\left(2^{n/\log n}\right)$ (recall that $t_{\text{aux}} \approx d_{\text{GV}}(n,k)$). Therefore, as Algorithm 1 running time is exponential (in n) for our considered parameters, it won't affect it. Furthermore, there are false candidates when computing $\mathscr{H}$ and it is crucial to estimate their numbers.

Our analysis of Sections 3 and 5 has been made in the idealized-model where $\mathcal{C}_{\text{aux}}$ is a random code equipped with genie aided decoders. But, by choosing b as in Equation (16), analysis of Propositions 2 and 5 is still verified with our particular choice of $\mathcal{C}_{\text{aux}}$ (up to negligible factors) as justified in Appendix G.

8. Links with Dual Attacks in Lattice Based Cryptography

The purpose of this section is to give more details about the close connection between dual attacks in coding theory (*a.k.a* "statistical decoding" after the pioneering work of [Jab01]) and dual attacks in lattice based cryptography. Basically, with some slight differences highlighted in [PS23, App. A], the lattice based analogue of the dual attack presented here is the slight improvement [CST22] of the Matzov attack [MAT22]. The improvement in [CST22] is based on the fact that the modulus switching technique used in [MAT22] can be viewed as a suboptimal source distortion code for the Euclidean metric which can be replaced by an almost optimal polar code. The approach followed here should carry over to this lattice setting as well and in particular, the fundamental duality Proposition 4. Let us just observe now that a simple duality equality (together with a gross approximation based on the considerations of §5.2) can be used to explain the results observed in [DP23b, Fig. 3]. It was shown there that predictions of the score function based on standard independence assumptions made for dual attacks in lattice based cryptography seem to be off in some parameter region (what can be called the "error-floor" region due to its

similarity with the Low-Density-Parity-Check codes literature). To explain this point, we will use the same notation as in [DP23b] and will not redefine the quantities appearing here.

Let us first observe that an immediate corollary of Proposition 4 is

Corollary 1. *Consider an $[n,k]$ linear code $\mathcal{C}$ and consider some word $\mathbf{y}=\mathbf{c}+\mathbf{e}\in\mathbb{F}_2^n$ where $\mathbf{c}$ is in $\mathcal{C}$. Let $\mathscr{W}$ be the set of codewords of weight w in $\mathcal{C}^\perp$ and let $f_{\mathscr{W}}(\mathbf{y})\stackrel{def}{=}\sum_{\mathbf{w}\in\mathscr{W}}(-1)^{\langle\mathbf{y},\mathbf{w}\rangle}$. We have*

$$f_{\mathscr{W}}(\mathbf{y})=\frac{1}{2^k}\sum_{i=0}^{n}N_iK_w^n(i)$$

where N_i is the number of words of weight i in $\mathcal{C}+\mathbf{e}$.

It is insightful to view these Krawtchouk polynomials as the Fourier transform of the indicator function of a Hamming sphere, see Fact 1. Similarly, the lattice based analogue of Corollary 1 involving the lattice based analogue of $f_{\mathscr{W}}$, which is called the score function in [DP23b] will involve the Bessel function of the first kind (see for instance [DDRT23, Fact 4.9]). We namely obtain

Proposition 7. *Consider a lattice $\Lambda\subseteq\mathbb{R}^n$ and consider some word $\mathbf{y}=\mathbf{x}+\mathbf{e}\in\mathbb{R}^n$ where $\mathbf{x}$ is in Λ. Let $\widetilde{\mathscr{W}}$ be the set of dual lattice vectors of Euclidean weights in $(w-\varepsilon,w+\varepsilon)$ in $\Lambda^\vee$ and let $f_{\widetilde{\mathscr{W}}}(\mathbf{y})\stackrel{def}{=}\sum_{\mathbf{w}\in\widetilde{\mathscr{W}}}\cos(2\pi\langle\mathbf{x},\mathbf{y}\rangle)$. We have*

$$f_{\widetilde{\mathscr{W}}}(\mathbf{y})=\frac{1}{|\Lambda^\vee|}\sum_{j\geqslant 0}\frac{N_j}{j^n\,(2\pi)^{n/2}}\Big((2\pi(w+\varepsilon)j)^{n/2}J_{n/2}(2\pi(w+\varepsilon)j)\\ -(2\pi(w-\varepsilon)j)^{n/2}J_{n/2}(2\pi(w-\varepsilon)j)\Big)\tag{17}$$

where N_j is the number of words of Euclidean norm j in $\Lambda+\mathbf{e}$ and J_ν is the Bessel function of the first kind of order[1] *ν.*

The proof is given in Appendix H. Let us take some subset $\mathscr{W}$ of $\widetilde{\mathscr{W}}$ of size N say. We make the approximation $f_{\mathscr{W}}(\mathbf{y})\approx\frac{N}{|\widetilde{\mathscr{W}}|}f_{\widetilde{\mathscr{W}}}(\mathbf{y})$ and by using the Gaussian heuristic and some computations that are detailed in Appendix H:

$$f_{\mathscr{W}}(\mathbf{y})\approx N\frac{\sqrt{n\pi}}{e}\sum_{j\geqslant 0}N_j\left(\frac{n}{2\pi ewj}\right)^{n/2-1}J_{n/2-1}(2\pi wj).\tag{18}$$

We can use now a similar heuristic as the one described in §5.2 and predict that the abnormal large values of the score function $f_{\mathscr{W}}(\mathbf{y})$ appear when $\mathbf{y}$ is abnormally close to Λ, say $N_{\leqslant x}\neq 0$, where $N_{\leqslant x}=|\{\mathbf{c}\in\Lambda:|\mathbf{y}-\mathbf{c}|\leqslant x\}|$ when $\mathbb{P}\left(N_{\leqslant x}\neq 0\right)\ll 1$. In this case, we make the crude approximation that the sum (18) is dominated by the term j_0 which is the smallest in it:

$$f_{\mathscr{W}}(\mathbf{y})\approx N\frac{\sqrt{n\pi}}{e}N_{j_0}\left(\frac{n}{2\pi ewj_0}\right)^{n/2-1}J_{n/2-1}(2\pi wj_0).\tag{19}$$

The survival function $\mathbb{P}\left(f_{\mathscr{W}}(\mathbf{y})\geqslant X\right)$ is then crudely approximated as the probability that such an event happens

$$\begin{aligned}\mathbb{P}\left(f_{\mathscr{W}}(\mathbf{y})\geqslant N\frac{\sqrt{n\pi}}{e}N_x\left(\frac{n}{2\pi ewx}\right)^{n/2-1}J_{n/2-1}(2\pi wx)\right)&\approx\mathbb{P}\left(N_{\leqslant x}\geqslant 1\right)\\&\approx\mathbb{E}(N_{\leqslant x})\\&\approx\left(\frac{x}{\sqrt{\frac{n}{2\pi e}\cdot(\pi n)^{1/n}\cdot|\Lambda|^{1/n}}}\right)^n\end{aligned}$$

[1] Here the j's belong to the discrete set of all possible norms in the lattice and should not be viewed as an integer value.

where the last approximation is the Gaussian heuristic. In the context of the experiments described in [DP23b, §5], $\Lambda \stackrel{\text{def}}{=} \mathcal{L}(\mathbf{B})$ is given by[2]

$$\mathbf{B} \stackrel{\text{def}}{=} \left[\begin{array}{c|c} \mathbf{I}_{n/2} & \mathbf{A} \\ \hline \mathbf{0} & q \cdot \mathbf{I}_{n/2} \end{array}\right] \cdot \left[\begin{array}{c|c} 2 \cdot \mathbf{I}_{k_{\text{fft}}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I}_{n-k_{\text{fft}}} \end{array}\right] \tag{20}$$

Then we use the same *full sieve* algorithm as in [DP23b] to produce short vectors $\mathscr{W} \subset \Lambda^\vee$. In what follows, we use the practical values of N and w that we obtained by experiments. We have reused the implementation for the experiments in [DP23b, §5][3]. This very crude estimation seems to capture the error-floor behavior of the survival function as shown in Figure 3. The point is that it is precisely this part of the curve which is not predicted by the standard independence assumption and which had no explanation so far. It can also be observed that the duality result is nothing but a straighforward use of the Poisson formula which has also be used very recently in [WE23] to predict the abnormal variance of the BDD score distribution observed in [DP23b, Table 1].

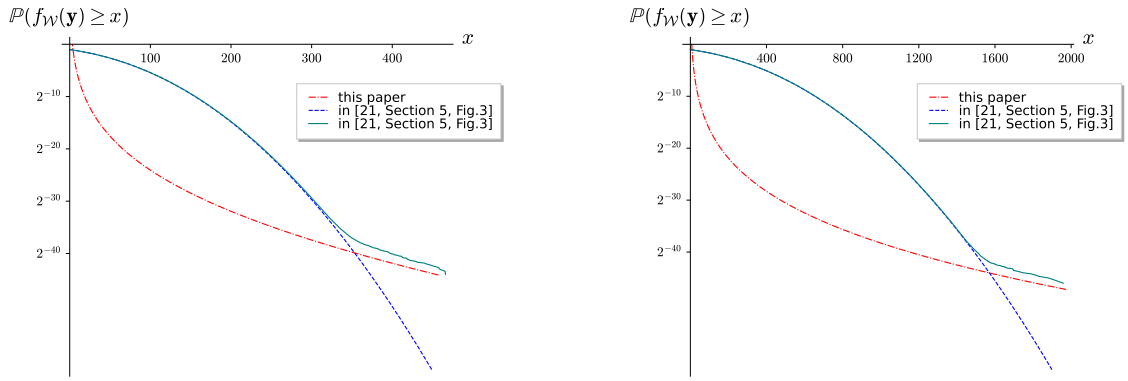

FIGURE 3. Crude estimation of the survival function (red, dash-dot line) compared to the experiments in [DP23b, §5] (green, full line) and the prediction with the standard independence assumption (blue, dashed line). (left) $q = 3329$, $n = 60$, $T = 2^{45}$, $N = 5040$ and $w = 0.0320$; (right) $q = 3329$, $n = 80$, $T = 2^{48}$, $N = 89494$ and $w = 0.0376$.

A more precise prediction. One can remark (see Figure 3) that *i*) our newly introduced approximate distribution for $f_{\mathscr{W}}$ given in Equation (19) matches the experimental curves specifically in the waterfall-floor zone and *ii*) the distribution of $f_{\mathscr{W}}$ given by the independence heuristic [DP23b, Heuristic 3] matches the experimental curves up to this waterfall-floor zone. A natural idea to predict the experimental curve on the whole support is therefore to take the convolution of these two distributions. Indeed, for any support point, there is always one distribution which exponentially dominates the other one.

Distribution in the waterfall-floor zone. Let us denote by $\mathbf{X}_{\text{floor}}$ the random variable given by Equation (19), namely:

$$\mathbf{X}_{\text{floor}} \stackrel{\text{def}}{=} G(j_0) \tag{21}$$

where

$$G(j) = N \frac{\sqrt{n\pi}}{e} \left(\frac{n}{2\pi e w j}\right)^{n/2-1} J_{n/2-1}(2\pi w j)$$

and j_0 is the length of the shortest vector of the lattice. We only have to compute the distribution of j_0 to compute the distribution of $\mathbf{X}_{\text{floor}}$. To that extend we make the following classic model.

[2] In [DP23b], Λ and $\mathbf{B}$ are actually respectively Λ' and $\mathbf{B}'$

[3] https://github.com/ludopulles/DoesDualSieveWork

Model 2. *Model for the number of lattice points in a ball. Let Λ be a random lattice of full rank n and of volume V. We make the model that:*

$$|\Lambda \setminus \{0\} \cap \mathcal{B}_z| \sim \text{Poisson}\left(\frac{\text{Vol}\left(\mathcal{B}_1\right) z^n}{V}\right)$$

where $\mathcal{B}_z$ denotes the Euclidean ball of center $\mathbf{0}$ and radius z and $\text{Vol}\left(\mathcal{B}_1\right) = \frac{\sqrt{\pi^n}}{\Gamma\left(\frac{n}{2}+1\right)}$.

This model allows us to write the following fact regarding the distribution of the length of the j'th shortest vector:

Fact 2. *Under Model 2, and for $k = 0 \cdots \infty$ the distribution of j_k,* i.e. *the k'th non-zero shortest vector of a random lattice Λ of full rank n and of volume V, is given by:*

$$j_k^n \sim \text{Gamma}\left(k+1,\ \frac{\text{Vol}\left(\mathcal{B}_1\right)}{V}\right)$$

where $\mathbf{Z} \sim \text{Gamma}\left(b, \theta\right)$ has the following survival function when b is an integer:

$$\mathbb{P}\left(\mathbf{Z} \geqslant \alpha\right) \overset{def}{=} e^{-\theta\alpha} \sum_{i=0}^{b-1} \frac{\left(\theta\alpha\right)^i}{i!}.$$

Proof. For any $z > 0$, we have that

$$\begin{aligned}
\mathbb{P}\left(j_k^n > z^n\right) &= \mathbb{P}\left(j_k > z\right) \\
&= \mathbb{P}\left(\bigcup_{i=0}^{k} \text{“}|\Lambda \setminus \{0\} \cap \mathcal{B}_z| = i\text{”}\right) \\
&= \sum_{i=0}^{k} \mathbb{P}\left(|\Lambda \setminus \{0\} \cap \mathcal{B}_z| = i\right) && \text{(disjoint union)} \\
&= \sum_{i=0}^{k} \frac{\left(\text{Vol}\left(\mathcal{B}_1\right)\ z^n/V\right)^i\ e^{-\left(\text{Vol}\left(\mathcal{B}_1\right)\ z^n/V\right)}}{i\,!} && \text{(Model 2)}
\end{aligned}$$

which completes the proof. □

Distribution in the waterfall zone. Let us denote by $\mathbf{X}_{\text{fall}}$ the random variable $f_{\mathscr{W}}$ under the independence heuristic. As given by [DP23b, Lemma 3] and the discussion that follows their lemma we have

Fact 3. $\mathbf{X}_{\text{fall}}$ *follows a normal distribution of mean 0 and variance $\frac{1}{2}N$. More precisely, its probability density function p is given by*

$$p(x) = \frac{1}{\sqrt{\pi N}} e^{-x^2/N}.$$

We now make the refined model that $f_{\mathscr{W}}\left(\mathbf{y}\right)$ follows the same distribution as $\mathbf{X}_{\text{fall}} + \mathbf{X}_{\text{floor}}$ where the distribution of $\mathbf{X}_{\text{floor}}$ is computed numerically by using Fact 2 along with Equation (21). We show in Figure 4 that the distribution of this refined model well approximates the behavior of the experimental distribution of $f_{\mathscr{W}}$ on the whole support.

Concurrent work. Note that very recently we have been made aware of the concurrent work [DP23a] which similarly to what we do here, uses Bessel functions to predict the score with a related approach and similar predictions (see [DP23a, §4.3]).

References

[AAB+21a] Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, and Gilles Zémor. BIKE. Round 3 Submission to the NIST Post-Quantum Cryptography Call, v. 4.2, September 2021.

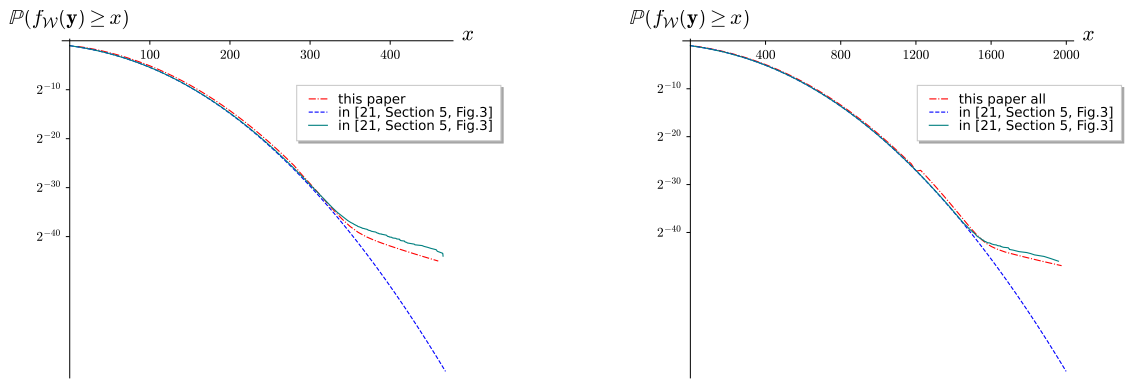

FIGURE 4. Refined estimation of the survival function (red, dash-dot line) compared to the experiments in [DP23b, §5] (green, full line) and the prediction with the standard independence assumption (blue, dashed line). (left) $q = 3329$, $n = 60$, $T = 2^{45}$, $N = 5040$ and $w = 0.0320$; (right) $q = 3329$, $n = 80$, $T = 2^{48}$, $N = 89494$ and $w = 0.0376$

[AAB+21b] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos. HQC. Round 3 Submission to the NIST Post-Quantum Cryptography Call, June 2021. https://pqc-hqc.org/doc/hqc-specification_2021-06-06.pdf.

[AGS11] Carlos Aguilar, Philippe Gaborit, and Julien Schrek. A new zero-knowledge code based identification scheme with reduced communication. In *Proc. IEEE Inf. Theory Workshop- ITW 2011*, pages 648–652. IEEE, October 2011.

[Alb17] Martin R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, volume 10211 of *Lecture Notes in Computer Science*, pages 103–129, 2017.

[Arı09] Erdal Arıkan. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inform. Theory*, 55(7):3051–3073, 2009.

[BCL+19] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Mizoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, and Wang Wen. Classic McEliece: conservative code-based cryptography. https://classic.mceliece.org, March 2019. Second round submission to the NIST post-quantum cryptography call.

[BCN89] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-Regular Graphs*. Number 18 in Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Verlag Berlin Heidelberg, 1989.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

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

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: ball-collision decoding. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760, 2011.

[BM17] Leif Both and Alexander May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In *WCC Workshop on Coding and Cryptography*, September 2017.

[BM18] Leif Both and Alexander May. Decoding linear codes with high error rate and its impact for LPN security. In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography 2018*, volume 10786 of *LNCS*, pages 25–46, Fort Lauderdale, FL, USA, April 2018. Springer.

[CDMT22] Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Statistical decoding 2.0: Reducing decoding to LPN. In *Advances in Cryptology - ASIACRYPT 2022*, LNCS. Springer, 2022.

[CST22] Kevin Carrier, Yixin Shen, and Jean-Pierre Tillich. Faster dual lattice attacks by using coding theory. Cryptology ePrint Archive, Paper 2022/1750, 2022. https://eprint.iacr.org/2022/1750.

[CVA10] Pierre-Louis Cayrel, Pascal Véron, and Sidi Mohamed El Yousfi Alaoui. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In *Selected Areas in Cryptography*, pages 171–186, 2010.

[DDRT23] Thomas Debris-Alazard, Léo Ducas, Nicolas Resch, and Jean-Pierre Tillich. Smoothing codes and lattices: Systematic study and new bounds. *IEEE Trans. Inform. Theory*, 69(9):6006–6027, 2023.

[DP23a] Léo Ducas and Ludo N. Pulles. Accurate score prediction for dual attacks. preprint, November 2023. preprint.

[DP23b] Léo Ducas and Ludo N. Pulles. Does the dual-sieve attack on learning with errors even work? In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023*, volume 14083 of *LNCS*, pages 37–69, Santa Barbara, CA, USA, August 2023. Springer.

[DT17a] Thomas Debris-Alazard and Jean-Pierre Tillich. Statistical decoding. preprint, January 2017. arXiv:1701.07416.

[DT17b] Thomas Debris-Alazard and Jean-Pierre Tillich. Statistical decoding. Slides of the ISIT talk, June 2017. See `https://tdalazard.io/slidesDecoStat.pdf`.

[DT17c] Thomas Debris-Alazard and Jean-Pierre Tillich. Statistical decoding. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2017*, pages 1798–1802, Aachen, Germany, June 2017.

[Dum86] Ilya Dumer. On syndrome decoding of linear codes. In *Proceedings of the 9th All-Union Symp. on Redundancy in Information Systems, abstracts of papers (in russian), Part 2*, pages 157–159, Leningrad, 1986.

[Dum89] Il'ya Dumer. Two decoding algorithms for linear codes. *Probl. Inf. Transm.*, 25(1):17–23, 1989.

[Dum91] Ilya Dumer. On minimum distance decoding of linear codes. In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pages 50–52, Moscow, 1991.

[EJK20] Thomas Espitau, Antoine Joux, and Natalia Kharchenko. On a dual/hybrid approach to small secret LWE - A dual/enumeration technique for learning with errors and application to security estimates of FHE schemes. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 440–462. Springer, 2020.

[EKM17] Andre Esser, Robert Kübler, and Alexander May. LPN decoded. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017*, volume 10402 of *LNCS*, pages 486–514, Santa Barbara, CA, USA, August 2017. Springer.

[Ess22] Andre Esser. Revisiting nearest-neighbor-based information set decoding. Cryptology ePrint Archive, Paper 2022/1328, 2022. https://eprint.iacr.org/2022/1328.

[FJR22] Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs. *IACR Cryptol. ePrint Arch.*, page 188, 2022.

[GJ21] Qian Guo and Thomas Johansson. Faster dual lattice attacks for solving LWE with applications to CRYSTALS. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV*, volume 13093 of *Lecture Notes in Computer Science*, pages 33–62. Springer, 2021.

[GJL14] Qian Guo, Thomas Johansson, and Carl Löndahl. Solving LPN using covering codes. In *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 1–20. Springer, 2014.

[Gol17] Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, 2017.

[GPS22] Shay Gueron, Edoardo Persichetti, and Paolo Santini. Designing a practical code-based signature scheme from zero-knowledge proofs with trusted setup. *Cryptogr.*, 6(1):5, 2022.

[Gre66] Richard R. Green. A serial orthogonal decoder. *JPL Space Programs Summary*, 37-39-IV:247–253, 1966.

[Jab01] Abdulrahman Al Jabri. A statistical decoding algorithm for general linear block codes. In Bahram Honary, editor, *Cryptography and coding. Proceedings of the 8th IMA International Conference*, volume 2260 of *LNCS*, pages 1–8, Cirencester, UK, December 2001. Springer.

[KS21] Naomi Kirshner and Alex Samorodnitsky. A moment ratio bound for polynomials and some extremal properties of krawchouk polynomials and hamming spheres. *IEEE Trans. Inform. Theory*, 67(6):3509–3541, 2021.

[KU10] Satish B. Korada and Rüdiger Urbanke. Polar codes are optimal for lossy source coding. *IEEE Trans. Inform. Theory*, 56(4):1751–1768, 2010.

[LF06] Éric Levieil and Pierre-Alain Fouque. An improved LPN algorithm. In *Proceedings of the 5th international conference on Security and Cryptography for Networks*, volume 4116 of *LNCS*, pages 348–359. Springer, 2006.

[MAT22] MATZOV. Report on the Security of LWE: Improved Dual Lattice Attack, April 2022.

[McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

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

[MS86] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. North–Holland, Amsterdam, fifth edition, 1986.

[MT23] Charles Meyer-Hilfiger and Jean-Pierre Tillich. Rigorous foundations for dual attacks in coding theory. In *Theory of Cryptography Conference, TCC 2023*, LNCS. Springer Verlag, December 2023. to appear.

[Ove06] Raphael Overbeck. Statistical decoding revisited. In Reihaneh Safavi-Naini Lynn Batten, editor, *Information security and privacy : 11th Australasian conference, ACISP 2006*, volume 4058 of *LNCS*, pages 283–294. Springer, 2006.

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

[PS23] Amaury Pouly and Yixin Shen. Provable dual attacks on learning with errors. Cryptology ePrint Archive, Paper 2023/1508, 2023. https://eprint.iacr.org/2023/1508.

[Şaş11] Eren Şaşoğlu. Polarization and polar codes. *Foundations and Trends in Communications and Information Theory*, 8(4):259–381, 2011.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.

[Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In D.R. Stinson, editor, *Advances in Cryptology - CRYPTO'93*, volume 773 of *LNCS*, pages 13–21. Springer, 1993.

[TV12] Ido Tal and Alexander Vardy. List decoding of polar codes. *CoRR*, abs/1206.0050, 2012.

[Vér96] Pascal Véron. Improved identification schemes based on error-correcting codes. *Appl. Algebra Eng. Commun. Comput.*, 8(1):57–69, 1996.

[vL99] Jacobus Hendricus van Lint. *Introduction to coding theory*. Graduate texts in mathematics. Springer, 3rd edition edition, 1999.

[WE23] Andreas Wiemers and Stephan Ehlen. A remark on the independence heuristic in the dual attack. IACR Cryptology ePrint Archive, Report2023/1238, August 2023. http://eprint.iacr.org/2023/1238.

Appendix A. Proof of Proposition 2

Let us first recall this proposition

Proposition 2. *Suppose that the parameters are such that for some constant $\alpha > 0$*

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} = \omega\left(\frac{n^\alpha}{\delta^2}\right) \qquad \text{where} \qquad \delta \stackrel{def}{=} \frac{K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}. \tag{7}$$

Moreover suppose that

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^k} = \mathcal{O}(n^\alpha) \quad \text{and} \quad \frac{\binom{s}{t_{\text{aux}}}}{2^{s-k_{\text{aux}}}} = \mathcal{O}(n^\alpha)\,. \tag{8}$$

Let $\mathscr{N}$ be a set of $n-s$ positions in $[\![1,n]\!]$ and $\mathscr{P} \stackrel{def}{=} [\![1,n]\!]\backslash\mathscr{N}$. Let $\mathbf{e}$ be a vector of weight u on $\mathscr{N}$ and $t-u$ on $\mathscr{P}$. Let $\mathcal{C}$ and $\mathcal{C}_{\text{aux}}$ be $[n,k]$ and $[s,k_{\text{aux}}]$ linear codes respectively. Let us choose $(\mathbf{c}_{\text{aux}}, \mathbf{h})$ uniformly at random in

$$\widetilde{\mathscr{H}} = \{(\mathbf{h}, \mathbf{c}_{\text{aux}}) \in \mathcal{C}^\perp \times \mathcal{C}_{\text{aux}} \,:\, |\mathbf{h}_{\mathscr{N}}| = w \text{ and } |\mathbf{h}_{\mathscr{P}} + \mathbf{c}_{\text{aux}}| = t_{\text{aux}}\}.$$

Then for a proportion $1-o(1)$ of codes $\mathcal{C}_{\text{aux}}$ and $\mathcal{C}$ we have that

$$\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\stackrel{\$}{\leftarrow}\widetilde{\mathscr{H}}}{\text{bias}}(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle) = \delta(1+o(1)).$$

The proof of this Proposition 2 will be a consequence of the following lemma.

Lemma 2. *Let $w, s, k, k_{\text{aux}}, t_{\text{aux}}, n \in \mathbb{N}$ be such that (for some constant $a > 0$)*

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^k} = \mathcal{O}(n^\alpha) \quad \text{and} \quad \frac{\binom{s}{t_{\text{aux}}}}{2^{s-k_{\text{aux}}}} = \mathcal{O}(n^\alpha) \tag{22}$$

Let $\mathscr{N}$ be a fixed set of $n-s$ positions in $[\![1,n]\!]$ and $\mathscr{P} \stackrel{def}{=} [\![1,n]\!]\backslash\mathscr{N}$. Let $\mathbf{e} \in \mathbb{F}_2^n$ be some error of weight u on $\mathscr{N}$.

Assume that $\mathcal{C}$ is an $[n,k]$-linear code chosen by picking an $(n-k)\times n$ binary parity-check matrix $\mathbf{H}$ uniformly at random and that $\mathcal{C}_{\text{aux}}$ is chosen by picking an $(s-k_{\text{aux}})\times s$ binary parity-check matrix $\mathbf{H}_{\text{aux}}$ uniformly at random. Let us define for $b \in \{0,1\}$,

$$E_b \stackrel{def}{=} \left|\left\{(\mathbf{e}', \mathbf{h}) \in \mathcal{S}^s_{t_{\text{aux}}} \times \mathcal{C}^\perp :\ |\mathbf{h}_{\mathscr{N}}| = w \ \text{ and } \ \mathbf{e}' + \mathbf{h}_{\mathscr{P}} \in \mathcal{C}_{\text{aux}},\ \langle \mathbf{e}', \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle = b\right\}\right|,$$

$$E'_b \stackrel{def}{=} \left|\left\{(\mathbf{e}', \mathbf{h}) \in \mathcal{S}^s_{t_{\text{aux}}} \times \mathbb{F}_2^n :\ |\mathbf{h}_{\mathscr{N}}| = w \ \text{ and } \ \langle \mathbf{e}', \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle = b\right\}\right|.$$

Then,

$$\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}(E_b) \;=\; \Theta(1)\,\frac{E'_b}{2^{k+s-k_{\text{aux}}}} \tag{23}$$

$$\mathbf{Var}_{\mathbf{H},\mathbf{H}_{\text{aux}}}(E_b) \;=\; \mathcal{O}(n^\alpha)\,\frac{E'_b}{2^{k+s-k_{\text{aux}}}} \tag{24}$$

Proof. Let $\mathbf{1}_{\mathbf{e}',\mathbf{h}}$ be the indicator function of the event "$\mathbf{h} \in \mathcal{C}^\perp$ and $\mathbf{e}' + \mathbf{h}_{\mathscr{P}} \in \mathcal{C}_{\text{aux}}$". Define

$$\mathcal{E}_b \stackrel{\text{def}}{=} \left\{(\mathbf{e}', \mathbf{h}) \in \mathcal{S}^s_{t_{\text{aux}}} \times \mathbb{F}_2^n \colon |\mathbf{h}_{\mathscr{N}}| = w \text{ and } \langle \mathbf{e}', \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle = b\right\}.$$

Notice that $E'_b = |\mathcal{E}_b|$. By definition and linearity of the expectation

$$\begin{aligned}
\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}(E_b) &= \mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\sum_{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b} \mathbf{1}_{\mathbf{e}',\mathbf{h}}\right) \\
&= \sum_{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b} \mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}(\mathbf{1}_{\mathbf{e}',\mathbf{h}}) \\
&= \sum_{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b} \mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h} \in \mathcal{C}^\perp, \mathbf{h}_{\mathscr{P}} + \mathbf{e}' \in \mathcal{C}_{\text{aux}}\right)
\end{aligned} \tag{25}$$

We have that,

$$\mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h}\in\mathcal{C}^{\perp},\mathbf{h}_{\mathscr{P}}+\mathbf{e}'\in\mathcal{C}_{\text{aux}}\right)=\begin{cases}\frac{1}{2^{k+s-k_{\text{aux}}}} & \text{if } \mathbf{h}_{\mathscr{P}}+\mathbf{e}'\neq\mathbf{0}\\ \frac{1}{2^k} & \text{otherwise.}\end{cases} \tag{26}$$

Indeed, notice that events "$\mathbf{h}\in\mathcal{C}^{\perp}$" and "$\mathbf{h}_{\mathscr{P}}+\mathbf{e}'\in\mathcal{C}_{\text{aux}}$" are independent. Furthermore, $\mathbf{h}$ cannot be equal to $\mathbf{0}$ as $|\mathbf{h}_{\mathscr{N}}|=w>0$. Therefore,

$$\begin{aligned}\mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h}\in\mathcal{C}^{\perp},\mathbf{h}_{\mathscr{P}}+\mathbf{e}'\in\mathcal{C}_{\text{aux}}\right)&=\mathbb{P}_{\mathbf{H}}\left(\mathbf{h}\in\mathcal{C}^{\perp}\right)\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}_{\mathscr{P}}+\mathbf{e}'\in\mathcal{C}_{\text{aux}}\right)\\&=\frac{1}{2^k}\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}_{\mathscr{P}}+\mathbf{e}'\in\mathcal{C}_{\text{aux}}\right)\end{aligned}$$

Now, plugging Equation (26) in (25) leads to,

$$\begin{aligned}\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(E_b\right)&=\sum_{\substack{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b\\ \mathbf{h}_{\mathscr{P}}\neq\mathbf{e}'}}\frac{1}{2^{k+s-k_{\text{aux}}}}+\sum_{\substack{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b\\ \mathbf{h}_{\mathscr{P}}=\mathbf{e}'}}\frac{1}{2^k}\\&=\sum_{\mathbf{e}'\in\mathcal{S}^s_{t_{\text{aux}}}}\left(\frac{\left|\mathscr{E}^{\mathbf{e}'}_{b,1}\right|}{2^{k+s-k_{\text{aux}}}}+\frac{\left|\mathscr{E}^{\mathbf{e}'}_{b,2}\right|}{2^k}\right)\end{aligned} \tag{27}$$

where for a fixed $\mathbf{e}'$,

$$\mathscr{E}^{\mathbf{e}'}_{b,1}\overset{\text{def}}{=}\left\{\mathbf{h}\in\mathbb{F}_2^n:\ (\mathbf{e}',\mathbf{h})\in\mathscr{E}_b\text{ and }\mathbf{h}_{\mathscr{P}}\neq\mathbf{e}'\right\}, \tag{28}$$

$$\mathscr{E}^{\mathbf{e}'}_{b,2}\overset{\text{def}}{=}\left\{\mathbf{h}\in\mathbb{F}_2^n:\ (\mathbf{e}',\mathbf{h})\in\mathscr{E}_b\text{ and }\mathbf{h}_{\mathscr{P}}=\mathbf{e}'\right\}. \tag{29}$$

Notice that for any $\mathbf{e}'$,

$$|\mathscr{E}_{b,1}|=\frac{|\mathscr{E}_{b,2}|}{2^s} \tag{30}$$

It is readily seen that,

$$|\mathscr{E}_b|=\sum_{\mathbf{e}'\in\mathcal{S}^s_{t_{\text{aux}}}}\left(\left|\mathscr{E}^{\mathbf{e}'}_{b,1}\right|+\left|\mathscr{E}^{\mathbf{e}'}_{b,2}\right|\right)$$

which implies that

$$\sum_{\mathbf{e}'\in\mathcal{S}^s_{t_{\text{aux}}}}\left|\mathscr{E}^{\mathbf{e}'}_{b,1}\right|=\frac{|\mathscr{E}_b|}{1+\frac{1}{2^s}}=\Theta\left(1\right)|\mathscr{E}_b|\quad\text{and}\quad\sum_{\mathbf{e}'\in\mathcal{S}^s_{t_{\text{aux}}}}\left|\mathscr{E}^{\mathbf{e}'}_{b,2}\right|=\frac{|\mathscr{E}_b|}{2^s-1}=\Theta\left(2^{-s}\right)|\mathscr{E}_b|$$

Plugging this into Equation (27) leads to,

$$\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(E_b\right)=\Theta\left(1\right)\frac{|\mathscr{E}_b|}{2^{k+s-k_{\text{aux}}}}+\Theta\left(1\right)\frac{|\mathscr{E}_b|}{2^{k+s}}=\Theta\left(1\right)\frac{|\mathscr{E}_b|}{2^{k+s-k_{\text{aux}}}} \tag{31}$$

which shows Equation (23). Let us show now Equation (24). By definition

$$\begin{aligned}\mathbf{Var}\left(E_b\right)&=\sum_{(\mathbf{e}',\mathbf{h})\in\mathcal{E}_b}\mathbf{Var}\left(\mathbf{1}_{\mathbf{e}',\mathbf{h}}\right)+\sum_{\substack{(\mathbf{e}'_0,\mathbf{h}^0),(\mathbf{e}'_1,\mathbf{h}^1)\in\mathcal{E}_b\\(\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}}\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\ \mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)-\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)\\&\leqslant\frac{E'_b}{2^{k+s-k_{\text{aux}}}}+\sum_{\substack{(\mathbf{e}'_0,\mathbf{h}^0),(\mathbf{e}'_1,\mathbf{h}^1)\in\mathcal{E}_b\\(\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}}\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\ \mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)-\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)\end{aligned}$$

where we used that $\mathbf{Var}(\mathbf{1}_{\mathbf{e}',\mathbf{h}})\leqslant\mathbb{E}\left(\mathbf{1}^2_{\mathbf{e},\mathbf{h}}\right)=\mathbb{E}\left(\mathbf{1}_{\mathbf{e},\mathbf{h}}\right)$ and Equation (31).

To compute the above expectations, we will split in two cases according to $\mathscr{E}^{\mathbf{e}'}_{b,1}$ and $\mathscr{E}^{\mathbf{e}'}_{b,2}$ which are respectively defined in Equations (28) and (29). More precisely, we will fix $\mathbf{e}'_b$ and suppose that $\mathbf{h}^b$ belongs to $\mathscr{E}_{b,1}$ or $\mathscr{E}_{b,2}$. We will treat the following disjoint cases.

1. $\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}=\left\{(\mathbf{h}^0,\mathbf{h}^1):\ \mathbf{h}^0\in\mathscr{E}^{\mathbf{e}'_0}_{b,1}\text{ and }\mathbf{h}^1\in\mathscr{E}^{\mathbf{e}'_1}_{b,1}\right\}$,
2. $\mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1}=\left\{(\mathbf{h}^0,\mathbf{h}^1):\ \mathbf{h}^0\in\mathscr{E}^{\mathbf{e}'_0}_{b,2}\text{ and }\mathbf{h}^1\in\mathscr{E}^{\mathbf{e}'_1}_{b,1}\right\}$
3. $\mathscr{F}_2^{\mathbf{e}'_0,\mathbf{e}'_1}=\left\{(\mathbf{h}^0,\mathbf{h}^1):\ \mathbf{h}^0\in\mathscr{E}^{\mathbf{e}'_0}_{b,1}\text{ and }\mathbf{h}^1\in\mathscr{E}^{\mathbf{e}'_1}_{b,2}\right\}$

4. $\mathscr{F}_3^{\mathbf{e}'_0,\mathbf{e}'_1} = \left\{(\mathbf{h}^0,\mathbf{h}^1):\ \mathbf{h}^0 \in \mathscr{E}_{b,2}^{\mathbf{e}'_0} \text{ and } \mathbf{h}^1 \in \mathscr{E}_{b,2}^{\mathbf{e}'_1}\right\}$

In particular,

$$\begin{aligned}\mathbf{Var}\left(E_b\right) \leqslant \frac{E'_b}{2^{k+s-k_{\text{aux}}}} + \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \Bigg(& \underbrace{\sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)}_{\stackrel{\text{def}}{=} F_0} \\ & + \underbrace{\sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)}_{\stackrel{\text{def}}{=} F_1} \\ & + \underbrace{\sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_2^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)}_{\stackrel{\text{def}}{=} F_2} \\ & + \underbrace{\sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_3^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)}_{\stackrel{\text{def}}{=} F_3} \Bigg) \end{aligned} \tag{32}$$

Let,

$$\text{Cov} \stackrel{\text{def}}{=} F_0 + F_1 + F_2 + F_3 \tag{33}$$

For each cases, we will split according to the following subcases.

i. $\mathbf{e}'_0 = \mathbf{e}'_1,\ \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$,
ii. $\mathbf{e}'_0 = \mathbf{e}'_1,\ \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$,
iii. $\mathbf{e}'_0 \neq \mathbf{e}'_1$ and $\mathbf{h}^0 = \mathbf{h}^1$
iv. $\mathbf{e}'_0 \neq \mathbf{e}'_1,\ \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$
v. $\mathbf{e}'_0 \neq \mathbf{e}'_1, \mathbf{h}^0 \neq \mathbf{h}^1, \mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$
vi. $\mathbf{e}'_0 \neq \mathbf{e}'_1, \mathbf{h}^0 \neq \mathbf{h}^1, \mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$

Case 1: Recall that in this case we have

$$\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{e}'_0 \quad \text{and} \quad \mathbf{h}^1_{\mathscr{P}} \neq \mathbf{e}'_1 \tag{34}$$

We have,

$$\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) = \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2$$

Let us compute $\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)$ when $(\mathbf{e}'_0,\mathbf{h}^0) \neq (\mathbf{e}'_1,\mathbf{h}^1)$. By definition

$$\begin{aligned}\mathbb{E}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) &= \mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) \\ &= \mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp\right)\mathbb{P}_{\mathbf{H},\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right)\end{aligned}$$

Therefore,

$$\sum_{\mathbf{e}'_0,\mathbf{e}'_1} F_0 = \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2$$
$$= \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \text{Cov}^{(0)} \tag{35}$$

where,

$$\text{Cov}^{(0)} \stackrel{\text{def}}{=} \mathbb{P}_{\mathbf{H}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp\right) \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2$$

Our aim now it to upper-bound $\text{Cov}^{(0)}$ according to the above 6 sub-cases.

Sub-case i. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. We have

$$\begin{aligned}
\text{Cov}^{(0)} &= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2 \qquad (\text{as } \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1) \\
&= \frac{1}{2^{2k}}\,\frac{1}{2^{s-k_{\text{aux}}}} - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2
\end{aligned}$$

where in the last line we used Equation (34). Therefore, in that case

$$\text{Cov}^{(0)} \leqslant \frac{1}{2^{2k}}\,\frac{1}{2^{s-k_{\text{aux}}}}.$$

Sub-case ii. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1, \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$. We have

$$\begin{aligned}
\text{Cov}^{(0)} &= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}\right)\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2
\end{aligned} \tag{36}$$

where in the last line we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$showing that these two vectors are linearly independent (we work in $\mathbb{F}_2$), and thus that both events are independent. But, as they are different from $\mathbf{0}$ (according to Equation (34)) we have for ($b \in \{0,1\}$)

$$\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^b_{\mathscr{P}} + \mathbf{e}'_b \in \mathcal{C}_{\text{aux}}\right) = \frac{1}{2^{s-k_{\text{aux}}}}$$

Therefore, plugging this in Equation (36) leads to

$$\text{Cov}^{(0)} = 0.$$

Sub-case iii. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 = \mathbf{h}^1$. In that case,

$$\begin{aligned}
\text{Cov}^{(0)} &= \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0 \in \mathcal{C}^\perp\right)\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2 \\
&= \frac{1}{2^{k}}\,\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}\right)\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2 \\
&= \frac{1}{2^{k}}\,\left(\frac{1}{2^{s-k_{\text{aux}}}}\right)^2 - \left(\frac{1}{2^{k+s-k_{\text{aux}}}}\right)^2
\end{aligned}$$

where in the second equality we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$ and are different from $\mathbf{0}$ (according to Equation (34)) which implies that both events are independent. Therefore, in that case

$$\mathrm{Cov}^{(0)} \leqslant \frac{1}{2^{k+2s-2k_{\mathrm{aux}}}} \tag{37}$$

Sub-case iv. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. In that case,

$$\begin{aligned}
\mathrm{Cov}^{(0)} &= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}\right) \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= 0
\end{aligned}$$

where in the second equality we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$ which implies that both events are independent.

Sub-case v. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. We have

$$\begin{aligned}
\mathrm{Cov}^{(0)} &= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}} \frac{1}{2^{s-k_{\mathrm{aux}}}} - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2
\end{aligned}$$

Therefore,

$$\mathrm{Cov}^{(0)} \leqslant \frac{1}{2^{2k+s-k_{\mathrm{aux}}}}$$

Sub-case vi. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. In that case we can write

$$\begin{aligned}
\mathrm{Cov}^{(0)} &= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \frac{1}{2^{2k}} \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}\right) \mathbb{P}_{\mathbf{H}_{\mathrm{aux}}} \left(\mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 \\
&= \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2 - \left(\frac{1}{2^{k+s-k_{\mathrm{aux}}}}\right)^2
\end{aligned}$$

Therefore we obtain,

$$\mathrm{Cov}^{(0)} = 0.$$

Case 2: Recall that in this case we have

$$\mathbf{h}^0_{\mathscr{P}} = \mathbf{e}'_0 \quad \text{and} \quad \mathbf{h}^1_{\mathscr{P}} \neq \mathbf{e}'_1 \tag{38}$$

We have,

$$\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0, \mathbf{h}^0}\right) \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1, \mathbf{h}^1}\right) = \frac{1}{2^k} \frac{1}{2^{k+s-k_{\mathrm{aux}}}} = \frac{1}{2^{2k+s-k_{\mathrm{aux}}}}$$

Let us compute $\mathbb{E}_{\mathbf{H}, \mathbf{H}_{\mathrm{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0, \mathbf{h}^0}\, \mathbf{1}_{\mathbf{e}'_1, \mathbf{h}^1}\right)$ when $(\mathbf{e}'_0, \mathbf{h}^0) \neq (\mathbf{e}'_1, \mathbf{h}^1)$. By definition

$$\begin{aligned}
\mathbb{E}_{\mathbf{H}, \mathbf{H}_{\mathrm{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0, \mathbf{h}^0}\, \mathbf{1}_{\mathbf{e}'_1, \mathbf{h}^1}\right) &= \mathbb{P}_{\mathbf{H}, \mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0, \mathbf{h}^1 \in \mathcal{C}^{\perp}, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) \\
&= \mathbb{P}_{\mathbf{H}, \mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0, \mathbf{h}^1 \in \mathcal{C}^{\perp}\right) \mathbb{P}_{\mathbf{H}, \mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right)
\end{aligned}$$

Therefore,

$$\sum_{\mathbf{e}'_0,\mathbf{e}'_1} F_1 = \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\ \mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \text{Cov}^{(1)} \tag{39}$$

where,

$$\text{Cov}^{(1)} \stackrel{\text{def}}{=} \mathbb{P}_{\mathbf{H}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp\right) \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$

Our aim now it to upper-bound $\text{Cov}^{(1)}$ according to the above 6 sub-cases.

Sub-case i. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. This subcase is impossible according to Equation (38). Therefore,

$$\text{Cov}^{(1)} = 0.$$

Sub-case ii. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1, \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$. We have

$$\text{Cov}^{(1)} = \frac{1}{2^{2k}}\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \frac{1}{2^{2k}}\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}} \tag{40}$$

where in the last line we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$ showing that these two vectors are linearly independent (we work in $\mathbb{F}_2$), and thus that both events are independent. Furthermore, we also used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{0}$ according to Equation (38). But,

$$\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) = \frac{1}{2^{s-k_{\text{aux}}}}$$

Therefore, plugging this in Equation (40) leads to

$$\text{Cov}^{(1)} = 0.$$

Sub-case iii. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 = \mathbf{h}^1$. In that case,

$$\text{Cov}^{(1)} = \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0 \in \mathcal{C}^\perp\right) \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \frac{1}{2^k}\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}\right) \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \frac{1}{2^k}\ \frac{1}{2^{s-k_{\text{aux}}}} - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$

where in the second equality we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$ which implies that both events are independent. Furthermore, we also used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{0}$ according to Equation (38). Therefore, in that case

$$\text{Cov}^{(1)} \leqslant \frac{1}{2^{k+s-k_{\text{aux}}}} \tag{41}$$

Sub-case iv. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. In that case,

$$\text{Cov}^{(1)} = \frac{1}{2^{2k}}\ \mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\text{aux}}, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \frac{1}{2^{2k}}\mathbb{P}_{\mathbf{H}_{\text{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\text{aux}}\right) - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= \frac{1}{2^{2k+s-k_{\text{aux}}}} - \frac{1}{2^{2k+s-k_{\text{aux}}}}$$
$$= 0$$

where in the second equality we used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$ which implies that both events are independent. Furthermore, we also used that $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{0}$ according to Equation (38).

Sub-case v. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. This subcase is impossible according to Equation (38). Therefore,

$$\mathrm{Cov}^{(1)} = 0$$

Sub-case vi. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. In that case we can write

$$\begin{aligned}
\mathrm{Cov}^{(0)} &= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k+s-k_{\mathrm{aux}}}} \\
&= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k+s-k_{\mathrm{aux}}}} \\
&= \frac{1}{2^{2k+s-k_{\mathrm{aux}}}} - \frac{1}{2^{2k+s-k_{\mathrm{aux}}}}
\end{aligned}$$

Therefore we obtain,

$$\mathrm{Cov}^{(1)} = 0.$$

Case 3: This situation is symmetric to Case 2.

Case 4: Recall that in this case we have

$$\mathbf{h}^0_{\mathscr{P}} = \mathbf{e}'_0 \quad \text{and} \quad \mathbf{h}^1_{\mathscr{P}} = \mathbf{e}'_1 \tag{42}$$

We have,

$$\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\right)\mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) = \frac{1}{2^{2k}}$$

Let us compute $\mathbb{E}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right)$ when $(\mathbf{e}'_0,\mathbf{h}^0) \neq (\mathbf{e}'_1,\mathbf{h}^1)$. By definition

$$\begin{aligned}
\mathbb{E}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) &= \mathbb{P}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp, \mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) \\
&= \mathbb{P}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp\right)\mathbb{P}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right)
\end{aligned}$$

Therefore,

$$\begin{aligned}
\sum_{\mathbf{e}'_0,\mathbf{e}'_1} F_3 &= \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_3^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathbb{E}\left(\mathbf{1}_{\mathbf{e}'_0,\mathbf{h}^0}\,\mathbf{1}_{\mathbf{e}'_1,\mathbf{h}^1}\right) - \frac{1}{2^{2k}} \\
&= \sum_{\mathbf{e}'_0,\mathbf{e}'_1} \sum_{\substack{\mathbf{h}^0,\mathbf{h}^1 \in \mathscr{F}_3^{\mathbf{e}'_0,\mathbf{e}'_1} \\ (\mathbf{e}'_0,\mathbf{h}^0)\neq(\mathbf{e}'_1,\mathbf{h}^1)}} \mathrm{Cov}^{(3)}
\end{aligned} \tag{43}$$

where,

$$\mathrm{Cov}^{(3)} \stackrel{\mathrm{def}}{=} \mathbb{P}_{\mathbf{H}}\left(\mathbf{h}^0,\mathbf{h}^1 \in \mathcal{C}^\perp\right)\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k}}$$

Our aim now it to upper-bound $\mathrm{Cov}^{(1)}$ according to the above 6 sub-cases.

Sub-case i. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. We have

$$\begin{aligned}
\mathrm{Cov}^{(3)} &= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}, \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1 \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k}} \\
&= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{0} \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k}} \\
&= \frac{1}{2^{2k}} - \frac{1}{2^{2k}}
\end{aligned}$$

where in the second equality we used Equation (42). Therefore, in that case

$$\mathrm{Cov}^{(3)} = 0.$$

Sub-case ii. Suppose that $\mathbf{e}'_0 = \mathbf{e}'_1, \mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$. According to Equation (42) this sub-case is impossible. Therefore,

$$\mathrm{Cov}^{(3)} = 0.$$

Sub-case iii. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 = \mathbf{h}^1$. According to Equation (42) this sub-case is impossible. Therefore,

$$\mathrm{Cov}^{(3)} = 0.$$

Sub-case iv. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$ and $\mathbf{h}^0_{\mathscr{P}} = \mathbf{h}^1_{\mathscr{P}}$. According to Equation (42) this sub-case is impossible. Therefore,

$$\mathrm{Cov}^{(3)} = 0.$$

Sub-case v. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 = \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. We have

$$\begin{aligned}
\mathrm{Cov}^{(3)} &= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k}} \\
&= \frac{1}{2^{2k}}\,\mathbb{P}_{\mathbf{H}_{\mathrm{aux}}}\left(\mathbf{0} \in \mathcal{C}_{\mathrm{aux}}\right) - \frac{1}{2^{2k}} \\
&= \frac{1}{2^{2k}} - \frac{1}{2^{2k}}
\end{aligned}$$

where in the second equality we used Equation (42). Therefore,

$$\mathrm{Cov}^{(3)} = 0$$

Sub-case vi. Suppose that $\mathbf{e}'_0 \neq \mathbf{e}'_1$, $\mathbf{h}^0 \neq \mathbf{h}^1$, $\mathbf{h}^0_{\mathscr{P}} \neq \mathbf{h}^1_{\mathscr{P}}$ and $\mathbf{h}^0_{\mathscr{P}} + \mathbf{e}'_0 \neq \mathbf{h}^1_{\mathscr{P}} + \mathbf{e}'_1$. According to Equation (42) this sub-case is impossible. Therefore,

$$\mathrm{Cov}^{(3)} = 0.$$

We are now ready to gather Cases 1, 2, 3 and 4 according to Subcases i, ii, iii, iv, v and vi. Our aim is to bound Cov that were defined in Equation 33. We can already notice that Case 4 has no impact on this sum while Cases 2 and 3 have an influence only in Subcase iii. Furthermore, ii, iv and vi have no contribution to this sum, whatever is the considered case.

Let us upper-bound Cov according to the different subcases where Cov_i denotes the terms involved in Cov coming from Subcase i (in particular Cov_i is defined as a certain sum of $\mathrm{Cov}^{(i)}$, see Equations (35), (39) and (36)).

Subcase i: We have,

$$\mathrm{Cov}_1 \leqslant \sum_{(\mathbf{e}'_0,\mathbf{h}^0)\in\mathcal{E}_b} \sum_{\substack{\mathbf{h}^1:(\mathbf{e}'_0,\mathbf{h}^1)\in\mathcal{E}_b \\ \mathbf{h}^1\neq\mathbf{h}^0,\mathbf{h}^0_{\mathscr{P}}=\mathbf{h}^1_{\mathscr{P}}}} \frac{1}{2^{2k}}\frac{1}{2^{s-k_{\mathrm{aux}}}} \leqslant \sum_{(\mathbf{e}_0,\mathbf{h}^0)\in\mathcal{E}_b} \frac{\binom{n-s}{w}}{2^{2k+s-k_{\mathrm{aux}}}} = \frac{\binom{n-s}{w}}{2^k}\frac{E'_b}{2^{k+s-k_{\mathrm{aux}}}}$$

Subcase ii: We have,

$$\mathrm{Cov}_2 = 0.$$

Subcase iii: We have here to split the computation here between Cases 1 and 2. Recall that they are given by

$$\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1} = \left\{(\mathbf{h}^0,\mathbf{h}^1) :\ \mathbf{h}^0 \in \mathscr{E}_{b,1}^{\mathbf{e}'_0} \text{ and } \mathbf{h}^1 \in \mathscr{E}_{b,1}^{\mathbf{e}'_1}\right\},$$

$$\mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1} = \left\{(\mathbf{h}^0,\mathbf{h}^1) :\ \mathbf{h}^0 \in \mathscr{E}_{b,2}^{\mathbf{e}'_0} \text{ and } \mathbf{h}^1 \in \mathscr{E}_{b,1}^{\mathbf{e}'_1}\right\}$$

where,

$$\mathscr{E}_{b,1}^{\mathbf{e}'} \stackrel{\text{def}}{=} \left\{\mathbf{h} \in \mathbb{F}_2^n :\ (\mathbf{e}',\mathbf{h}) \in \mathscr{E}_b \text{ and } \mathbf{h}_{\mathscr{P}} \neq \mathbf{e}'\right\},$$

$$\mathscr{E}_{b,2}^{\mathbf{e}'} \stackrel{\text{def}}{=} \left\{\mathbf{h} \in \mathbb{F}_2^n :\ (\mathbf{e}',\mathbf{h}) \in \mathscr{E}_b \text{ and } \mathbf{h}_{\mathscr{P}} = \mathbf{e}'\right\}.$$

But recall according to Equation (30) that,

$$|\mathscr{E}_{b,1}| = \frac{|\mathscr{E}_{b,2}|}{2^s}$$

Therefore, in Subcase iii,

$$\begin{aligned}
\mathrm{Cov}_3 &= \sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}} \mathrm{Cov}^{(0)} + 2\sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1}} \mathrm{Cov}^{(1)} \\
&= \sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}} \frac{1}{2^{k+2s-2k_{\mathrm{aux}}}} + 2\sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_1^{\mathbf{e}'_0,\mathbf{e}'_1}} \frac{1}{2^{k+s-k_{\mathrm{aux}}}} \quad \text{(Equations (37)) and (41)} \\
&= \sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}} \frac{1}{2^{k+2s-2k_{\mathrm{aux}}}} + \frac{1}{2^s}\sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}} \frac{1}{2^{k+s-k_{\mathrm{aux}}}} \\
&= \mathcal{O}(1)\sum_{\mathbf{e}'_0\neq\mathbf{e}'_1}\sum_{\mathbf{h}^0=\mathbf{h}^1\in\mathscr{F}_0^{\mathbf{e}'_0,\mathbf{e}'_1}} \frac{1}{2^{k+2s-2k_{\mathrm{aux}}}}
\end{aligned}$$

where we basically use the same reasoning than for proving Equation (31). There in this subcase,

$$\mathrm{Cov}_3 \leqslant \sum_{(\mathbf{e}'_0,\mathbf{h}^0)\in\mathcal{E}_b}\sum_{\substack{(\mathbf{e}'_1,\mathbf{h}^0)\in\mathcal{E}_b\\ \mathbf{h}^1=\mathbf{h}^0,\mathbf{e}'_0\neq\mathbf{e}'_1}} \frac{1}{2^{k+2s-2k_{\mathrm{aux}}}} \leqslant \sum_{(\mathbf{e}'_0,\mathbf{h}^0)\in\mathcal{E}_b} \frac{\binom{s}{t_{\mathrm{aux}}}}{2^{k+2s-2k_{\mathrm{aux}}}} = \frac{\binom{s}{t_{\mathrm{aux}}}}{2^{s-k_{\mathrm{aux}}}}\,\frac{E'_b}{2^{k+s-k_{\mathrm{aux}}}}$$

Subcase iv: We have,

$$\mathrm{Cov}_4 = 0.$$

Subcase v: We have,

$$\begin{aligned}
\mathrm{Cov}_5 &\leqslant \sum_{(\mathbf{e}'_0,\mathbf{h}^0)\in\mathcal{E}_b}\sum_{\substack{(\mathbf{e}'_1,\mathbf{h}^1)\in\mathcal{E}_b\\ \mathbf{h}^1\neq\mathbf{h}^0,\ \mathbf{h}^0_{\mathscr{P}}\neq\mathbf{h}^1_{\mathscr{P}},\ \mathbf{e}'_0\neq\mathbf{e}'_1\\ \mathbf{e}'_0+\mathbf{h}^0_{\mathscr{P}}=\mathbf{e}'_1+\mathbf{h}^1_{\mathscr{P}}}} \frac{1}{2^{2k+s-k_{\mathrm{aux}}}} \leqslant \sum_{(\mathbf{e}_0,\mathbf{h}^0)\in\mathcal{E}_b} \frac{\binom{s}{t_{\mathrm{aux}}}\binom{n-s}{w}}{2^{2k+s-k_{\mathrm{aux}}}} \\
&= \frac{\binom{n-s}{w}\binom{s}{t_{\mathrm{aux}}}}{2^k}\,\frac{E'_b}{2^{k+s-k_{\mathrm{aux}}}}
\end{aligned}$$

Subcase vi: We have,

$$\mathrm{Cov}_6 = 0.$$

Plugging all these bounds on the Cov_i together and using that $\mathrm{Cov} = \sum_i \mathrm{Cov}_i$ leads to

$$\begin{aligned}
\mathrm{Cov} &\leqslant \left(\frac{\binom{n-s}{w}}{2^k} + \frac{\binom{s}{t_{\mathrm{aux}}}}{2^{s-k_{\mathrm{aux}}}} + \frac{\binom{n-s}{w}\binom{s}{t_{\mathrm{aux}}}}{2^k}\right)\frac{E'_b}{2^{k+s-k_{\mathrm{aux}}}} \\
&= \mathcal{O}(n^\alpha)\,\frac{E'_b}{2^{k+s-k_{\mathrm{aux}}}}
\end{aligned}$$

where in the last lines we used the constraints (22) given in the proposition. Plugging this equation in Equation (32) concludes the proof. □

We are now ready to prove our proposition:

Proof of Proposition 2. Let E_b and E'_b (for $b \in \{0,1\}$) be defined as in Lemma 2. By using the Bienaymé-Tchebychev inequality, we obtain for any function f mapping the positive integers to positive real numbers:

$$\mathbb{P}_{\mathbf{H},\mathbf{H}_{\mathrm{aux}}}\left(|E_b - \mathbb{E}\left(E_b\right)| \geqslant \sqrt{f(n)\mathbb{E}\left(E_b\right)}\right) \leqslant \frac{\mathbf{Var}(E_b)}{f(n)\mathbb{E}(E_b)} = \frac{\mathcal{O}(n^\alpha)}{f(n)}$$

where the last inequality is a consequence of Lemma 2. Since,

$$\underset{(\mathbf{h},\mathbf{c}_{\mathrm{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\mathrm{bias}}\left(\langle \mathbf{c}_{\mathrm{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) = \frac{E_0 - E_1}{E_0 + E_1},$$

we have with probability greater than $1 - \frac{\mathcal{O}(n^\alpha)}{f(n)}$ that

$$\frac{\mu_0 - \mu_1 - \sqrt{2f(n)}\sqrt{\mu_0+\mu_1}}{\mu_0+\mu_1+\sqrt{2f(n)}\sqrt{\mu_0+\mu_1}} \leqslant \underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) \leqslant \frac{\mu_0 - \mu_1 + \sqrt{2f(n)}\sqrt{\mu_0+\mu_1}}{\mu_0+\mu_1-\sqrt{2f(n)}\sqrt{\mu_0+\mu_1}} \quad (44)$$

where

$$\mu_i \overset{\text{def}}{=} \mathbb{E}\left(E_i\right)$$

and where we used that for all positive x and y, $\sqrt{x}+\sqrt{y} \leqslant \sqrt{2(x+y)}$. Let,

$$N = \mu_0 + \mu_1$$

It is readily seen that,

$$N = \frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}}$$

We let $f(n) = \delta\sqrt{N}/2$. Since $N = \mu_0 + \mu_1$ this implies $f(n) = \delta\sqrt{\mu_0+\mu_1}/2$. By Equation (7), note that $\frac{f(n)}{\mathcal{O}(n^\alpha)}$ tends to infinity as n tends to infinity. We notice that

$$\begin{aligned}\sqrt{2f(n)}\sqrt{\mu_0+\mu_1} &= \delta^{1/2}(\mu_0+\mu_1)^{3/4} \\ &= o\left(\delta(\mu_0+\mu_1)\right)\end{aligned}$$

because

$$\frac{\delta^{1/2}(\mu_0+\mu_1)^{3/4}}{\delta(\mu_0+\mu_1)} = \frac{1}{\sqrt{\delta\sqrt{\mu_0+\mu_1}}} = \frac{1}{\sqrt{2f(n)}} \underset{n\to+\infty}{\longrightarrow} 0.$$

Equation (44) can now be rewritten as

$$\frac{\mu_0 - \mu_1 - o\left(\delta(\mu_0+\mu_1)\right)}{\mu_0+\mu_1+o\left(\delta(\mu_0+\mu_1)\right)} \leqslant \text{bias}\left(\langle \mathbf{e}'', \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) \leqslant \frac{\mu_0 - \mu_1 + o\left(\delta(\mu_0+\mu_1)\right)}{\mu_0+\mu_1-o\left(\delta(\mu_0+\mu_1)\right)} \quad (45)$$

Now on the other hand

$$\begin{aligned}\delta &= \underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) \\ &= \frac{E'_0 - E'_1}{E'_0 + E'_1} \\ &= \frac{\frac{E'_0}{2^{k+s-k_{\text{aux}}}} - \frac{E'_1}{2^{k+s-k_{\text{aux}}}}}{\frac{E'_0}{2^{k+s-k_{\text{aux}}}} + \frac{E'_1}{2^{k+s-k_{\text{aux}}}}} \\ &= \frac{\mu_0 - \mu_1}{\mu_0+\mu_1}\end{aligned}$$

where the last equality is a consequence of Lemma 2, in particular Equation (23). From this it follows that we can rewrite (45) as

$$\frac{\delta}{1+o(\delta)} - o(\delta) \leqslant \underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) \leqslant \frac{\delta}{1-o(\delta)} + o(\delta)$$

from which it follows immediately that

$$\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) = \delta(1+o(1))$$

which concludes the proof. □

Appendix B. Correctness and Running-Time of the double-RLPN algorithm (Algorithm 4)

In this section we prove the correctness of Algorithm 4 in Subsection B.1. Furthermore, we give its running-time in Subsection B.2. To this aim, we instantiate Instructions 1 (ParityCheckEquations) 1 (Decode) of Algorithm 1.

Notation 3.
- *Instantiation of Algorithm 4.*
  - *We instantiate ParityCheckEquations instruction with the technique devised in [CDMT22, §5] to compute all the parity-checks of a given weight in a code (which is inspired from [BJMM12]). Its asymptotic complexity is recalled in Proposition 11.*
  - *The family of auxiliary $[s, k_{\mathrm{aux}}]$ linear codes $\mathcal{C}_{\mathrm{aux}}$ used will be product of $\log s$ random codes as devised in Section 7 . Using these the Decode procedure outputs almost all codeword at distance t_{aux} in time $2^{o(s)} \max\left(\frac{\binom{s}{t_{\mathrm{aux}}}}{2^{s-k_{\mathrm{aux}}}}, 1\right)$.*
- *Framework for the analysis of Algorithm 4*
  - *We prove the correctness (Proposition 8) and we make the complexity analysis (Proposition 9) in the framework of Proposition 5. More specifically, analysis is made for $\mathcal{C}$ and $\mathcal{C}_{\mathrm{aux}}$ being random $[n, k]$ and $[s, k]_{\mathrm{aux}}$ codes. We argue in Section 7 that the proof would be roughly the same (but more complicated) if we were to make it using $\mathcal{C}_{\mathrm{aux}}$ being random product codes. The complexity of Algorithm 4 would only grow by a factor of $2^{o(s)}$ when using these codes.*
  - *Note that with the ParityCheckEquations and Decode procedures we have chosen, Algorithm 4 computes in fact all the possible LPN samples, namely we have (as required in Proposition 5):*
$$\mathscr{H} = \widetilde{\mathscr{H}}$$
  - *We reuse notation introduced in Proposition 5: the set $\mathscr{S}^{(j)}$ of candidates for the j'th auxiliary code $\mathcal{C}_{\mathrm{aux}}^{(j)}$ is defined by*
$$\mathscr{S}^{(j)} \stackrel{def}{=} \{\mathbf{s} \in \mathbb{F}_2^{k_{\mathrm{aux}}} : \widehat{f_{\mathbf{y},\widetilde{\mathscr{H}},\mathbf{G}_{\mathrm{aux}}^{(j)}}}(\mathbf{s}) \geqslant \frac{\delta}{2}\widetilde{H}\}, \tag{46}$$
where
$$\widetilde{H} \stackrel{def}{=} \frac{\binom{n-s}{w}\binom{s}{t_{\mathrm{aux}}}}{2^{k-k_{\mathrm{aux}}}}, \qquad \delta \stackrel{def}{=} \frac{K_w^{(n-s)}(u)\, K_{t_{\mathrm{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\mathrm{aux}}}}. \tag{47}$$

B.1. **Correctness of the algorithm.** The goal of this section is to prove that double-RLPN, namely Algorithm 4, outputs the desired error vector $\mathbf{e}$ after essentially $N_{\mathrm{iter}} \approx \frac{\binom{n}{t}}{\binom{s}{t-u}\binom{n-s}{u}}$ iterations of the outer loop (Line (2) of Algorithm 4). This is given by the following proposition.

Proposition 8. *Let $\mathcal{C}$ be a code taken uniformly at random among the $[n, k]$ linear codes and $\mathcal{C}_{\mathrm{aux}}^{(1)}, \ldots, \mathcal{C}_{\mathrm{aux}}^{(N_{\mathrm{aux}})}$ which are N_{aux} codes taken uniformly at random among the $[s, k_{\mathrm{aux}}]$ linear codes. Let $\mathbf{y} \stackrel{def}{=} \mathbf{c} + \mathbf{e}$ where $\mathbf{c} \in \mathcal{C}$ and where $\mathbf{e} \in \mathcal{S}_t^n$ is a fixed error vector of weight t. As long as the parameters $s, k_{\mathrm{aux}}, t_{\mathrm{aux}}, w, u$ verify the Parameters constraint (1) and as long as $N_{\mathrm{iter}} = \omega\left(\frac{\binom{n}{t}}{\binom{s}{t-u}\binom{n-s}{u}}\right)$ and $N_{\mathrm{aux}} = \mathcal{O}(1)$, Algorithm 4 outputs the error vector $\mathbf{e}$ with probability $1 - o(1)$.*

It is readily seen that when $N_{\mathrm{iter}} = \omega\left(\frac{\binom{n}{t}}{\binom{s}{t-u}\binom{n-s}{u}}\right)$ then, with probability $1 - o(1)$ over the choice of $\mathscr{P}$ there exists an iteration such that $|\mathbf{e}_{\mathscr{N}}| = u$. We only have left to show that for such an iteration we have with high probability that $\mathbf{e}_{\mathscr{P}}\left(\mathbf{G}_{\mathrm{aux}}^{(j)}\right)^{\top} \in \mathscr{S}^{(j)}$ for $j = 1, \ldots, N_{\mathrm{aux}}$ which is the purpose of the following lemma.

Lemma 3. *Let us reuse the setting of Proposition 8. Moreover, let us fix $\mathscr{P}$ and $\mathscr{N}$ two complementary sets of $[\![1, n]\!]$ of size s and $n - s$ respectively and such that $|\mathbf{e}_{\mathscr{N}}| = u$. Let us*

denote by $\mathbf{G}_{\text{aux}}^{(1)}, \ldots, \mathbf{G}_{\text{aux}}^{(N_{\text{aux}})}$ *the generators matrices of the codes* $\mathcal{C}_{\text{aux}}^{(1)}, \ldots, \mathcal{C}_{\text{aux}}^{(N_{\text{aux}})}$ *respectively. Then,*

$$\mathbb{P}\left(\bigcap_{j=1}^{N_{\text{aux}}} \text{“}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \in \mathscr{S}^{(j)}\text{”}\right) = 1 - o(1). \tag{48}$$

Proof. First, notice that

$$\begin{aligned}\mathbb{P}\left(\bigcap_{j=1}^{N_{\text{aux}}} \text{“}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \in \mathscr{S}^{(j)}\text{”}\right) &= 1 - \mathbb{P}\left(\bigcup_{j=1}^{N_{\text{aux}}} \text{“}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \notin \mathscr{S}^{(j)}\text{”}\right) \\ &\geqslant 1 - \sum_{j=1}^{N_{\text{aux}}} \mathbb{P}\left(\text{“}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \notin \mathscr{S}^{(j)}\text{”}\right)\end{aligned}$$

where we used the union-bound. Now, as $N_{\text{aux}} = \mathcal{O}(1)$ we only have to show that $\mathbb{P}\left(\text{“}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \notin \mathscr{S}^{(j)}\text{”}\right) = o(1)$ to prove Equation (48). By using Fact 4,

$$\text{”}\mathbf{e}_{\mathscr{P}}\, \mathbf{G}_{\text{aux}}^{(j)\intercal} \notin \mathscr{S}^{(j)}\text{”} \iff \underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}}{\text{bias}}(\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}}\rangle) < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}$$

Our aim is to show,

$$\mathbb{P}\left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}}{\text{bias}}(\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}}\rangle) < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right) = o(1).$$

To simplify notation let $b \stackrel{\text{def}}{=} \text{bias}_{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}}(\langle \mathbf{y}, \mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{c}_{\text{aux}}\rangle)$. It is readily seen that $\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(\left|\widetilde{\mathscr{H}}\right|\right) = \widetilde{H}\,(1 + o(1))$ and $\mathbf{Var}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(\left|\widetilde{\mathscr{H}}\right|\right) \leqslant \widetilde{H}(1 + o(1))$. Therefore, by using Bienaymé-Tchebychev inequality, for any a,

$$\mathbb{P}\left(\left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| \geqslant \sqrt{a\widetilde{H}}\right) \leqslant \frac{1 + o(1)}{a}$$

We have the following computation,

$$\begin{aligned}\mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right) &= \mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|} \mid \left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| \geqslant \sqrt{a\widetilde{H}}\right)\mathbb{P}\left(\left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| \geqslant \sqrt{a\widetilde{H}}\right) \\ &\quad + \mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|} \mid \left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| < \sqrt{a\widetilde{H}}\right)\mathbb{P}\left(\left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| < \sqrt{a\widetilde{H}}\right)\end{aligned}$$

Therefore,

$$\begin{aligned}\mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right) &\leqslant \mathbb{P}\left(\left|\left|\widetilde{\mathscr{H}}\right| - (1 + o(1))\widetilde{H}\right| \geqslant \sqrt{a\widetilde{H}}\right) + \mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{(1 + o(1))\widetilde{H} - \sqrt{a\widetilde{H}}}\right) \\ &\leqslant \frac{1 + o(1)}{a} + \mathbb{P}\left(b < \frac{\delta}{2}\frac{1}{(1 + o(1)) - \sqrt{\frac{a}{\widetilde{H}}}}\right)\end{aligned}$$

Let us choose $a = \widetilde{H}^{1/2}$. Recall that $\widetilde{H} = \omega\left(\frac{n^{\alpha+8}}{\delta^2}\right)$ where $\delta \leqslant 1$. Therefore,

$$\begin{aligned}\mathbb{P}\left(b < \frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right) &= o(1) + \mathbb{P}\left(b < \frac{\delta}{2}(1 + o(1))\right) \\ &= o(1)\end{aligned}$$

where in the last equality we used Proposition 7. It concludes the proof. □

B.2. **Asymptotic complexity of** double-RLPN**.** We now have every tool to give the complexity of our algorithm, namely, we can compute the expected number of candidates at each iteration given by Proposition 5 and we have the correctness of our algorithm which is given by Proposition 8.

Proposition 9. *Asymptotic complexity exponent of the* double-RLPN *algorithm. Define*

$$R \stackrel{def}{=} \lim_{n\to\infty} \frac{k}{n}, \quad \tau \stackrel{def}{=} \lim_{n\to\infty} \frac{t}{n}, \quad \sigma \stackrel{def}{=} \lim_{n\to\infty} \frac{s}{n}, \quad R_{\text{aux}} \stackrel{def}{=} \lim_{n\to\infty} \frac{k_{\text{aux}}}{n}$$
$$\tau_{\text{aux}} \stackrel{def}{=} \lim_{n\to\infty} \frac{t_{\text{aux}}}{n}, \omega \stackrel{def}{=} \lim_{n\to\infty} \frac{w}{n}, \quad \mu \stackrel{def}{=} \lim_{n\to\infty} \frac{u}{n}$$

Suppose that de DECODE *procedure has an expected time complexity of* $2^{n\cdot\sigma\cdot o(1)}$*. The expected complexity of the* double-RLPN *algorithm to decode a code of rate* R *at relative distance* τ *is upper bounded by* $2^{n\,(\alpha_{\text{double-RLPN}}+o(1))}$ *where*

$$\alpha_{\text{double-RLPN}} \leqslant -\pi + \max\left((1-\sigma)\cdot\alpha_{\text{eq}}\left(\frac{R-\sigma}{1-\sigma}, \frac{\omega}{1-\sigma}\right),\ \nu_{\text{sample}},\ R_{\text{aux}},\ \nu_{\text{candidate}}\cdot N_{\text{aux}} + \alpha_{\text{ISD}}\right)$$

where

$$\begin{aligned}
\pi &\stackrel{def}{=} h(\tau) - \sigma\cdot h_2\left(\frac{\tau-\mu}{\sigma}\right) - (1-\sigma)\cdot h\left(\frac{\mu}{1-\sigma}\right),\\
\nu_{\text{samples}} &\stackrel{def}{=} (1-\sigma)\cdot h_2\left(\frac{\omega}{1-\sigma}\right) + \sigma\cdot h_2\left(\frac{\tau_{\text{aux}}}{\sigma}\right) - (R - R_{\text{aux}}),\\
\alpha_{\text{ISD}} &\stackrel{def}{=} \max\left(\sigma\cdot\alpha_{\text{ISD-Dumer}}\left(1 - \frac{N_{\text{aux}}\cdot\tau_{\text{aux}}}{\sigma}, \frac{\tau-\mu}{\sigma}\right), \nu_{\text{ISD}} + (1-\sigma)\cdot\alpha_{\text{ISD-Dumer}}\left(\frac{R-\sigma}{1-\sigma}, \frac{\mu}{1-\sigma}\right)\right),\\
\nu_{\text{ISD}} &\stackrel{def}{=} \max\left(\sigma\cdot h_2\left(\frac{\tau-\mu}{\sigma}\right) - N_{\text{aux}}\cdot\tau_{\text{aux}},\ 0\right)\\
\nu_{\text{candidates}} &\stackrel{def}{=} \max\left(\max_{(\eta,\zeta)\in\mathcal{A}} \sigma\cdot h_2\left(\frac{\zeta}{\sigma}\right) + (1-\sigma)\cdot h_2\left(\frac{\eta}{1-\sigma}\right) - (1-R),\ 0\right),
\end{aligned}$$

with

$$\mathcal{A} \stackrel{def}{=} \left\{(\eta,\zeta)\in[0,1-\sigma]\times[0,\sigma] \ : \sigma\left[\widetilde{\kappa}\left(\frac{t_{\text{aux}}}{\sigma}, \frac{\tau-\mu}{\sigma}\right) - \widetilde{\kappa}\left(\frac{t_{\text{aux}}}{\sigma}, \frac{\zeta}{\sigma}\right)\right] + (1-\sigma)\left[\widetilde{\kappa}\left(\frac{\omega}{1-\sigma}, \frac{\mu}{1-\sigma}\right) - \widetilde{\kappa}\left(\frac{\omega}{1-\sigma}, \frac{\eta}{1-\sigma}\right)\right] \leqslant 0\right\},$$

and

- $\alpha_{\text{eq}}(R',\tau')$ *is the complexity exponent of* PARITYCHECKEQUATIONS *to compute all parity-checks of relative weight* τ' *of a code of rate* R'*. It is instantiated here with a technique devised in* [CDMT22, §5 Eq. (5.4)] *and its complexity is recalled in Proposition 11.*
- $\alpha_{\text{ISD-Dumer}}(R',\tau')$ *is the complexity exponent of* DECODE-DUMER *to return all the solutions to the decoding problem in a code of rate* R' *at relative distance* τ'*. Its complexity is recalled in Proposition 10.*

Moreover, σ*,* R_{aux}*,* τ_{aux}*,* ω*,* μ*, are non-negative and such that*

$$\sigma \leqslant R, \quad \tau - \sigma \leqslant \mu \leqslant \tau, \quad \omega \leqslant 1-\sigma,$$

$$\nu_{\text{samples}} \geqslant -2\,\varepsilon_{\text{bias}}, \tag{49}$$

$$0 \geqslant (1-\sigma)\,h_2\left(\frac{\omega}{1-\sigma}\right) + \sigma h_2\left(\frac{\tau_{\text{aux}}}{\sigma}\right) - R \tag{50}$$

$$0 \geqslant \sigma\,h_2\left(\frac{\tau_{\text{aux}}}{\sigma}\right) - (\sigma - R_{\text{aux}}) \tag{51}$$

where $\widetilde{\kappa}$ is the function defined in Proposition 1 and

$$\varepsilon_{\text{bias}} \stackrel{def}{=} \sigma \left[\widetilde{\kappa}\left(\frac{t_{\text{aux}}}{\sigma}, \frac{\tau-\mu}{\sigma}\right) - h_2\left(\frac{\tau_{\text{aux}}}{\sigma}\right)\right] + (1-\sigma)\left[\widetilde{\kappa}\left(\frac{\omega}{1-\sigma}, \frac{\mu}{1-\sigma}\right) - h_2\left(\frac{\omega}{1-\sigma}\right)\right].$$

Finally, we require that $N_{\text{aux}} = \mathcal{O}(1)$.

Remark 5. *In practice our parameters are such that we decode the auxiliary code at Gilbert-Varshamov distance, namely $\tau_{\text{aux}} = \sigma\, h_2^{-1}(1 - R_{\text{aux}})$.*

While initially Dumer's decoder [Dum91] is designed to produce only one solution to the decoding problem it suffices to re-run it as many time as the number of solutions we expect from the decoding problem to find all of them. We get the following proposition giving the asymptotic complexity of the DECODE-DUMER procedure.

Proposition 10 (Asymptotic time complexity of ISD Decoder [Dum91] to produce **all** solutions to the decoding problem)**.** *Let $R \stackrel{def}{=} \lim_{n\to\infty} \frac{k}{n}, \tau \stackrel{def}{=} \lim_{n\to\infty} \frac{t}{n}$. Let ℓ and w be two (implicit) parameters of the algorithm and define $\lambda \stackrel{def}{=} \lim_{n\to\infty} \frac{\ell}{n}, \omega \stackrel{def}{=} \lim_{n\to\infty} \frac{w}{n}$. The time and space complexities of* [Dum91] *to find a proportion $1 - o(1)$ of all solutions to the decoding problem at distance t on an $[n, k]$ linear code are given by $2^{n\,(\alpha_{\text{ISD-Dumer}}+o(1))}$ and $2^{n\,(\beta_{\text{ISD-Dumer}}+o(1))}$ respectively where*

$$\alpha_{\text{ISD-Dumer}} \stackrel{def}{=} \min_{\omega,\lambda}\left(\pi + \max\left(\frac{R+\lambda}{2} h_2\left(\frac{\omega}{R+\lambda}\right), (R+\lambda)\, h_2\left(\frac{\omega}{R+\lambda}\right) - \lambda\right)\right), \tag{52}$$

$$\pi \stackrel{def}{=} h_2(\tau) - (1-R-\lambda) h_2\left(\frac{\tau-\omega}{1-R-\lambda}\right) - (R+\lambda) h_2\left(\frac{\omega}{R+\lambda}\right), \tag{53}$$

$$\nu_{\text{sol}} \stackrel{def}{=} \max\left(h_2(\tau) - (1-R), 0\right), \tag{54}$$

$$\beta_{\text{ISD-Dumer}} \stackrel{def}{=} \frac{R+\lambda}{2} h_2\left(\frac{\omega}{R+\lambda}\right). \tag{55}$$

Moreover λ and ω must verify the following constraints:

$$0 \leqslant \lambda \leqslant 1-R, \qquad \max\left(R+\lambda+\tau-1, 0\right) \leqslant \omega \leqslant \min\left(\tau, R+\lambda\right).$$

The expected number of solutions is given by $2^{n\,(\nu_{\text{sol}}+o(1))}$.

We recall here the asymptotic complexity of the technique devised in [CDMT22, §5, Equation (5.4)] based on [BJMM12] decoder to produce all parity-checks of low weight of a code.

Proposition 11. *Asymptotic time complexity exponent of BJMM technique* [BJMM12], [CDMT22, §5, Equation (5.4)] *to produce all parity-checks of relative weight ω of a code of rate R*

$$\alpha_{BJMM}(R,\omega) \stackrel{def}{=} \min_{\pi_1,\pi_2,\lambda_1,\lambda_2} \gamma \tag{56}$$

where

$$\gamma \stackrel{def}{=} \max(\gamma_1, \gamma_2, \gamma_3)$$

$$\gamma_1 \stackrel{def}{=} \max\left(\nu_0,\, 2\,\nu_0 - \lambda_1\right), \quad \gamma_2 \stackrel{def}{=} \max\left(\nu_1,\, 2\,\nu_1 - (\lambda_2 - \lambda_1)\right), \quad \gamma_3 \stackrel{def}{=} \max\left(\nu_2,\, 2\,\nu_2 - (\lambda - \lambda_2)\right)$$

$$\nu_0 \stackrel{def}{=} \frac{h(\pi_1)}{2}, \quad \nu_1 \stackrel{def}{=} h(\pi_1) - \lambda_1, \quad \nu_2 \stackrel{def}{=} h(\pi_2) - \lambda_2, \quad \nu_3 \stackrel{def}{=} h(\omega) - \lambda.$$

and the constraint region $\mathscr{R}$ is defined by the sub-region of nonnegative tuples $(\pi_1, \pi_2, \lambda_1, \lambda_2)$ such that

$$\lambda_1 \leqslant \lambda_2 \leqslant \lambda, \quad \pi_1 \leqslant \pi_2 \leqslant \pi, \quad \pi_2 \leqslant 2\pi_1, \quad \pi \leqslant 2\pi_2, \quad \pi_2 \leqslant \lambda_1, \quad \pi \leqslant \lambda_2,$$

and

$$\lambda_1 = \pi_2 + (1-\pi_2) h\left(\frac{\pi_1 - \pi_2/2}{1-\pi_2}\right), \tag{57}$$

$$\lambda_2 = \omega + (1-\omega) h\left(\frac{\pi_2 - \omega/2}{1-\omega}\right) \tag{58}$$

The expected number of parity-checks computed is given by $2^{n\,(\nu_3+o(1))}$

Appendix C. Proof of Proposition 4

Let us recall Proposition 4.

Proposition 4. *Let $\mathscr{P}$ and $\mathscr{N}$ be two complementary subsets of $[\![1,n]\!]$ of size s and $n-s$ respectively. Let $\mathcal{C}$ be an $[n,k]$-code such that $\mathcal{C}_{\mathscr{P}}$ is of dimension s and let $\mathcal{C}_{\rm aux}$ be an $[s,k_{\rm aux}]$-code. We have for any $\mathbf{x}\in\mathbb{F}_2^s$*

$$\underset{(\mathbf{h},\mathbf{c}_{\rm aux})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\rm bias}(\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\rm aux}\rangle)=\frac{1}{2^{k-k_{\rm aux}}}\frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{i=0}^{n-s}\sum_{j=0}^{s}N_{i,j}K_w^{(n-s)}(i)\,K_{t_{\rm aux}}^{(s)}(j)\tag{10}$$

where

$$\begin{aligned}N_{i,j}&\overset{def}{=}\left|\left\{\left(\mathbf{r},\mathbf{c}^{\mathscr{N}}\right)\in(\mathbf{x}+\mathcal{C}_{\rm aux}^{\perp})\times\mathcal{C}^{\mathscr{N}}\,:|\mathbf{r}|=j\text{ and }\left|(\mathbf{r}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathbf{c}^{\mathscr{N}}\right|=i\right\}\right|,\\ \widetilde{\mathscr{H}}&=\{(\mathbf{h},\mathbf{c}_{\rm aux})\in\mathcal{C}^{\perp}\times\mathcal{C}_{\rm aux}\,:\,|\mathbf{h}_{\mathscr{N}}|=w\text{ and }|\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\rm aux}|=t_{\rm aux}\}\end{aligned}$$

and where $\mathbf{R}\in\mathbb{F}_2^{s\times(n-s)}$ is such that for any $\mathbf{h}\in\mathcal{C}^{\perp}$ we have $\mathbf{h}_{\mathscr{P}}=\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}$.

Let us devise a more convenient expression for $\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\rm aux}\rangle$. By noticing that $\mathbf{h}_{\mathscr{P}}$ and $\mathbf{h}_{\mathscr{N}}$ are linearly linked we get the following lemma.

Lemma 4. *Let $\mathscr{P}$ and $\mathscr{N}$ be two complementary subsets of $[\![1,n]\!]$ of size s and $n-s$ respectively. Let $\mathcal{C}$ and $\mathcal{C}_{\rm aux}$ be two $[n,k]$ linear and $[s,k_{\rm aux}]$ linear codes respectively such that $\mathcal{C}_{\mathscr{P}}$ is of dimension s. Let $\mathbf{x}\in\mathbb{F}_2^s$ and $(\mathbf{h},\mathbf{c}_{\rm aux})\in\widetilde{\mathscr{H}}$ where recall that*

$$\widetilde{\mathscr{H}}\overset{def}{=}\{(\mathbf{h},\mathbf{c}_{\rm aux})\in\mathcal{C}^{\perp}\times\mathcal{C}_{\rm aux}\,:|\mathbf{h}_{\mathscr{N}}|=w\text{ and }|\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\rm aux}^{\perp}|=t_{\rm aux}\}.$$

We have that

$$\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\rm aux}\rangle=\langle(\mathbf{x}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle+\langle\mathbf{x},\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\rm aux}\rangle\tag{59}$$

where $\mathbf{R}\in\mathbb{F}_2^{s\times(n-s)}$ is (independently of the parity-check $\mathbf{h}$) such that

$$\mathbf{h}_{\mathscr{P}}=\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}.\tag{60}$$

Proof. First, let us show Equation (60). Suppose without loss of generality that $\mathscr{P}=[\![1,s]\!]$ and $\mathscr{N}=[\![s+1,n]\!]$. Let $\mathbf{G}\in\mathbb{F}_2^{k\times n}$ be a generator matrix of $\mathcal{C}$. Because $\mathcal{C}_{\mathscr{P}}$ is of dimension s there exists an invertible $\mathbf{J}\in\mathbb{F}_2^{k\times k}$ such that

$$\mathbf{JG}=\begin{pmatrix}\mathbf{Id}_s & \mathbf{R}\\ \mathbf{0}_{k-s} & \mathbf{R}'\end{pmatrix}$$

where $\mathbf{R}\in\mathbb{F}_2^{s\times(n-s)}$ and $\mathbf{R}'\in\mathbb{F}_2^{(k-s)\times(n-s)}$. Furthermore, $\mathbf{JG}$ is another generator matrix for $\mathcal{C}$. Therefore for any $\mathbf{h}\in\mathcal{C}^{\perp}$ we have $\mathbf{JG}\,\mathbf{h}^{\intercal}=\mathbf{0}$. Since $\mathbf{JGh}^{\intercal}=\mathbf{h}_{\mathscr{P}}^{\intercal}+\mathbf{Rh}_{\mathscr{N}}^{\intercal}$, this gives (60). Now, let us prove (59). Recall that, using Equation (60) we have:

$$\begin{aligned}\langle\mathbf{y},\mathbf{h}\rangle&=\langle\mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle+\langle\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle\\ &=\langle\mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\top}\rangle+\langle\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle\\ &=\langle\mathbf{e}_{\mathscr{P}}\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle,\end{aligned}$$

and

$$\begin{aligned}\langle\mathbf{x},\mathbf{c}_{\rm aux}\rangle&=\langle\mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle+\langle\mathbf{x},\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\rm aux}\rangle\\ &=\langle\mathbf{xR},\mathbf{h}_{\mathscr{N}}\rangle+\langle\mathbf{x},\mathbf{h}_{\mathscr{P}}+\mathbf{c}_{\rm aux}\rangle\end{aligned}$$

where in the last equality we used Equation (60). This concludes the proof. □

Proof of Proposition 4. Let us consider $\mathbf{R} \in \mathbb{F}_2^{s\times(n-s)}$ as in Lemma 4 and let us prove Equation (10). By definition of the bias and $\widetilde{\mathscr{H}}$ given Equation (60) we have the following computation and ,

$$\begin{aligned}
&\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}))\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{c}_{\text{aux}}\rangle\right)\\
&\qquad = \frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{(\mathbf{h},\mathbf{c}_{\text{aux}})\in\widetilde{\mathscr{H}}}(-1)^{\langle \mathbf{y},\mathbf{h}\rangle+\langle \mathbf{x},\mathbf{c}_{\text{aux}}\rangle}\\
&\qquad = \frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{\substack{(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}})\in\left(\mathcal{C}^{\perp}\right)_{\mathscr{N}}\times\mathcal{C}_{\text{aux}}\\ |\mathbf{h}_{\mathscr{N}}|=w,|\mathbf{R}\mathbf{h}_{\mathscr{N}}+\mathbf{c}_{\text{aux}}|=t_{\text{aux}}}}(-1)^{\langle(\mathbf{x}+\mathbf{e}_{\mathscr{P}})\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle+\langle \mathbf{x},\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}+\mathbf{c}_{\text{aux}}\rangle}
\end{aligned}$$

where in the last equality we used Lemma 4. Therefore,

$$\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}))\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}} = \frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}})\in\left(\mathcal{C}^{\perp}\right)_{\mathscr{N}}\times\mathcal{C}_{\text{aux}}} f(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}}) \tag{61}$$

where,

$$f(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}}) \overset{\text{def}}{=} (-1)^{\langle(\mathbf{x}+\mathbf{e}_{\mathscr{P}})\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle+\langle \mathbf{x},\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}+\mathbf{c}_{\text{aux}}\rangle}\mathbf{1}_{\{|\mathbf{h}_{\mathscr{N}}|=w,|\mathbf{h}_{\mathscr{N}}\mathbf{R}^{\intercal}+\mathbf{c}_{\text{aux}}|=t_{\text{aux}}\}}.$$

Using Equation 3 we have that $\left(\mathcal{C}^{\perp}\right)_{\mathscr{N}} = \left(\mathcal{C}^{\mathscr{N}}\right)^{\perp}$ and thus $\left(\left(\mathcal{C}^{\mathscr{N}}\right)^{\perp}\times\mathcal{C}_{\text{aux}}\right)^{\perp} = \mathcal{C}^{\mathscr{N}}\times\mathcal{C}_{\text{aux}}^{\perp}$. By using the Poisson formula (see [MS86, Lemma 2, Ch. 5.2]), together with the fact that $\dim\left(\mathcal{C}^{\mathscr{N}}\times\mathcal{C}_{\text{aux}}^{\perp}\right) = k - k_{\text{aux}}$, we get

$$\sum_{(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}})\in\left(\mathcal{C}^{\mathscr{N}}\right)^{\perp}\times\mathcal{C}_{\text{aux}}} f(\mathbf{h}_{\mathscr{N}},\mathbf{c}_{\text{aux}}) = \frac{1}{2^{k-k_{\text{aux}}}}\sum_{\left(\mathbf{c}^{\mathscr{N}},\mathbf{c}_{\text{aux}}^{\perp}\right)\in\mathcal{C}^{\mathscr{N}}\times\mathcal{C}_{\text{aux}}^{\perp}}\widehat{f}(\mathbf{c}^{\mathscr{N}},\mathbf{c}_{\text{aux}}^{\perp}). \tag{62}$$

Let us compute the right-hand term. By definition of f, it is readily seen that

$$\begin{aligned}
\widehat{f}(\mathbf{y}_1,\mathbf{y}_2) &= \sum_{\substack{\mathbf{z}_1\in\mathbb{F}_2^{n-1},\mathbf{z}_2\in\mathbb{F}_2^{s}\\ |\mathbf{z}_1|=w,|\mathbf{z}_1\mathbf{R}^{\top}+\mathbf{z}_2|=t_{\text{aux}}}}(-1)^{\langle \mathbf{y}_1,\mathbf{z}_1\rangle+\langle \mathbf{y}_2,\mathbf{z}_2\rangle}(-1)^{\langle(\mathbf{x}+\mathbf{e}_{\mathscr{P}})\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{z}_1\rangle+\langle \mathbf{x},\mathbf{z}_1\mathbf{R}^{\intercal}+\mathbf{z}_2\rangle}\\
&= \sum_{\mathbf{z}_1\in\mathbb{F}_2^{n-s}:|\mathbf{z}_1|=w}(-1)^{\langle \mathbf{y}_1+(\mathbf{x}+\mathbf{e}_{\mathscr{P}}+\mathbf{y}_2)\mathbf{R}+\mathbf{e}_{\mathscr{N}},\mathbf{z}_1\rangle}\sum_{\mathbf{z}_2\in\mathbb{F}_2^{s}:|\mathbf{z}_1\mathbf{R}^{\intercal}+\mathbf{z}_2|=t_{\text{aux}}}(-1)^{\langle \mathbf{y}_2+\mathbf{x},\mathbf{z}_1\mathbf{R}^{\intercal}+\mathbf{z}_2\rangle}\\
&= K_w^{(n-s)}\left(|\mathbf{y}_1+(\mathbf{y}_2+\mathbf{x}+\mathbf{e}_{\mathscr{P}})\mathbf{R}+\mathbf{e}_{\mathscr{N}}|\right)\ K_{t_{\text{aux}}}^{(s)}\left(|\mathbf{y}_2+\mathbf{x}|\right)
\end{aligned}$$

where in the last equality we used Fact 1. Plugging this into Equation (62) and then into Equation (61) concludes the proof. □

Appendix D. Proof of Proposition 5

The proof of this Appendix is to prove Proposition 5 which we recall is given by

Proposition 5. *Using Distribution 1 for $\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{e}$ and $\mathbf{y}$ and given that our parameters verify Parameter Constraint 1, that the number of computed* LPN *samples is the total number of available* LPN *samples,* i.e. *$\mathscr{H} = \widetilde{\mathscr{H}}$ and under Conjecture 1 we have that the expected number of candidates per iteration is bounded by*

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(|\mathscr{S}|\right) = \widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}}\frac{\binom{s}{j}\binom{n-s}{i}}{2^{n-k}}\right) + 1 \tag{11}$$

where

$$\mathcal{A} \overset{def}{=} \left\{(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!],\ \left|\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right| \leqslant n^{3.2}\right\}. \tag{12}$$

The set $\mathscr{S}$ of candidates is defined by

$$\mathscr{S} \stackrel{def}{=} \left\{ \mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}} \ : \widehat{f_{\mathbf{y},\widetilde{\mathscr{H}},\mathbf{G}_{\text{aux}}}}(\mathbf{s}) \geqslant \frac{\delta}{2}\, \widetilde{H} \right\}, \tag{13}$$

where

$$\widetilde{H} \stackrel{def}{=} \frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} \qquad \text{and} \qquad \delta \stackrel{def}{=} \frac{K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}. \tag{14}$$

The proof is divided in the following steps.

Step 1: in Lemma 5 we show that the expected size of $\mathscr{S}$ is related to the probability that the bias of $\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle$ is superior to the threshold $\approx \frac{\delta}{2}$.

Step 2: We give an exponential bound on the aforementioned probability by using Poisson summation formula as it was done in the proof of Proposition 4.

Step 1. Recall that we have from Equation 13 that

$$\mathscr{S} \stackrel{\text{def}}{=} \left\{ \mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}} \ : \widehat{f_{\mathbf{y},\widetilde{\mathscr{H}},\mathbf{G}_{\text{aux}}}}(\mathbf{s}) \geqslant \frac{\delta}{2}\, \widetilde{H} \right\}.$$

By using Lemma 1 we get the following condition for an element $\mathbf{s}$ to be a candidate:

Fact 4. *Let $\mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}}$ and $\mathbf{x} \in \mathbb{F}_2^s$ such that $\mathbf{x}\mathbf{G}_{\text{aux}}^\intercal = \mathbf{s}$. We have,*

$$\mathbf{s} \in \mathscr{S} \iff \underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \stackrel{\$}{\leftarrow} \widetilde{\mathscr{H}}}{\text{bias}}(\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{c}_{\text{aux}} \rangle) \geqslant \frac{\delta}{2}\, \frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}.$$

From there, we can derive the following lemma linking the expected size of $\mathscr{S}$ and the previous bias.

Lemma 5. *Under Distribution 1, using notation of Proposition 5 and under the constraint of Proposition 5 that $\mathscr{H} = \widetilde{\mathscr{H}}$ we have*

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(|\mathscr{S}|) \leqslant 2^{k_{\text{aux}}} \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}} \left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \stackrel{\$}{\leftarrow} \widetilde{\mathscr{H}}}{\text{bias}}(\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{c}_{\text{aux}} \rangle) \geqslant \frac{\delta}{2}\, \frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|} \right) + 1$$

where $\mathbf{x}$ is taken uniformly at random in $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^\perp + \mathbf{e}_{\mathscr{P}}\}$.

Proof. We have the following computation,

$$\begin{aligned}
\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(|\mathscr{S}|) &= \mathbb{E}\left(\sum_{\mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}}} \mathbf{1}_{\mathbf{s} \in \mathscr{S}} \right) \\
&\leqslant 1 + \mathbb{E}\left(\sum_{\mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}} : \mathbf{s} \neq \mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^\intercal} \mathbf{1}_{\mathbf{s} \in \mathscr{S}} \right) \\
&= 1 + \mathbb{E}\left(\sum_{\mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}} : \mathbf{s} \neq \mathbf{e}_{\mathscr{P}} \mathbf{G}_{\text{aux}}^\intercal} \frac{1}{2^{s-k_{\text{aux}}}} \sum_{\mathbf{z} \in \mathbb{F}_2^s : \mathbf{z}\, \mathbf{G}_{\text{aux}}^\intercal = \mathbf{s}} \mathbf{1}_{\mathbf{z}\mathbf{G}_{\text{aux}}^\intercal \in \mathscr{S}} \right)
\end{aligned}$$

where in the last equality we used that $\mathbf{G}_{\text{aux}}$, which is a generator matrix of $\mathcal{C}_{\text{aux}}$, has rank $s - k_{\text{aux}}$ according to Distribution 1. Now, from the linearity of the expectation we get,

$$\begin{aligned}
\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(|\mathscr{S}|) &\leqslant 1 + \frac{1}{2^{s-k_{\text{aux}}}} \sum_{\mathbf{z} \in \mathbb{F}_2^s : \mathbf{z} \notin \mathcal{C}_{\text{aux}}^\perp + \mathbf{e}_{\mathscr{P}}} \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(\mathbf{z}\mathbf{G}_{\text{aux}}^\intercal \in \mathscr{S}) \\
&= 1 + 2^{k_{\text{aux}}}\, \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}(\mathbf{x}\mathbf{G}_{\text{aux}}^\intercal \in \mathscr{S})
\end{aligned}$$

where in the last line we used that $\mathbf{G}_{\text{aux}}$ has full rank, $\left|\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\right|=2^s$ and $\mathbf{x}$ is taken uniformly at random in $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$. Using Fact 4 concludes the proof. □

Step 2. The following lemma relates the upper-bound given in Lemma 5 to the involved probability in Conjecture 1.

Lemma 6. *Using Distribution 1 and notation of Proposition 5 we have*

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}(\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\text{aux}}\rangle)\geqslant\frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right)=$$

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{(n-s)}(i)\,N_{i,j}\geqslant\frac{1}{2}\,K_{w}^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right).$$

where $\mathbf{x}$ *is taken uniformly at random in* $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$.

Proof. Recall that we have that from notation of Proposition 5,

$$\widetilde{H}\overset{\text{def}}{=}\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}},\qquad\delta\overset{\text{def}}{=}\frac{K_{w}^{(n-s)}(u)K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.\tag{63}$$

According to Proposition 4 we have the following computation,

$$\begin{aligned}
&\mathbb{P}\left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}(\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\text{aux}}\rangle)\geqslant\frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right)\\
&=\mathbb{P}\left(\frac{1}{2^{k-k_{\text{aux}}}}\frac{1}{\left|\widetilde{\mathscr{H}}\right|}\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{n-s}(i)\,N_{i,j}\geqslant\frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right)\\
&=\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{n-s}(i)\,N_{i,j}\geqslant\frac{K_{w}^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{2}\right)
\end{aligned}$$

where in the last equality we used Equation (63). It concludes the proof. □

We will now use Conjecture 1 to bound the right-hand term of Lemma 6 by the probability of the event "$N_{i,j}\neq 0$" for some low i and j (more precisely when $K_{w}^{(n-s)}(u)K_{t_{\text{aux}}}^{(s)}(t-u)\leqslant K_{w}^{(n-s)}(i)K_{t_{\text{aux}}}^{(s)}(j)$).

Lemma 7. *Under Distribution 1 we have that for* $(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!]$,

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_{i,j}\neq 0\right)=\mathcal{O}\left(\frac{\binom{s}{j}\binom{n-s}{i}}{2^{k_{\text{aux}}+n-k}}\right)$$

where $\mathbf{x}$ *is taken uniformly at random in* $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$.

Proof. This is proved in the first lemma of Appendix E. □

We are now ready to prove Proposition 5.

proof of Proposition 5. Recall that we want to show,

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(|\mathscr{S}|\right)=\widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}}\frac{\binom{s}{j}\binom{n-s}{i}}{2^{n-k}}\right)+1.$$

Lemma 5 gives us that

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(|\mathscr{S}|\right)\leqslant 2^{k_{\text{aux}}}\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}(\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\text{aux}}\rangle)\geqslant\frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right)+1\tag{64}$$

Now using Lemma 6 we get that

$$\mathbb{P}\left(\underset{(\mathbf{h},\mathbf{c}_{\text{aux}})\xleftarrow{\$}\widetilde{\mathscr{H}}}{\text{bias}}(\langle\mathbf{y},\mathbf{h}\rangle+\langle\mathbf{x},\mathbf{c}_{\text{aux}}\rangle)\geqslant\frac{\delta}{2}\frac{\widetilde{H}}{\left|\widetilde{\mathscr{H}}\right|}\right)=$$

$$\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{(n-s)}(i)\,N_{i,j}\geqslant\frac{1}{2}K_{w}^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right). \quad (65)$$

From Conjecture 1,

$$\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{(n-s)}(i)\,N_{i,j}\geqslant\frac{1}{2}K_{w}^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right)=\widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}}\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}(N_{i,j}\neq0)\right)$$

Therefore, using Lemma 7 we get

$$\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_{w}^{(n-s)}(i)\,N_{i,j}\geqslant\frac{1}{2}K_{w}^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right)=\widetilde{\mathcal{O}}\left(\frac{\binom{s}{j}\binom{n-s}{i}}{2^{k_{\text{aux}}+n-k}}\right)$$

Plugging this into Equation (65) and then in (64) concludes the proof. which proves our result. □

Appendix E. About the distribution of the $N_{i,j}$

This appendix is dedicated to studying the distribution of $N_{i,j}$ and in particular to prove Lemma 7 which was used in Appendix C to prove Proposition 4. We recall that it is given by

Lemma 7. *Under Distribution 1 we have that for* $(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!]$,

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}(N_{i,j}\neq0)=\mathcal{O}\left(\frac{\binom{s}{j}\binom{n-s}{i}}{2^{k_{\text{aux}}+n-k}}\right)$$

where $\mathbf{x}$ *is taken uniformly at random in* $\mathbb{F}_2^s\setminus\{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$.

First, using the union bound we can devise the following upper bound on our target probability:

Fact 5.

$$\mathbb{P}(N_{i,j}\neq0)\leqslant\mathbb{E}(N_{i,j}).$$

To compute this expected value, we first need to give the following lemma giving the probability that a word belongs to a random code.

Lemma 8. *Let* $\mathcal{C}$ *be chosen uniformly at random among the* $[n,k]$ *linear codes. Let* $\mathbf{c}\in\mathbb{F}_2^n\setminus\{\mathbf{0}\}$ *we have*

$$\mathbb{P}_{\mathcal{C}}(\mathbf{c}\in\mathcal{C})=\frac{2^k-1}{2^n-1}, \quad (66)$$

$$\mathbb{P}_{\mathcal{C}}(\mathbf{0}\in\mathcal{C})=1. \quad (67)$$

Proof. This lemma directly follows from [BCN89, §3, Lemma 9.3.2, (iii)]. □

We now give the preliminary lemma which breaks down the expected value of $N_{i,j}$ on the $\mathcal{C}_{\text{aux}}^{\perp}$ part and on the $\mathcal{C}^{\mathscr{N}}$ part.

Lemma 9. *Under Distribution 1 we denote by*

$$\overline{N_j^{(\mathcal{C}_{\text{aux}}^{\perp})}}\overset{def}{=}\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_j\left(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\right)$$

where $\mathbf{x}$ *is taken uniformly at random in* $\mathbb{F}_2^s\setminus\{\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{e}_{\mathscr{P}}\}$ *and* $\mathbf{r}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}$. *We denote by fixing* $\mathbf{x}$,

$$\overline{N_i^{(\mathcal{C}^{\mathscr{N}})}}\overset{def}{=}\mathbb{E}_{\mathcal{C}}\left(N_i\left(\mathcal{C}^{\mathscr{N}}+(\mathbf{r}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R}+\mathbf{e}_{\mathscr{N}}\right)\right) \quad (68)$$

We have that

$$\overline{N_i^{(\mathcal{C}^{\mathscr{N}})}} = \frac{\binom{n-s}{i}}{2^{n-k}}\left(1+\mathcal{O}\left(2^{-(s-k)}\right)\right) \tag{69}$$

$$\overline{N_j^{(\mathcal{C}_{\mathrm{aux}}^{\perp})}} \leqslant \frac{\binom{s}{j}}{2^{k_{\mathrm{aux}}}}\left(1+\mathcal{O}\left(2^{-(s-k_{\mathrm{aux}})}\right)\right) \tag{70}$$

Furthermore, the term $\mathcal{O}\left(2^{-(s-k_{\mathrm{aux}})}\right)$ *in Equation* (69) *does not depend on* i *.*

Proof. Under Distribution 1, $\mathcal{C}$ is taken at random among the $[n,k]$-codes that are such that $\mathcal{C}_{\mathscr{P}}$ is of full rank dimension s. Therefore, it is the same as if $\mathcal{C}$ was chosen by taking its generator matrix $\mathbf{G} \in \mathbb{F}_2^{k\times n}$ as follows:

$$\mathbf{G}_{\mathscr{P}} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbf{I}_s \\ \mathbf{0}_{k-s} \end{pmatrix}, \qquad \mathbf{G}_{\mathscr{N}} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbf{R} \\ \mathbf{G}^{\mathscr{N}} \end{pmatrix}.$$

where $\mathbf{R}$ is chosen uniformly at random among matrices of $\mathbb{F}_2^{s\times(n-s)}$ and $\mathbf{G}^{\mathscr{N}}$ is any generator matrix of a code chosen uniformly at random among the $[n-s,k-s]$-codes. In particular, $\mathbf{G}^{\mathscr{N}}$ and $\mathbf{R}$ are independent.

Now, by definition $\mathbf{x} \in \mathbb{F}_2^s \setminus \{\mathcal{C}_{\mathrm{aux}}^{\perp} + \mathbf{e}_{\mathscr{P}}\}$ and $\mathbf{r} \in \mathcal{C}_{\mathrm{aux}}^{\perp} + \mathbf{x}$, therefore $\mathbf{r} + \mathbf{e}_{\mathscr{P}} \neq \mathbf{0}$. We deduce that, $(\mathbf{r}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R}$ is uniformly distributed in $\mathbb{F}_2^{n-s}$ as a non-zero sum of uniformly distribution vectors. To simplify the notations let us define the uniformly distributed vector

$$\mathbf{v} \stackrel{\text{def}}{=} (\mathbf{r}+\mathbf{e}_{\mathscr{P}})\,\mathbf{R} + \mathbf{e}_{\mathscr{N}}$$

which is independent of $\mathcal{C}^{\mathscr{N}}$ (by construction $\mathbf{G}^{\mathscr{N}}$ and $\mathbf{R}$ are independent). Now, let us show Equation (69). We have by linearity of the expected value that

$$\begin{aligned}
\overline{N_i^{(\mathcal{C}^{\mathscr{N}})}} &= \sum_{\mathbf{z}\in\mathcal{S}_i^{n-s}} \mathbb{P}_{\mathcal{C},\mathbf{v}}\left(\mathbf{z} \in \mathcal{C}^{\mathscr{N}} + \mathbf{v}\right) \\
&= \sum_{\mathbf{z}\in\mathcal{S}_i^{n-s}} \mathbb{P}_{\mathcal{C},\mathbf{v}}\left(\mathbf{z} \in \mathcal{C}^{\mathscr{N}} + \mathbf{v} \middle| \mathbf{v} = \mathbf{z}\right)\mathbb{P}_{\mathcal{C},\mathbf{v}}\left(\mathbf{v}=\mathbf{z}\right) + \mathbb{P}_{\mathcal{C},\mathbf{v}}\left(\mathbf{z} \in \mathcal{C}^{\mathscr{N}} + \mathbf{v} \middle| \mathbf{v} \neq \mathbf{z}\right)\mathbb{P}_{\mathcal{C},\mathbf{v}}\left(\mathbf{v}\neq\mathbf{z}\right) \\
&= \sum_{\mathbf{z}\in\mathcal{S}_i^{n-s}} \frac{1}{2^{n-s}} + \frac{2^{k-s}-1}{2^{n-s}-1}\left(1-\frac{1}{2^{n-s}}\right) \qquad \text{(Lemma 8)} \\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\left(\frac{2^{n-k}}{2^{n-s}} + 2^{n-k}\,\frac{2^{k-s}-1}{2^{n-s}-1}\,\mathcal{O}(1)\right) \\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\left(\frac{1}{2^{k-s}} + \frac{2^{-s}-2^{-k}}{2^{-s}-2^{-n}}\,\mathcal{O}(1)\right) \\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\left(\frac{1}{2^{k-s}} + \frac{1-2^{-k+s}}{1-2^{-n+s}}\,\mathcal{O}(1)\right) \\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\left(1 + \frac{1}{2^{k-s}} + \mathcal{O}\left(2^{-k+s}\right)\right) \quad (s \leqslant k \leqslant n)
\end{aligned}$$

Let us now show Equation (70). Recall that

$$\overline{N_j^{(\mathcal{C}_{\mathrm{aux}}^{\perp})}} \stackrel{\text{def}}{=} \mathbb{E}_{\mathcal{C}_{\mathrm{aux}},\mathbf{x}}\left(N_j\left(\mathcal{C}_{\mathrm{aux}}^{\perp}+\mathbf{x}\right)\right)$$

where $\mathbf{x}$ is taken uniformly at random in $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^\perp + \mathbf{e}_{\mathscr{P}}\}$. By definition,

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_j\left(\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}\right)\right) &= \sum_{\mathbf{z}\in\mathcal{S}_j^s} \mathbb{P}_{\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\mathbf{z} \in \mathcal{C}_{\text{aux}}^\perp + \mathbf{x}\right) \\
&= \sum_{\mathbf{z}\in\mathcal{S}_j^s, \mathbf{x}_0\in\mathbb{F}_2^s} \mathbb{P}_{\mathcal{C}_{\text{aux}}}\left(\mathbf{z} - \mathbf{x}_0 \in \mathcal{C}_{\text{aux}}^\perp\right) \mathbb{P}_{\mathbf{x},\mathcal{C}_{\text{aux}}}\left(\mathbf{x} = \mathbf{x}_0\right) \\
&\leqslant \sum_{\mathbf{z}\in\mathcal{S}_j^s} \left(\sum_{\mathbf{x}_0\in\mathbb{F}_2^s} \frac{2^{s-k_{\text{aux}}}-1}{2^s-1} \mathbb{P}_{\mathbf{x},\mathcal{C}_{\text{aux}}}\left(\mathbf{x} = \mathbf{x}_0\right) + \mathbb{P}_{\mathbf{x},\mathcal{C}_{\text{aux}}}\left(\mathbf{x} = \mathbf{z}\right) \right) \\
&\leqslant \binom{s}{j} \frac{2^{s-k_{\text{aux}}}-1}{2^s-1} + \frac{\binom{s}{j}}{2^s - 2^{k_{\text{aux}}}} \\
&\leqslant \frac{\binom{s}{j}}{2^{k_{\text{aux}}}} \, 2^{k_{\text{aux}}} \, \frac{2^{s-k_{\text{aux}}}-1}{2^s-1} + \frac{\binom{s}{j}}{2^{k_{\text{aux}}}} \, \frac{2^{k_{\text{aux}}}}{2^s - 2^{k_{\text{aux}}}} \\
&\leqslant \frac{\binom{s}{j}}{2^{k_{\text{aux}}}} \, \frac{2^s - 2^{k_{\text{aux}}}}{2^s-1} + \frac{\binom{s}{j}}{2^{k_{\text{aux}}}} \, \frac{1}{2^{s-k_{\text{aux}}}-1} \\
&\leqslant \frac{\binom{s}{j}}{2^{k_{\text{aux}}}} \, \left(1 + \mathcal{O}\left(2^{k_{\text{aux}}-s}\right)\right)
\end{aligned}$$

which completes the proof. □

We can now show that the expected value of $N_{i,j}$ is the product of the two previously computed quantities:

Lemma 10. *Under Distribution 1 and when $\mathbf{x}$ is taken uniformly at random in $\mathbb{F}_2^s \setminus \{\mathcal{C}_{\text{aux}}^\perp + \mathbf{e}_{\mathscr{P}}\}$ we have*

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_{i,j}\right) = \overline{N_j^{(\mathcal{C}_{\text{aux}}^\perp)}} \; \overline{N_i^{(\mathcal{C}^{\mathscr{N}})}}$$

where,

$$N_{i,j} \stackrel{def}{=} \left|\left\{\left(\mathbf{r}, \mathbf{c}^{\mathscr{N}}\right) \in \left(\mathbf{x} + \mathcal{C}_{\text{aux}}^\perp\right) \times \mathcal{C}^{\mathscr{N}} \;:\; |\mathbf{r}| = j \text{ and } \left|\left(\mathbf{r} + \mathbf{e}_{\mathscr{P}}\right)\mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathbf{c}^{\mathscr{N}}\right| = i\right\}\right|$$

and,

$$\overline{N_j^{(\mathcal{C}_{\text{aux}}^\perp)}} \stackrel{def}{=} \mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_j\left(\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}\right)\right) \quad ; \quad \overline{N_i^{(\mathcal{C}^{\mathscr{N}})}} \stackrel{def}{=} \mathbb{E}_{\mathcal{C}}\left(N_i\left(\mathcal{C}^{\mathscr{N}} + \left(\mathbf{r} + \mathbf{e}_{\mathscr{P}}\right)\mathbf{R} + \mathbf{e}_{\mathscr{N}}\right)\right).$$

Proof. By definition,

$$N_{i,j} = \sum_{u=0}^{N_j\left(\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}\right)} N_i\left(\left(\mathbf{r}^{(u)} + \mathbf{e}_{\mathscr{P}}\right)\mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathcal{C}^{\mathscr{N}}\right)$$

where $\mathbf{r}^{(u)}$ is the u'th codeword of weight j of $\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}$ and $N_j(\mathcal{C}_{\text{aux}}^\perp + \mathbf{x})$ counts the number of elements in $\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}$ of Hamming weight j. Therefore,

$$\begin{aligned}
N_{i,j} &= \sum_{\mathbf{z}\in\mathcal{S}_j^s} N_i\left(\left(\mathbf{z} + \mathbf{e}_{\mathscr{P}}\right)\mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathcal{C}^{\mathscr{N}}\right) \; \mathbb{1}_{\text{“}\mathbf{z}\in\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}''} \\
&= \sum_{\mathbf{z}\in\mathcal{S}_j^s, \mathbf{w}\in\mathcal{S}_i^{n-s}} \mathbb{1}_{\text{“}\mathbf{w}\in(\mathbf{z}+\mathbf{e}_{\mathscr{P}})\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\text{”}} \; \mathbb{1}_{\text{“}\mathbf{z}\in\mathcal{C}_{\text{aux}}^\perp + \mathbf{x}''}
\end{aligned}$$

We deduce that,

$$\begin{aligned}
\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_{i,j}\right) &= \sum_{\mathbf{z}\in\mathcal{S}_j^s,\mathbf{w}\in\mathcal{S}_i^{n-s}} \mathbb{P}\left(\mathbf{w}\in\left(\mathbf{z}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}},\ \mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\\
&= \sum_{\mathbf{z}\in\mathcal{S}_j^s,\mathbf{w}\in\mathcal{S}_i^{n-s}} \mathbb{P}\left(\mathbf{w}\in\left(\mathbf{z}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\mid \mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\mathbb{P}\left(\mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\\
&= \sum_{\mathbf{z}\in\mathcal{S}_j^s}\left(\sum_{\mathbf{w}\in\mathcal{S}_i^{n-s}} \mathbb{P}\left(\mathbf{w}\in\left(\mathbf{z}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\mid \mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\right)\mathbb{P}\left(\mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\\
&= \sum_{\mathbf{z}\in\mathcal{S}_j^s}\overline{N_i^{(\mathcal{C}^{\mathscr{N}})}}\,\mathbb{P}\left(\mathbf{z}\in\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)\\
&= \overline{N_i^{(\mathcal{C}^{\mathscr{N}})}}\,\overline{N_j^{(\mathcal{C}_{\text{aux}}^{\perp})}}
\end{aligned}$$

which completes the proof. □

Proof of Lemma 7. We prove our result by using Fact 5, then Lemmas 9 and 10. □

Appendix F. Proof of Proposition 6

F.1. **A more minimalistic conjecture.** The goal of this section is to devise a more minimalistic but stronger conjecture which implies Conjecture 1 (in the sense that it involves only concentration bound of the weight enumerator of some random linear codes). Furthermore, the aforementioned implication is a key step of the proof of Proposition 6 which shows that the experimental model implies Conjecture 1.

Conjecture 2. *For any* $(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!]$ *and any* $v\in\left[\!\left[0,\overline{V_j}+n^{1.1}\max\left(\sqrt{\overline{V_j}},1\right)\right]\!\right]$, *we have under Distribution 1,*

$$\mathbb{P}_{\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|V_j-\overline{V_j}\right|>n^{1.1}\max\left(\sqrt{\overline{V_j}},1\right)\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right), \tag{71}$$

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|N_{i,j}-v\,\overline{N_i}\right|>n^{1.1}\max\left(\sqrt{v\,\overline{N_i}},\,1\right)\middle|\,N_j=v\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right). \tag{72}$$

where

$$V_j \overset{def}{=} N_j\left(\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}\right)$$

and

$$\overline{N_i}\overset{def}{=}\frac{\binom{n-s}{i}}{2^{n-k}},\quad \overline{V_j}\overset{def}{=}\frac{\binom{s}{j}}{2^{k_{\text{aux}}}}. \tag{73}$$

Remark 6. *Recall that* $N_{i,j}\overset{def}{=}\sum_{u=1}^{V_j}N_i^{(u)}$ *where* $N_i^{(u)}\overset{def}{=}N_i\left(\left(\mathbf{r}^{(u)}+\mathbf{e}_{\mathscr{P}}\right)\mathbf{R}+\mathbf{e}_{\mathscr{N}}+\mathcal{C}^{\mathscr{N}}\right)$ *and* $\mathbf{r}^{(u)}$ *is the* u*'th codeword of weight* j *of* $\mathcal{C}_{\text{aux}}^{\perp}+\mathbf{x}$. *From this and using Lemma 9 it is readily seen that we have that*

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(N_{i,j}\middle|\,V_j=v\right)=v\,\overline{N_i}\left(1+o(1)\right).$$

As such, Equation (72) in the previous Conjecture can also really be seen as a concentration inequality.

Proposition 12. *Conjecture 2 implies Conjecture 1.*

The following lemmas will be useful to prove the this proposition.

Lemma 11 (Centering Lemma.)**.** *We have,*

$$\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_w^{(n-s)}(i)\,N_{i,j}=\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_w^{(n-s)}(i)\left(N_{i,j}-V_j\overline{N_i}\right).$$

Proof. From the orthogonality of Krawtchouk polynomials relatively to the measure $\mu(i) = \binom{n-s}{i}$ [MS86, Ch. 5. §7. Theorem 16] we have:

$$\sum_{i=0}^{n-s} \binom{n-s}{i} K_w^{(n-s)}(i) = 0.$$

By using the definition of $\overline{N_i}$ in Equation (73), we get,

$$\begin{aligned} 0 &= \sum_{j=0}^{s} V_j \, K_{t_{\text{aux}}}^{(s)}(j) \sum_{i=0}^{n-s} K_w^{(n-s)}(i) \, \overline{N_i} \\ &= \sum_{j=0}^{s} \sum_{i=0}^{n-s} K_w^{(n-s)}(i) \, K_{t_{\text{aux}}}^{(s)}(j) \, V_j \, \overline{N_i}. \end{aligned}$$

Therefore,

$$\sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{(n-s)}(i) \, N_{i,j} = \sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{(n-s)}(i) \left(N_{i,j} - V_j \overline{N_i}\right)$$

which completes the proof. □

Corollary 2. *We have,*

$$\mathbb{P}\left(\sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{(n-s)}(i) \, N_{i,j} \geqslant \frac{1}{2} K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)\right) =$$

$$\widetilde{\mathcal{O}}\left(\max_{(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!]} \mathbb{P}\left(\left|N_{i,j} - V_j \, \overline{N_i}\right| \geqslant \frac{1}{2\,(n+1)^2} \left| \frac{K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i) \, K_{t_{\text{aux}}}^{(s)}(j)} \right| \right)\right)$$

Proof. The event

$$\sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{n-s}(i) \left(N_{i,j} - V_j \overline{N_i}\right) \geqslant \frac{1}{2} K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)$$

implies that it exists $j \in [\![0, s]\!]$ and $i \in [\![0, n-s]\!]$ such that

$$K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{n-s}(i) \left(N_{i,j} - V_j \overline{N_i}\right) \geqslant \frac{K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)}{2\,(n-s+1)\,(s+1)}. \tag{74}$$

Therefore,

$$\begin{aligned} &\mathbb{P}\left(\sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{(n-s)}(i) \, N_{i,j} \geqslant \frac{1}{2} K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)\right) \\ &= \mathbb{P}\left(\sum_{j=0}^{s} \sum_{i=0}^{n-s} K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{n-s}(i) \left(N_{i,j} - V_j \overline{N_i}\right) \geqslant \frac{1}{2} K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)\right) \quad \text{(Lemma 11)} \\ &\leqslant \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(\bigvee_{j=0}^{s} \bigvee_{i=0}^{n-s} \left(K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{n-s}(i) \left(N_{i,j} - V_j \overline{N_i}\right) \geqslant \frac{K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)}{2\,(n-s+1)\,(s+1)}\right)\right) \quad \text{(using (74))} \\ &\leqslant \sum_{j=0}^{s} \sum_{i=0}^{n-s} \mathbb{P}\left(K_{t_{\text{aux}}}^{(s)}(j) \, K_w^{n-s}(i) \left(N_{i,j} - V_j \overline{N_i}\right) \geqslant \frac{K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)}{2\,(n-s+1)\,(s+1)}\right) \quad \text{(union bound)} \\ &= \mathcal{O}(n^2) \max_{\substack{i=0\ldots n-s \\ j=0\ldots s}} \mathbb{P}\left(\left|N_{i,j} - V_j \overline{N_i}\right| \geqslant \frac{1}{2\,(n+1)^2} \left| \frac{K_w^{(n-s)}(u) \, K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i) \, K_{t_{\text{aux}}}^{(s)}(j)} \right| \right) \end{aligned}$$

which completes the proof. □

Lemma 12. *Under Parameters constraint 1 we have that*

$$\left(\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right)^2 = \omega\left(n^{\alpha+8}\right)\overline{N_i}\max\left(\overline{V_j},\frac{1}{\mathcal{O}(n^\alpha)}\right)$$

Proof. First, we simplify $\left(K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right)^2$ by using Constraint (i) of Parameters constraint 1 which we recall is given by:

$$\frac{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}{2^{k-k_{\text{aux}}}} = \frac{\omega\left(n^{\alpha+8}\right)}{\delta^2}, \quad \text{where } \delta \stackrel{\text{def}}{=} \frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{\binom{n-s}{w}\binom{s}{t_{\text{aux}}}}.$$

By reordering the terms in the previous equation we get:

$$\left(K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right)^2 = 2^{k-k_{\text{aux}}}\binom{s}{t_{\text{aux}}}\binom{n-s}{w}\omega(n^{\alpha+8}).$$

Now, to show the lemma we only have to show that

$$\frac{2^{k-k_{\text{aux}}}\binom{s}{t_{\text{aux}}}\binom{n-s}{w}}{\left(K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)\right)^2}) \geqslant \overline{N_i}\max\left(\overline{V_j},\frac{1}{\mathcal{O}(n^\alpha)}\right). \tag{75}$$

First ,let us lower bound $\frac{1}{\left(K_w^{(n-s)}(i)\right)^2}$. From the orthonormality relations of the Krawtchouk polynomials [MS86, Ch. 5. §7. Theorem 16] with the measure $\mu_1(v) = \frac{\binom{n-s}{v}}{2^{n-s}}$ we have that

$$\sum_{v=0}^{n-s}\binom{n-s}{v}\left(K_w^{(n-s)}(v)\right)^2 = \binom{n-s}{w}2^{n-s},$$

and thus, as the previous sum is composed of positive terms, we have that

$$\frac{1}{\left(K_w^{(n-s)}(i)\right)^2} \geqslant \frac{\binom{n-s}{i}}{\binom{n-s}{w}2^{n-s}}. \tag{76}$$

Now, let us lower-bound $\frac{1}{\left(K_{t_{\text{aux}}}^{(s)}(j)\right)^2}$. Using the same orthonormality argument relatively to the measure $\mu_2(v) = \frac{\binom{s}{v}}{2^s}$ we get

$$\frac{1}{\left(K_{t_{\text{aux}}}^{(s)}(j)\right)^2} \geqslant \frac{\binom{s}{j}}{\binom{s}{t_{\text{aux}}}2^s}.$$

Furthermore, from Fact 1 we can also deduce the following inequality

$$\left(K_{t_{\text{aux}}}^{(s)}(j)\right)^2 \leqslant \binom{s}{t_{\text{aux}}}^2.$$

Combining the last two equations we get that

$$\frac{1}{\left(K_{t_{\text{aux}}}^{(s)}(j)\right)^2} \geqslant \min\left(\frac{\binom{s}{j}}{\binom{s}{t_{\text{aux}}}2^s},\frac{1}{\binom{s}{t_{\text{aux}}}^2}\right). \tag{77}$$

Finally let us show Equation (75) by using Equation (76) and (77) :

$$\begin{aligned}
\frac{2^{k-k_{\text{aux}}}\binom{s}{t_{\text{aux}}}\binom{n-s}{w}}{\left(K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)\right)^2} &\geqslant 2^{k-k_{\text{aux}}}\binom{s}{t_{\text{aux}}}\binom{n-s}{w}\frac{\binom{n-s}{i}}{\binom{n-s}{w}2^{n-s}}\min\left(\frac{\binom{s}{j}}{\binom{s}{t_{\text{aux}}}2^s},\frac{1}{\binom{s}{t_{\text{aux}}}^2}\right)\\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\min\left(\frac{\binom{s}{j}}{2^{k_{\text{aux}}}},\ \frac{2^{s-k_{\text{aux}}}}{\binom{s}{t_{\text{aux}}}}\right)\\
&= \frac{\binom{n-s}{i}}{2^{n-k}}\min\left(\frac{\binom{s}{j}}{2^{k_{\text{aux}}}},\frac{1}{\mathcal{O}(n^\alpha)}\right) \quad \text{(Constraint } (iii) \text{ of Eq. (15))}\\
&= \overline{N_i}\min\left(\overline{V_j},\frac{1}{\mathcal{O}(n^\alpha)}\right).
\end{aligned}$$

This completes the proof. □

Proof of Proposition 12. Let us suppose that the Parameter constraint 1 is verified and that Conjecture 2 is true. We want to show Conjecture 1 holds, namely that

$$\mathbb{P}\left(\sum_{j=0}^{s}\sum_{i=0}^{n-s}K_{t_{\text{aux}}}^{(s)}(j)\,K_w^{(n-s)}(i)\,N_{i,j}\geqslant\frac{1}{2}K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)\right)$$
$$=\widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}}\mathbb{P}\left(N_{i,j}\neq 0\right)+2^{-n}\right).$$

Using Corollary 2, we only have to show that for any $(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!]$ we have

$$\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant\frac{1}{2\,(n+1)^2}\left|\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right|\right)=\widetilde{\mathcal{O}}\left(\max_{(i^*,j^*)\in\mathcal{A}}\mathbb{P}\left(N_{i^*,j^*}\neq 0\right)+2^{-n}\right).$$

To ease up the notations let us denote by

$$R_{i,j}\overset{\text{def}}{=}\frac{1}{2\,(n+1)^2}\left|\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right|. \tag{78}$$

Thus, we only have to show that

$$\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant R_{i,j}\right)=\widetilde{\mathcal{O}}\left(\max_{(i^*,j^*)\in\mathcal{A}}\mathbb{P}\left(N_{i^*,j^*}\neq 0\right)+2^{-n}\right). \tag{79}$$

We prove the previous equality for each cases: $(i,j)\in\mathcal{A}$ or $(i,j)\notin\mathcal{A}$, where recall that

$$\mathcal{A}\overset{\text{def}}{=}\left\{(i,j)\in[\![0,n-s]\!]\times[\![0,s]\!],\ \left|\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right|\leqslant n^{3.2}\right\}.$$

Cases 1: Here we suppose that $(i,j)\in\mathcal{A}$. Let us prove Equation (79). Using the law of total probability we have that

$$\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant R_{i,j}\right)\leqslant\mathbb{P}\left(N_{i,j}\neq 0\right)+\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant R_{i,j},\ N_{i,j}=0\right).$$

As $(i,j)\in\mathcal{A}$,

$$\mathbb{P}\left(N_{i,j}\neq 0\right)=\widetilde{\mathcal{O}}\left(\max_{(i^*,j^*)\in\mathcal{A}}\mathbb{P}\left(N_{i^*,j^*}\neq 0\right)\right)$$

we only have left to show that:

$$\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant R_{i,j},\ \ N_{i,j}=0\right)=\widetilde{\mathcal{O}}\left(\max_{(i^*,j^*)\in\mathcal{A}}\mathbb{P}\left(N_{i^*,j^*}\neq 0\right)+2^{-n}\right).$$

We now show the previous equation, by proving that,

$$\mathbb{P}\left(\left|N_{i,j}-V_j\,\overline{N_i}\right|\geqslant R_{i,j},\ \ N_{i,j}=0\right)=\widetilde{\mathcal{O}}\left(2^{-n}\right). \tag{80}$$

We have:

$$\begin{aligned}
\mathbb{P}\left(\left|N_{i,j} - V_j\,\overline{N_i}\right| \geqslant R_{i,j},\ \ N_{i,j}=0\right) &= \mathbb{P}\left(V_j\,\overline{N_i} \geqslant R_{i,j}\right) \quad \text{(we used that } V_j, \overline{N_i} > 0\text{)} \\
&= \mathbb{P}\left(V_j \geqslant \frac{R_{i,j}}{\overline{N_i}}\right) \\
&= \mathbb{P}\left(V_j - \overline{V_j} \geqslant \frac{R_{i,j}}{\overline{N_i}} - \overline{V_j}\right) \\
&\leqslant \mathbb{P}\left(\left|V_j - \overline{V_j}\right| \geqslant \frac{R_{i,j}}{\overline{N_i}} - \overline{V_j}\right).
\end{aligned}$$

Recall that from Equation (71) of Conjecture 2 we have that

$$\mathbb{P}_{\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|V_j - \overline{V_j}\right| > n^{1.1}\max\left(\sqrt{\overline{V_j}}, 1\right)\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right).$$

Therefore, we only have to show that for n big enough we have

$$\frac{R_{i,j}}{\overline{N_i}} - \overline{V_j} \geqslant n^{1.1}\max\left(\sqrt{\overline{V_j}},\, 1\right) \tag{81}$$

to prove Equation (80). Let us prove Equation (81). By definition of $R_{i,j}$ in Equation (78) and using Lemma 12 we have that

$$\begin{aligned}
R_{i,j}^2 &= \frac{1}{4\,(n+1)^4}\left(\frac{K_w^{(n-s)}(u)\,K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\,K_{t_{\text{aux}}}^{(s)}(j)}\right)^2 \\
&= \frac{1}{4\,(n+1)^4}\,\omega\left(n^{\alpha+8}\right)\overline{N_i}\max\left(\overline{V_j}, \frac{1}{\mathcal{O}(n^\alpha)}\right) \\
&= f(n)\max\left(\overline{N_i}\,\overline{V_j}, n^{-\alpha}\overline{N_i}\right)
\end{aligned} \tag{82}$$

where $f(n) = \omega\left(n^{\alpha+4}\right)$. Therefore,

$$\begin{aligned}
\frac{R_{i,j}^2}{\overline{N_i}^2}\,\frac{1}{n^{2.4}\max\left(\overline{V_j}^2,\,1\right)} &= \frac{f(n)\max\left(\overline{N_i}\,\overline{V_j}, n^{-\alpha}\,\overline{N_i}\right)}{n^{2.4}\,\overline{N_i}^2\max\left(\overline{V_j}^2,\,1\right)} \\
&= \frac{f(n)\max\left(\frac{\overline{V_j}}{\overline{N_i}}, \frac{n^{-\alpha}}{\overline{N_i}}\right)}{n^{2.4}\,\max\left(\overline{V_j}^2,\,1\right)} \\
&= \begin{cases} \frac{1}{n^{2.4}} f(n)\max\left(\frac{1}{\overline{N_i}\overline{V_j}}, \frac{n^{-\alpha}}{\overline{N_i}\overline{V_j}^2}\right) & \text{if } \overline{V_j} > 1 \\ \frac{1}{n^{2.4}} f(n)\max\left(\frac{\overline{V_j}}{\overline{N_i}}, \frac{n^{-\alpha}}{\overline{N_i}}\right) & \text{if } \overline{V_j} \leqslant 1 \end{cases} \\
&\geqslant \frac{1}{n^{2.4}} f(n)\min\left(\frac{1}{\overline{N_i}\overline{V_j}}, \frac{n^{-\alpha}}{\overline{N_i}}\right) \\
&\geqslant \frac{n^{-2\alpha}}{n^{2.4}}\ f(n)\ \min\left(\frac{1}{\overline{N_i}\overline{V_j}}, \frac{1}{n^{-\alpha}\,\overline{N_i}}\right) \\
&= \frac{n^{-2\alpha}}{n^{2.4}}\ \frac{f(n)}{\max\left(\overline{N_i}\overline{V_j}, n^{-\alpha}\,\overline{N_i}\right)} \\
&= \frac{n^{-2\alpha}}{n^{2.4}}\ \frac{f(n)^2}{R_{i,j}^2} \qquad \text{(By Equation (82))} \\
&= \frac{\omega\left(n^{5.6}\right)}{R_{i,j}^2} \qquad \left(f(n) = \omega\left(n^{\alpha+4}\right)\right) \\
&= \omega(1)
\end{aligned} \tag{83}$$

where in the last line we used the fact that $(i,j) \in \mathcal{A}$: by definition,

$$R_{i,j} = \frac{1}{2\,(n+1)^2} \left| \frac{K_w^{(n-s)}(u)\, K_{t_{\text{aux}}}^{(s)}(t-u)}{K_w^{(n-s)}(i)\, K_{t_{\text{aux}}}^{(s)}(j)} \right| \leqslant \frac{1}{2\,(n+1)^2}\, n^{3.2}$$

and thus

$$\frac{1}{R_{i,j}^2} \geqslant \frac{2\,(n+1)^2}{n^{3.2}}.$$

Finally, Equation (83) shows that for n big enough

$$\frac{R_{i,j}}{\overline{N_i}} \geqslant n^{1.2} \max\left(\overline{V_j},\, 1\right)$$

And as such, for n big enough

$$\begin{aligned} \frac{R_{i,j}}{\overline{N_i}} - \overline{V_j} &\geqslant n^{1.1} \max\left(\overline{V_j},\, 1\right) \\ &\geqslant n^{1.1} \max\left(\sqrt{\overline{V_j}},\, 1\right) \end{aligned}$$

which proves Equation (81). Therefore we have just proved Equation (79) in the case where $(i,j) \in \mathcal{A}$.

Case 2: . Here we suppose that $(i,j) \notin \mathcal{A}$. Let us prove Equation (79). We only have to prove that:

$$\mathbb{P}\left(\left|N_{i,j} - V_j\, \overline{N_i}\right| \geqslant R_{i,j}\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right).$$

Let M be defined as

$$M \stackrel{\text{def}}{=} \overline{V_j} + n^{1.1} \max\left(\sqrt{\overline{V_j}}, 1\right). \tag{84}$$

By the law of total probability we have that

$$\begin{aligned} \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > R_{i,j}\right) = \\ \mathbb{P}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > R_{i,j} | V_j > M\right) \mathbb{P}\left(V_j > M\right) + \\ \sum_{v=0}^{M} \mathbb{P}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > R_{i,j} | V_j = v\right) \mathbb{P}\left(V_j = v\right). \end{aligned}$$

Which we can upper bound by

$$\mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > R_{i,j}\right) \quad \leqslant \quad \mathbb{P}\left(V_j > M\right) \; + \; \max_{v=0\ldots M} \mathbb{P}\left(\left|N_{i,j} - v\,\overline{N_i}\right| > R_{i,j} | V_j = v\right).$$

By definition of M in Equation (84) and using Equation (71) of Conjecture 2 we get that

$$\mathbb{P}\left(V_j > M\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right).$$

Now, we only have left to prove that for any $v \in [\![0, M]\!]$ we have

$$\mathbb{P}\left(\left|N_{i,j} - v\,\overline{N_i}\right| > R_{i,j} | V_j = v\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right).$$

Let us consider $v \in [\![0, M]\!]$. Let us first show that for n big enough we have that

$$n^{1.1} \max\left(\sqrt{v\,\overline{N_i}},\, 1\right) \leqslant R_{i,j}. \tag{85}$$

We have

$$\begin{aligned} n^{2.2} \max\left(v\,\overline{N_i},\, 1\right) &\leqslant n^{2.2} \max\left(M\,\overline{N_i},\, 1\right) \\ &\leqslant n^{2.2} \max\left(\overline{V_j}\,\overline{N_i} + n^{1.1}\overline{N_i} \max\left(\sqrt{\overline{V_j}}, 1\right),\, 1\right) \qquad \text{(Using Equation (84))} \\ &\leqslant \max\left(2\,n^{2.2}\,\overline{V_j}\,\overline{N_i},\; 2\,n^{3.3}\overline{N_i}\sqrt{\overline{V_j}},\; 2\,n^{3.3}\overline{N_i},\; n^{2.2}\right) \end{aligned}$$

To show Equation (85), ne only have left to prove that, for n big enough, each term in the previous maximum is smaller than $R_{i,j}^2$. First let us recall that by definition of $R_{i,j}$ in Equation (78) and from Lemma 12,

$$R_{i,j}^2 = \max\left(\omega\left(n^{\alpha+4}\right)\overline{N_i}\,\overline{V_j}, \omega\left(n^4\right)\overline{N_i}\right).$$

For n big enough we have that:

$$\begin{aligned}
&2\,n^{2.2}\,\overline{V_j}\,\overline{N_i} && \leqslant n^{\alpha+4}\overline{N_i}\,\overline{V_j} \leqslant R_{i,j}^2,\\
&2\,n^{3.3}\overline{N_i}\sqrt{\overline{V_j}} && \leqslant \begin{cases} n^4\overline{N_i} \leqslant R_{i,j}^2 & \text{when } \overline{V_j} \leqslant 1\\ n^{\alpha+4}\overline{N_i}\,\overline{V_j} \leqslant R_{i,j}^2 & \text{when } \overline{V_j} > 1 \end{cases},\\
&2\,n^{3.3}\,\overline{N_i} && \leqslant n^4\overline{N_i} \leqslant R_{i,j}^2,\\
&n^{2.2} && \leqslant R_{i,j}^2.
\end{aligned}$$

Where in the last equation we used the fact that $(i,j) \notin \mathcal{A}$, thus $R_{i,j} \geqslant \frac{n^{3.2}}{2(n+1)^2}$ and thus $R_{i,j}^2 \geqslant n^{2.3}$ for n big enough. We have shown that

$$n^{2.2}\max\left(v\,\overline{N_i},\,1\right) \leqslant R_{i,j}^2$$

and thus we have shown Equation (85). Finally we have

$$\begin{aligned}
\mathbb{P}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > R_{i,j} | V_j = v\right) &= \mathcal{O}\left(\mathbb{P}\left(\left|N_{i,j} - V_j\overline{N_i}\right| > n^{1.1}\max\left(\sqrt{v\,\overline{N_i}},\,1\right)|V_j = v\right)\right)\\
&= \widetilde{\mathcal{O}}\left(2^{-n}\right)
\end{aligned}$$

where in the last line we used Equation (72) of Conjecture 2. This concludes the proof. □

Lemma 13. *The Poisson Model 1 imply Conjecture 2.*

Proof. Let M be defined as

$$M \overset{\text{def}}{=} \overline{V_j} + n^{1.1}\max\left(\sqrt{\overline{V_j}}, 1\right) \tag{86}$$

Recall that to show Conjecture 2 we only have to show that

$$\mathbb{P}_{\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|V_j - \overline{V_j}\right| \geqslant n^{1.1}\max\left(\sqrt{\overline{V_j}}, 1\right)\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right), \tag{87}$$

$$\forall v \in [\![0, M]\!],\ \mathbb{P}_{\mathcal{C},\mathcal{C}_{\text{aux}},\mathbf{x}}\left(\left|N_{i,j} - v\,\overline{N_i}\right| > n^{1.1}\max\left(\sqrt{v\,\overline{N_i}}, 1\right) \,\middle|\, N_j = v\right) = \widetilde{\mathcal{O}}\left(2^{-n}\right) \tag{88}$$

Under the Poisson Model 1 we have that

$$N_{i,j} \sim \text{Poisson}\left(V_j\,\overline{N_i}\right), \quad V_j \sim \text{Poisson}\left(\overline{V_j}\right).$$

We will use the following fact: when $\mathbf{X}$ follows a Poisson distribution of parameter λ and $g(n) = \omega(n)$, then we have that

$$\mathbb{P}\left(|\mathbf{X} - \lambda| > g(n)\max\left(\sqrt{\lambda}, 1\right)\right) = 2^{-\omega(n)}. \tag{89}$$

Let us prove this claim. It is known [Gol17, Prop 11.15] that we have the following exponential tail bound for $\mathbf{X}$:

$$\mathbb{P}\left(|\mathbf{X} - \lambda| > r\right) \leqslant 2\,e^{\frac{-r^2}{2(\lambda+r)}}.$$

Thus,

$$\begin{aligned}
\mathbb{P}\left(|\mathbf{X} - \lambda| > g(n)\max\left(\sqrt{\lambda}, 1\right)\right) &\leqslant 2\,e^{\frac{-g(n)^2\max(\lambda,1)}{2(\lambda+g(n)\max(\sqrt{\lambda},1))}}\\
&\leqslant 2\,e^{\frac{-g(n)}{2\left(\frac{\lambda+g(n)\max(\sqrt{\lambda},1)}{g(n)\max(\lambda,1)}\right)}}.
\end{aligned}$$

We only have left to show that

$$\frac{\lambda + g(n)\max\left(\sqrt{\lambda}, 1\right)}{g(n)\max\left(\lambda, 1\right)} = \mathcal{O}(1).$$

First it is readily seen that we have that ($g(n) = \omega(n)$)

$$\frac{\lambda}{g(n)\max(\lambda,1)} = \mathcal{O}(1)\,,$$

and second,

$$\frac{g(n)\max\left(\sqrt{\lambda},1\right)}{g(n)\max(\lambda,1)} = \begin{cases} 1 = \mathcal{O}(1) & \text{if } \lambda \leqslant 1 \\ \frac{1}{\sqrt{\lambda}} = \mathcal{O}(1) & \text{if } \lambda > 1. \end{cases}$$

which concludes the proof of Equation (89). Equation (87) directly follows from Equation (89). Equation (88) also directly follow sfrom Equation (89) by noticing that $N_{i,j} = v \sim \text{Poisson}\left(v\,\overline{N_i}\right)$ when $V_j = v$. □

Proof of Proposition 6. Apply successively Lemma 13 and Proposition 12. □

Appendix G. Instantiating the Auxiliary Code $\mathcal{C}_{\text{aux}}$ with an Efficient Decoder

We use here notation from §7. In particular, we suppose the auxiliary code $\mathcal{C}_{\text{aux}}$ is a product of b small random codes where

$$b = \Theta(\log n). \tag{90}$$

We have to show that for such b, the analyses from Propositions 2 and 5 still hold. Indeed, these analyses were done as if $\mathcal{C}_{\text{aux}}$ were a random code equipped with genie aided decoders. Here we compute $\mathscr{H}$ as a subset of

$$\widetilde{\mathscr{H}} \subseteq \left\{(\mathbf{h},\mathbf{c}_{\text{aux}}) \in \mathcal{C}^\perp \times \mathcal{C}_{\text{aux}} \;:\; \forall i \in [\![1,b]\!]\,,\; |\mathbf{h}_{\mathscr{N}}(i)| = \tfrac{w}{b} \text{ and } |\mathbf{h}_{\mathscr{P}}(i) + \mathbf{c}_i| = \tfrac{t_{\text{aux}}}{b}\right\}$$

by decoding each parity-check performing an exhaustive search on each block. We have therefore to show that in this case,

i. the bias

$$\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}}{\text{bias}} \left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right)$$

is of the same order as that given by Proposition 2,

ii. and the number of candidates to test

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}\left(|\mathscr{S}|\right)$$

is of the same order as that given by Proposition 5.

To prove item i., we first suppose that $\mathbf{e}_{\mathscr{P}}$ and $\mathbf{e}_{\mathscr{N}}$ have a weight which is fairly distributed, that is:

$$\forall i \in [\![1,b]\!]\,,\; |\mathbf{e}_{\mathscr{P}}(i)| = \tfrac{t-u}{b} \text{ and } |\mathbf{e}_{\mathscr{N}}(i)| = \tfrac{u}{b}. \tag{91}$$

This happens with a probability:

$$\mathbb{P}_{\text{succ}} = \frac{\binom{s/b}{(t-u)/b}^b \binom{(n-s)/b}{u/b}^b}{\binom{s}{t-u}\binom{n-s}{u}} = \Omega\left(n\left(\tfrac{b}{cn}\right)^b\right) \tag{92}$$

where c is constant in n. So we only need to iterate the whole double-RLPN algorithm a sub-exponential number of times, namely at most $\frac{1}{\mathbb{P}_{\text{succ}}}$ times. Note that (91) is not a necessary condition to achieve our decoding so this overcost is overestimated.

Now, assuming Condition (91), then we can see the bias above as the product of b independent biases involving smaller vectors. More formally, we have

$$\begin{aligned} &\underset{(\mathbf{h},\mathbf{c}_{\text{aux}}) \xleftarrow{\$} \widetilde{\mathscr{H}}}{\text{bias}} \left(\langle \mathbf{c}_{\text{aux}} + \mathbf{h}_{\mathscr{P}}, \mathbf{e}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}}\rangle\right) \\ &\qquad = \prod_{i=1}^{b} \underset{(\mathbf{h}(i),\mathbf{c}_{\text{aux}}(i)) \xleftarrow{\$} \widetilde{\mathscr{H}_i}}{\text{bias}} \left(\langle \mathbf{c}_{\text{aux}}(i) + \mathbf{h}_{\mathscr{P}}(i), \mathbf{e}_{\mathscr{P}}(i)\rangle + \langle \mathbf{e}_{\mathscr{N}}(i), \mathbf{h}_{\mathscr{N}}(i)\rangle\right) \end{aligned} \tag{93}$$

where

$$\begin{aligned} \widetilde{\mathscr{H}_i} \overset{\text{def}}{=} \Big\{ &(\mathbf{h}_{\mathscr{P}}(i), \mathbf{h}_{\mathscr{N}}(i), \mathbf{c}_{\text{aux}}(i)) \in \left(\mathcal{C}_{\mathscr{P}(i)\cup\mathscr{N}(i)}\right)^\perp \times \mathcal{C}_i \\ &\qquad : \; |\mathbf{h}_{\mathscr{N}}(i)| = \tfrac{w}{b} \text{ and } |\mathbf{h}_{\mathscr{P}}(i) + \mathbf{c}_i| = \tfrac{t_{\text{aux}}}{b} \Big\} \end{aligned} \tag{94}$$

Moreover, let us degrade the Constraints (7) of Proposition 2 by replacing the polynomial factor n^α by a super-polynomial

$$A \stackrel{\text{def}}{=} \frac{n^{\alpha-1+\log(c)+\log(n)}}{\log(n)^{\log(n)}}. \tag{95}$$

On the one hand, this super-polynomial factor is multiplied to the final complexity, but on the other hand the new constraint (with the original one (8)) induces:

$$\frac{\binom{(n-s)/b}{w/b}\binom{s/b}{t_{\text{aux}}/b}}{2^{(k-k_{\text{aux}})/b}} = \omega\left(\frac{n^{\alpha/\log(n)}}{\delta^{2/\log(n)}}\right) \tag{96}$$

and

$$\frac{\binom{(n-s)/b}{w/b}\binom{s/b}{t_{\text{aux}}/b}}{2^{k/b}} = \mathcal{O}\left(n^{\alpha/\log(n)}\right) \quad \text{and} \quad \frac{\binom{s/b}{t_{\text{aux}}/b}}{2^{(s-k_{\text{aux}})/b}} = \mathcal{O}\left(n^{\alpha/\log(n)}\right). \tag{97}$$

Which allows us to say, using Proposition 2, that for all $i \in [\![1, b]\!]$ and for a proportion $1 - o(1)$ of codes $\mathcal{C}_i$ and $\mathcal{C}_{\mathscr{P}(i)\cup\mathscr{N}(i)}$:

$$\underset{(\mathbf{h}(i),\mathbf{c}_{\text{aux}}(i))\stackrel{\$}{\leftarrow}\overline{\mathscr{H}}_i}{\text{bias}}\left(\langle \mathbf{c}_{\text{aux}}(i) + \mathbf{h}_{\mathscr{P}}(i), \mathbf{e}_{\mathscr{P}}(i)\rangle + \langle \mathbf{e}_{\mathscr{N}}(i), \mathbf{h}_{\mathscr{N}}(i)\rangle\right) = \delta^{1/\log(n)}(1 - o(1)). \tag{98}$$

By specifying the values of both $o(1)$ (see proof of Proposition 2 in Appendix A), we can deduce that i. is verified.

To verify item ii., we can adapt Section D to show that

$$\mathbb{E}_{\mathcal{C},\mathcal{C}_{\text{aux}}}(|\mathscr{S}|) = \widetilde{\mathcal{O}}\left(\max_{(i,j)\in\mathcal{A}} \frac{\binom{s/b}{j}^b\binom{(n-s)/b}{i}^b}{2^{n-k}}\right) + 1 \tag{99}$$

where

$$\mathcal{A} \stackrel{\text{def}}{=} \left\{(i,j) \in [\![0, \tfrac{n-s}{b}]\!] \times [\![0, \tfrac{s}{b}]\!], \frac{K_{w/b}^{((n-s)/b)}(u/b)\, K_{t_{\text{aux}}/b}^{(s/b)}((t-u)/b)}{K_{w/b}^{((n-s)/b)}(i)\, K_{t_{\text{aux}}/b}^{(s/b)}(j)} \leqslant n^{2/b}\right\}, \tag{100}$$

$$\mathscr{S} \stackrel{\text{def}}{=} \{\mathbf{s} \in \mathbb{F}_2^{k_{\text{aux}}} : \widehat{f_{\mathbf{y},\widetilde{\mathscr{H}},\mathbf{G}_{\text{aux}}}}(\mathbf{s}) \geqslant \frac{\delta}{2}\widetilde{H}\}, \tag{101}$$

and

$$\widetilde{H} \stackrel{\text{def}}{=} \frac{\binom{(n-s)/b}{w/b}^b\binom{s/b}{t_{\text{aux}}/b}^b}{2^{k-k_{\text{aux}}}}. \tag{102}$$

Finally, up to a sub-exponential factor, the above expectation is of the same order as in Proposition 5.

Appendix H. Proofs of the statements made in Section 8

Proof of Proposition 7

Proposition 7. *Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ and consider some word $\mathbf{y} = \mathbf{x} + \mathbf{e} \in \mathbb{R}^n$ where $\mathbf{x}$ is in Λ. Let $\widetilde{\mathscr{W}}$ be the set of dual lattice vectors of Euclidean weights in $(w-\varepsilon, w+\varepsilon)$ in $\Lambda^\vee$ and let $f_{\widetilde{\mathscr{W}}}(\mathbf{y}) \stackrel{def}{=} \sum_{\mathbf{w}\in\widetilde{\mathscr{W}}} \cos(2\pi\langle \mathbf{x}, \mathbf{y}\rangle)$. We have*

$$f_{\widetilde{\mathscr{W}}}(\mathbf{y}) = \frac{1}{|\Lambda^\vee|}\sum_{j\geqslant 0}\frac{N_j}{j^n\,(2\pi)^{n/2}}\Big((2\pi(w+\varepsilon)j)^{n/2}J_{n/2}(2\pi(w+\varepsilon)j) - (2\pi(w-\varepsilon)j)^{n/2}J_{n/2}(2\pi(w-\varepsilon)j)\Big) \tag{17}$$

where N_j is the number of words of Euclidean norm j in $\Lambda + \mathbf{e}$ and J_ν is the Bessel function of the first kind of order[4] ν.

[4]Here the j's belong to the discrete set of all possible norms in the lattice and should not be viewed as an integer value.

It is helpful to notice before the following link between the Bessel functions and the Fourier transform of the indicator function $\mathbb{1}_{\leqslant w}$ of the words of Euclidean norm $\leqslant w$ in $\mathbb{R}^n$ (see [DDRT23, Fact 4.11])

Lemma 14. *We have for any positive integer n, any $w \geqslant 0$, any $\mathbf{x}$ in $\mathbb{R}^n$*

$$\widehat{\mathbb{1}_{\leqslant w}}(\mathbf{x}) = \left(\frac{w}{\|\mathbf{x}\|_2}\right)^{n/2} J_{n/2}\left(2\pi w\|\mathbf{x}\|_2\right)$$

where $\widehat{f}(\mathbf{x}) = \int_{\mathbb{R}^n} f(\mathbf{x})e^{-2i\pi\langle \mathbf{x},\mathbf{y}\rangle}d\mathbf{y}$ for $f : \mathbb{R}^n \to \mathbb{C}$.

Proof of Proposition 7. First, notice that,

$$\begin{aligned} f_{\widehat{\mathscr{W}}}(\mathbf{y}) &= \frac{1}{2}\sum_{\mathbf{w}\in\widehat{\mathscr{W}}}\left(e^{2i\pi\langle \mathbf{w},\mathbf{y}\rangle} + e^{-2i\pi\langle \mathbf{x},\mathbf{y}\rangle}\right) \\ &= \sum_{\mathbf{w}\in\widehat{\mathscr{W}}} e^{-2i\pi\langle \mathbf{w},\mathbf{y}\rangle} \quad (\mathbf{w}\mapsto -\mathbf{w} \text{ is a bijection in } \mathscr{W}) \\ &= \sum_{\mathbf{w}\in\Lambda^\vee}\left(\mathbb{1}_{\leqslant w+\varepsilon}(\mathbf{w}) - \mathbb{1}_{\leqslant w-\varepsilon}(\mathbf{w})\right)e^{-2i\pi\langle \mathbf{w},\mathbf{y}\rangle} \end{aligned} \tag{103}$$

Recall now the Poisson summation formula, for any $\mathbf{y} \in \Lambda + \mathbf{e}$ and sufficiently regular function f,

$$\sum_{\mathbf{x}\in\Lambda^\vee} f(\mathbf{x})e^{-2i\pi\langle \mathbf{x},\mathbf{y}\rangle} = \frac{1}{|\Lambda^\vee|}\sum_{\mathbf{x}\in\Lambda+\mathbf{e}}\widehat{f}(\mathbf{x})$$

Plugging this formula into Equation (103) yields to,

$$\begin{aligned} f_{\widehat{\mathscr{W}}}(\mathbf{y}) &= \frac{1}{|\Lambda^\vee|}\sum_{\mathbf{x}\in\boldsymbol{\Lambda}+\mathbf{e}}\left(\widehat{\mathbb{1}_{\leqslant w+\varepsilon}}(\mathbf{x}) - \widehat{\mathbb{1}_{\leqslant w-\varepsilon}}(\mathbf{x})\right) \\ &= \frac{1}{|\Lambda^\vee|}\sum_{j\geqslant 0}\frac{N_j}{j^{n/2}}\left((w+\varepsilon)^{n/2}J_{n/2}\left(2\pi(w+\varepsilon)j\right) - (w-\varepsilon)^{n/2}J_{n/2}(2\pi(w-\varepsilon)j)\right) \\ &= \frac{1}{|\Lambda^\vee|}\sum_{j\geqslant 0}\frac{N_j}{(2\pi)^{n/2}\,j^n}\Big(\left(2\pi(w+\varepsilon)j\right)^{n/2}J_{n/2}\left(2\pi(w+\varepsilon)j\right) \\ &\qquad\qquad - \left(2\pi(w-\varepsilon)j\right)^{n/2}J_{n/2}(2\pi(w-\varepsilon)j)\Big) \end{aligned} \tag{104}$$

which concludes the proof. □

An Approximation. We have also an approximate form for $f_{\widehat{\mathscr{W}}}(\mathbf{y})$ which is given by

$$f_{\widehat{\mathscr{W}}}(\mathbf{y}) \approx \frac{4\pi\varepsilon}{|\Lambda^\vee|}\sum_{j\geqslant 0} jN_j\left(\frac{w}{j}\right)^{n/2}J_{n/2-1}(2\pi wj). \tag{105}$$

This follows from the fact that

$$\frac{d}{dx}\left(x^{n/2}J_{n/2}(x)\right) = x^{n/2}J_{n/2-1}(x). \tag{106}$$

Let,

$$X \overset{\text{def}}{=} 2\pi wj \quad \text{and} \quad h \overset{\text{def}}{=} 2\pi\varepsilon j$$

Notice that,

$$\begin{aligned} &\left((2\pi(w+\varepsilon)j)^{n/2}J_{n/2}\left(2\pi(w+\varepsilon)j\right) - (2\pi(w-\varepsilon)j)^{n/2}J_{n/2}(2\pi(w-\varepsilon)j)\right) \\ &\qquad = (X+h)^{n/2}J_{n/2}(X+h) - (X-h)^{n/2}J_{n/2}(X-h) \end{aligned}$$

From Equation (106),

$$\begin{aligned}(X+h)^{n/2}J_{n/2}(X+h)-(X-h)^{n/2}J_{n/2}(X-h) &\approx 2h\,\frac{d}{dX}\left(X^{n/2}J_{n/2}(X)\right)\\ &= 2h\;X^{n/2}J_{n/2-1}(X)\\ &= (4\pi\varepsilon j)\;(2\pi wj)^{n/2}J_{n/2-1}(2\pi wj)\end{aligned}$$

Plugging this into Equation (104) yields (105).

We also recall that we make the approximation

$$f_{\mathscr{W}}(\mathbf{y}) \approx \frac{N}{\left|\widetilde{\mathscr{W}}\right|}\; f_{\widetilde{\mathscr{W}}}(\mathbf{y}) \tag{107}$$

The number $N^{\vee}_{\leqslant x}$ of dual vectors of length $\leqslant x$ can be approximated using the Gaussian heuristic:

$$N^{\vee}_{\leqslant x} \approx \frac{x^n}{\sqrt{n\pi}\;\left(\frac{n}{2\pi e}\right)^{n/2}}\;\frac{1}{|\Lambda^{\vee}|}$$

Thus we have:

$$\left|\widetilde{\mathscr{W}}\right| = N^{\vee}_{\leqslant w+\varepsilon} - N^{\vee}_{\leqslant w-\varepsilon} \approx \frac{(w+\varepsilon)^n-(w-\varepsilon)^n}{\sqrt{\frac{n}{2\pi e}}^{n}\cdot\sqrt{\pi n}\cdot|\Lambda^{\vee}|} \approx \frac{2n\varepsilon w^{n-1}}{\sqrt{\frac{n}{2\pi e}}^{n}\;\sqrt{\pi n}\;|\Lambda^{\vee}|}$$

Putting this into Equation (107) shows,

$$f_{\mathscr{W}}(\mathbf{y}) \approx N\;\frac{|\Lambda^{\vee}|\;\sqrt{n\pi}\left(\frac{n}{2\pi e}\right)^{n/2}}{2n\varepsilon w^{n-1}}\;f_{\widetilde{\mathscr{W}}}(\mathbf{y})$$

and after some further computation

$$\begin{aligned}f_{\mathscr{W}}(\mathbf{y}) &\approx N\;|\Lambda^{\vee}|\,\frac{\sqrt{n\pi}\left(\frac{n}{2\pi e}\right)^{n/2}}{2n\varepsilon w^{n-1}}\;\frac{4\pi\varepsilon}{|\Lambda^{\vee}|}\;\sum_{j\geqslant 0} jN_j\;\left(\frac{w}{j}\right)^{n/2}\;J_{n/2-1}(2\pi wj)\\ &= N\;\frac{\sqrt{n\pi}}{2nw^{n-1}}\left(\frac{n}{2\pi e}\right)^{n/2}\;4\pi\sum_{j\geqslant 0} jN_j\;\left(\frac{w}{j}\right)^{n/2}\;J_{n/2-1}(2\pi wj)\\ &= N\;\frac{\sqrt{n}\;n^{n/2}}{n}\;\frac{1}{w^{n-1}}\;\frac{\sqrt{\pi}\;\pi}{\pi^{n/2}}\;\frac{4}{2\;2^{n/2}}\;\frac{1}{e^{n/2}}\;\sum_{j\geqslant 0} N_j\;w^{n/2}\frac{1}{j^{n/2-1}}\;J_{n/2-1}(2\pi wj)\\ &= N\;\sqrt{n}\;\sqrt{\pi}\;e^{-1}\;n^{n/2-1}\;\pi^{-(n/2-1)}\;2^{-(n/2-1)}e^{-(n/2-1)}\sum_{j\geqslant 0} N_j\left(\frac{1}{wj}\right)^{n/2-1}\;J_{n/2-1}(2\pi wj)\\ &= N\frac{\sqrt{n\pi}}{e}\sum_{j\geqslant 0} N_j\left(\frac{n}{2\pi ewj}\right)^{n/2-1}\;J_{n/2-1}(2\pi wj)\end{aligned}$$