Beyond Threshold Security: Additive Secret Sharing under Hamming-Weight Leakage

Aniruddha Biswas[1], Jihun Hwang[1], Hemanta K. Maji[1], Ilya D. Shkredov[2], and Xiuyu Ye[1]

[1]Department of Computer Science, Purdue University
[2]Department of Mathematics, Purdue University

Abstract

Side-channel attacks threaten even foundational primitives such as secret sharing, undermining threshold cryptography, and masking countermeasures. We study additive secret sharing over $\mathbb{Z}/N\mathbb{Z}$ under Hamming-weight leakage, focusing on local leakage resilience: statistical independence between the secret and the total leakage.

Prior guarantees were limited to Mersenne primes $N = 2^n - 1$ with $k \geqslant 5$, where insecurity was bounded by $n^{-k/4}$. For $k = 2$, the scheme is insecure, while for $k = 3, 4$ and for non-Mersenne moduli, no guarantees were known.

We remove these restrictions. For all N sufficiently close to 2^n, we prove insecurity at most $n^{-k/2}$ for every $k \geqslant 3$. This yields the first guarantees for $k = 3, 4$ and for non-Mersenne moduli, and (after our result) even square-root-sized moduli are less insecure than what previous work guaranteed. We also prove a matching lower bound, showing that our decay exponent is optimal.

Our proof introduces new analytic and spectral techniques to leakage-resilience analysis, combining Fourier analysis, complex analysis, and matrix methods. Our intermediate results resolve the ternary problem for Hamming slices, implying that the associated Cayley graphs of near-central slices have diameter at most 3.

Keywords. Secret sharing, side channel attacks, local leakage resilience, and Hamming weight leakage.
Technical keywords. Fourier analysis, generating functions, complex analysis, and matrix analysis.

Contents

1 Introduction

Secret sharing provides perfect privacy against threshold corruption: learning fewer than the reconstruction threshold of shares reveals nothing about the secret [Sha79, Bla79]. This all-or-nothing guarantee underlies threshold cryptography and a large body of masking-based countermeasures [ISW03, NRR06, NRS11]. Real implementations, however, are exposed to *distributed leakage*: side-channel measurements may reveal a tiny amount of information about many shares at once, and these weak signals can accumulate. Even extremely coarse per-share statistics, such as *Hamming weight* inferred from timing or power measurements, fall outside the classical corruption model yet may still correlate with the secret [Koc96, KJJ99, Mes00, BCO04]. Quantitative guarantees for secret sharing under such leakage are therefore essential, especially in light of NIST's standardization efforts on threshold schemes and related masked circuits [BMV19, BP26, NIS26].

We study a clean model of this phenomenon for *additive secret sharing*, one of the simplest and most widely used sharing mechanisms in practice. Let $G = \mathbb{Z}/N\mathbb{Z}$, identify each element of G with its canonical representative in $\{0, 1, \ldots, N-1\}$, and write $\mathrm{wt}(x)$ for the Hamming weight of the binary expansion of x. To share a secret $s \in G$ into $k \geqslant 2$ shares, sample $(s_1, s_2, \ldots, s_k) \in G^k$ uniformly subject to

$$s_1 + s_2 + \cdots + s_k = s.$$

The adversary does not observe the shares themselves, but only the leakage vector

$$\big(\mathrm{wt}(s_1), \mathrm{wt}(s_2), \ldots, \mathrm{wt}(s_k)\big)\,.$$

This is already a nontrivial model for side-channel threats. The guiding question is: *after one forgets almost everything about each share, can the aggregate leakage still retain a detectable imprint of the secret*?

Security metric. We investigate *local leakage resilience* [BDIR18, BDIR21]. Let $D(s)$ denote the distribution of the weight vector for fixed secret s, and let $D(U)$ denote the same distribution when the secret is uniform in G. Insecurity is measured by the total variational distance[1]

$$E_k(s) \;\coloneqq\; \Big\| D(s) - D(U) \Big\|_{\mathrm{TV}} = \frac{1}{2} \sum_{\mathbf{w} \in W^k} \Big| D(s)(\mathbf{w}) - D(U)(\mathbf{w}) \Big|, \quad (1) \qquad \text{and } E_k \;\coloneqq\; \max_{s \in G} E_k(s),$$

where $W \;\coloneqq\; \mathrm{wt}(G)$, the set of all possible weights. A small upper bound on E_k rules out every distinguisher based on the leaked Hamming weights. In this sense, it is stronger than analyzing only a particular statistic, such as bias, mutual information, or guessing entropy [DDF14, GBTP08, SMY09]. Conversely, a large value of E_k means that the leakage profile for some secret is atypical, exposing the scheme's vulnerability.

Even this stripped-down model is delicate. Over $\mathbb{F}_2$ vector spaces, there is an immediate obstruction: writing x as $(x_i)_i$ in a fixed binary basis, one has $\mathrm{wt}(x) = \sum_i x_i \pmod 2$. So the parities of the leaked weights reveal the parity of the secret's weight. Over cyclic groups $\mathbb{Z}/N\mathbb{Z}$, by contrast, no such general obstruction is known. The problem seems challenging even for $N = 2^n$, which is widely used in practice.

[1] Total variation distance measures how distinguishable two probability distributions are: it is the largest possible difference between the probabilities they assign to the same event, so 0 means identical, and values closer to 1 mean easier to tell apart.

Our main theorem (informal). *For every fixed $k \geqslant 3$ and every modulus N satisfying $|N - 2^n| \leqslant 2^n/n$, we have $E_k = n^{-k/2+\mathcal{O}(1)}$. Furthermore, $E_k \to 0$ as $n \to \infty$, for all $k \geqslant 3$, and E_2 is a positive constant.*

More precisely, we prove upper and lower bounds of this form. This improves on the only prior result we are aware of, due to Faust et al. [FMM+24], which treated the highly specialized Mersenne-prime case $N = 2^n - 1$ and obtained $E_k \leqslant n^{-k/4}$ only for $k \geqslant 5$. Our theorem essentially has the correct dependence on k and shows that neither the threshold $k = 5$ nor the specific Mersenne moduli are intrinsic: security already appears at $k = 3$ and persists over a robust window of moduli around 2^n.

Additive-combinatorial viewpoint. For $w \in W$, the *Hamming slice* is $S_w := \{x \in G \colon \mathrm{wt}(x) = G\}$. These sets are also called digital sum sets [Yat90]; for brevity, "digital sets" here. For digital set S_w, note:

$$D(s)(\mathbf{w}) = \frac{1}{N^{k-1}} \cdot \# \left\{ \mathbf{x} \in S_{\mathbf{w}_1} \times S_{\mathbf{w}_2} \times \cdots \times S_{\mathbf{w}_k} \,:\, \mathbf{x}_1 + \mathbf{x}_2 + \cdots + \mathbf{x}_k = s \right\},$$

so the leakage question becomes a structure additive-combinatorics problem. How regular are the representation counts in $S_w + S_w$? What is the additive energy of S_w? When do higher-fold sums $S_{w_1} + \cdots + S_{w_k}$ mix across G? Equivalently, what's the diameter of the Cayley graphs $\mathrm{Cay}(G, S_w)$? We adopt this viewpoint: *understanding Hamming-weight leakage in additive secret sharing amounts to understanding the additive geometry of Hamming slices in $\mathbb{Z}/N\mathbb{Z}$.*

Our structural results (informal). For central weights w (that is, $w \approx n/2$), we prove that the Cayley graph $\mathrm{Cay}(G, S_w)$ has diameter (at most) 3; that is, $S_w + S_w + S_w = G$. At a high level, although Hamming slices are neither algebraically structured nor pseudorandom, their central layers flatten rapidly under a small number of additive convolutions. This rapid smoothing is exactly what determines the exact insecurity.

1.1 Our Contributions

At present, it remains unclear which mathematical tools are best suited to analyzing leakage resilience. We place the problem at the interface of additive combinatorics and Fourier analysis, where it admits a precise formulation, connects to classical questions, and yields a practically motivated testbed. As evidence, we also resolve the *ternary representation problem* for near-central Hamming slices.

Upper bounds. We prove that there is an absolute constant $c > 0$ such that the following hold.

1. Theorem 2: If $|N - 2^n| \leqslant 2^n/n$, then the insecurity is at most $(cn)^{-k/2+5/4}$
2. Theorem 5: If $N = 2^n - 1$, then for odd n, the insecurity is at most $(cn)^{-k/2+1} \cdot \log n$
3. Theorem 1: If $N = 2^n - 1$ and $n \geqslant 3$ is prime, then the insecurity is at most $c \cdot n^{-k/2+1} \cdot \log n$

The leading terms of all our upper and lower bounds are of the shape: $n^{-\frac{1}{2}\cdot k + a + b\cdot\frac{\log\log n}{\log n} + \frac{k\log c}{\log n}}$; here $a, c > 0$ and $b \in \{0, 1\}$. As we shall see, the maximum gap between our upper and lower bounds is $n^{3/4}$ for near-dyadic moduli (those N that are close to a power of two).

Before our work, the only nontrivial upper bound was for $k \geqslant 5$ over Mersenne prime moduli $N = 2^n - 1$, where the insecurity was shown to decay only as $n^{-k/4}$ [FMM+24]; Appendix J includes a summary. Our results sharpen this in three ways. We establish security for every $k \geqslant 3$, settling the previously open cases $k = 3, 4$. We improve the decay exponent from $k/4$ to $k/2$, which the lower bounds below show is optimal. Now, even square-root-sized moduli are less insecure than previously guaranteed. And, we extend beyond the rigid Mersenne-prime setting to the broad near-dyadic regime $|N - 2^n| \leq 2^n/n$.

Technical approach summary. We introduce Fourier-friendly energy proxies for leakage resilience, enabling tools from additive combinatorics, spectral theory, transfer matrices, and complex analysis. Our opening is a Fourier-analytic gambit: sacrifice one share to pass to more tractable energy quantities, yet still recover the correct exponent up to constants (compare Theorem 1 and Theorem 6). This is particularly striking because each share contributes a constant amount to that exponent; ignoring a share seems self-defeating, particularly for the delicate "small $k = 3, 4$" cases. Next, our technical follow-up isolates a transfer-matrix/spectral estimate, which is new even to the digital sums literature in analytic number theory. Finally, the extension to the near-dyadic regime replaces the rigid cyclic-orbit structure of [FMM+24] with a Bernoulli-shift viewpoint and a transference argument showing that near-dyadic moduli are controlled perturbations of the dyadic model. Section 3 and Section 4 have the details.

Structural results. Consider the Cayley graph $\mathrm{Cay}(G, S_w)$ on G, where $x \to y$ iff $y - x \in S_w$.

Theorem 11: If $N = 2^n - 1$, odd n, and $\#S_w \gg N \cdot n^{-3/5}$, then the diameter of $\mathrm{Cay}(G, S_w)$ is $\leqslant 3$.

That is, every element in G is expressible as the sum of three elements in S_w, a ternary representation. The key input is our (additive) energy estimate for the Hamming slice, Lemma 1:

$$E^+(S_w) \ll N^{-1} \cdot \binom{n}{w}^4 \; + \; N^3 \cdot n^{-3},$$

For near-central w, the second term is lower order, leading to $S_w + S_w$ covering nearly all of G, and then

$$S_w + S_w + S_w = G. \tag{2}$$

The ternary problem (2) is of independent interest – even in the case of Mersenne primes – since the symmetry group of the set S_w is tiny compared to the size of S_w itself. To place our result in context, let p be a prime and $\Gamma \leqslant \mathbb{F}_p^*$. The existence form of the ternary problem asks whether $\Gamma + \Gamma + \Gamma = \mathbb{F}_p$. For $|\Gamma| = \Omega\big(p^{3/4}\big)$, despite $\Gamma + \Gamma$ missing only $\mathcal{O}(|\Gamma|)$ elements of $\mathbb{F}_p^*$, yet this level of control still does not suffice to resolve this problem; it is a well-known open question (see, for example, [AB14]). In contrast, for the digital set S_w, we solve the ternary representation problem.

This seems paradoxical: We settled the ternary problem for highly structured S_w, yet it remains out of reach for multiplicative subgroups, often viewed as more "random" objects (see [KS99]). From this perspective, Lemma 1 is a central contribution; even for Mersenne primes, it strictly strengthens L_∞-bounds by Parseval's identity or Chang's inequality [TV06, Section 4.6]. Fourier methods show that $S_w + S_w$ misses $\mathcal{O}(|S_w|)$ elements of G – precisely as in the case of multiplicative subgroups of size $\Omega(p^{3/4})$; and this alone doesn't give (2). Thus, our Lemma 1 is indeed a much deeper result. Its proof avoids exponential sums and instead relies on highly sophisticated methods that seem relatively new within the number theory community (see, for example, [Gel68, MS97, MR09]).

Lower bounds. Our upper bounds are essentially optimal. For an absolute constant $d > 0$, we prove the following lower bounds:

1. Theorem 7: If $|N - 2^n| \leqslant 2^{(1-\varepsilon)n}$, then the insecurity is $\geqslant \varepsilon^{1/2} \cdot (dn)^{-k/2+1/2}$
2. Theorem 6: If $N = 2^n - 1$, n is odd, and k is even, then the insecurity is $\geqslant (dn)^{-k/2+1}$
3. Theorem 8: If $|N - 2^n| \leqslant \varepsilon \cdot 2^n$ and $k = 2$, then the insecurity is $\geqslant 1 - \mathcal{O}\big(\varepsilon + n^{-1/2}\big)$.

We also identify a set of Fourier frequencies that provably carry information about the secret, yielding an explicit, though not necessarily exhaustive, collection of informative modes relevant to side-channel attacks.

Compare Theorem 1–Theorem 2–Theorem 5 with Theorem 6–Theorem 7; the dependence on k is essentially sharp. For $N = 2^n - 1$ and n an odd prime, the bounds match up to logarithmic factors. The lower bounds are particularly notable: such Ω-results are typically difficult in analytic number theory [IK21], but here the strong structure of Hamming-weight slices supports a delicate Fourier analysis, including precise control of signs, yielding both sharp upper and lower bounds. Lemma 1 indicates that these sets exhibit behavior even stronger than one would usually expect from multiplicatively rich sets of comparable size.

Closing remark. For even k, Theorem 6 suggests an $n^{-k/2+1}$ lower bound; for odd k, Theorem 7 suggests $n^{-k/2+1/2}$. Which exponent is correct? Possibly both. For even k, Theorem 1 matches Theorem 6, showing its tightness. For odd k, Figure 3 supports an $n^{-k/2+1/2}$ scaling for $E_3(0)$.

1.2 AI Disclosure

Use of AI tools. We used Google AI Ultra (Gemini) and ChatGPT Pro in a limited, auxiliary role.

1. Gemini suggested the carry-automaton viewpoint for Theorem 9.
2. ChatGPT suggested the phase $\phi = \exp(-\imath/\sqrt{n})$ in Theorem 7 and the dispersion lemma (Lemma 25). It also provided an optimized proof of the compression lemma Lemma 26, which we adapted in this draft.
3. ChatGPT supported numerical experiments and data generation (see Figure 1, Figure 2, and Figure 3).

All proofs and exposition were independently developed and verified by the authors.

2 Brief Preliminaries

We begin with some brief preliminaries; Appendix A has a more comprehensive one.

Background. Let $W = \{0, 1, \ldots, n\}$, where n is the closest power of 2 to N. Note that $\mathrm{wt}(G) \subseteq W$. For Fourier analysis over G, define $\mathrm{e}_N(x) := \exp(2\pi\imath \cdot x/N)$. Sets are equivalent to their characteristic functions. For $0 \leqslant t < N$, the corresponding (normalized) Fourier coefficient of $S \subseteq G$ is:

$$\widehat{S}(t) := \frac{1}{N} \sum_{x \in S} \mathrm{e}_N(-xt). \tag{3}$$

Local leakage resilience of additive secret sharing. Continuing from the notation introduced in the introduction, the *insecurity* of the additive secret sharing of a specific secret s against Hamming weight leakage in the local leakage resilience metric was defined by [BDIR18, BDIR21] as:

$$E_k(s) \;:=\; \Big\| D(s) - D(U) \Big\|_{\mathrm{TV}} = \sum_{\mathbf{w}\in W^k} \left| \sum_{t\neq 0} \mathrm{e}_N(-st) \prod_{j=1}^{k} \widehat{S_{\mathbf{w}_j}}(t) \right|. \tag{4}$$

Asymptotic notation. Standard Vinogradov $\gg$, $\asymp$, $\ll$, and asymptotic $\mathcal{O}(\cdot)$ and $\mathrm{o}(\cdot)$ notations are used.

3 Upper Bound: $N = 2^n - 1$

To introduce our new Fourier proxies, it is instructive to begin with our upper bound on insecurity for $N = 2^n - 1$, where n is an odd prime; N *itself need not be a prime.*

Theorem 1. *$E_k(s) \ll n^{-k/2+1} \log n$ for any odd prime n, $N = 2^n - 1$, $k \geqslant 3$, and $s \in \mathbb{Z}/N\mathbb{Z}$.*

To upper-bound $E_k(s)$, we introduce a new analytic quantity:

$$\text{Our new Fourier proxy:} \qquad F_m \;:=\; \sum_{\mathbf{w}\in W^m} \sqrt{\sum_{t\neq 0} \prod_{j=1}^{m} \left|\widehat{S_{\mathbf{w}_j}}(t)\right|^2} \tag{5}$$

Step 1. Lemma 7 in Appendix B.1 proves that

$$E_k(s) \leqslant F_{k-1}. \tag{6}$$

This result holds for arbitrary finite abelian groups and arbitrary leakage, and is best viewed as a purely functional-analytic statement: it arises from an ℓ^2 operator-norm bound in the Fourier domain (via Cauchy-Schwarz), independent of any structure specific to Hamming weight.

Conceptually, this bound trades off one share for a more analytically tractable, secret-independent quantity. Previous works like [BDIR18, FMM+24] instead applied a naïve triangle inequality (see Equation 28), leading to expressions in which each summand is a product of k Fourier coefficients. In contrast, our reduction yields products of only $(k-1)$ coefficients, with no direct comparison between the two bounds. Empirically (and ultimately analytically) this reduction proves decisive, particularly for small k, where it enables strictly sharper bounds (see Figure 1).

Step 2. Lemma 9 in Appendix B.2 proves that

$$F_m \leqslant n^{-1/2} \cdot F_{m-1}. \tag{7}$$

This uses the fact that, for any $w \in \{1, 2, \ldots, n-1\}$, the *doubling map* $x \longmapsto 2 \cdot x \pmod N$ induces length-n orbits on S_w when n is a prime. This structural property was also used by Faust et al. [FMM+24], though in conjunction with the triangle-inequality-based approach mentioned above. Applying Equation 7 iteratively, this result scaffolds down to:

$$F_m \leqslant n^{-(m-1)/2} \cdot F_1, \tag{8}$$

thereby reducing the problem to controlling the base case F_1.

Step 3. It remains to estimate:

$$F_1 = \sum_{w \in W} \sqrt{\sum_{t \neq 0} \left|\widehat{S_w}(t)\right|^2} \asymp \sum_{w \in W} \sqrt{\binom{n}{w} \cdot 2^{-n}}$$

The last relation is by Parseval's identity. Lemma 12 in Appendix B.3 proves that $F_1 \ll n^{1/4}$, via standard Gaussian approximations to the Binomial distribution.

Step 4. Putting things together, we get:

$$E_k(s) \leqslant F_{k-1} \leqslant n^{-(k-2)/2} \cdot F_1 \ll n^{-(k-2)/2} \cdot n^{1/4} = n^{-k/2+5/4}. \tag{9}$$

Touching base. This yields an insecurity bound of at most $\leqslant n^{-k/2+5/4}$, capturing the correct $k/2$ exponent but falling short of the constant in Theorem 1. Nevertheless, it already establishes security for $k = 3, 4$, resolving previously open cases. Sharpening the constant is particularly impactful for small k, where it significantly strengthens the resulting bounds.

Pinpointing the slack. Experiments indicate the primary source of slack to be the Step 2 inequality $F_2 \leqslant n^{-1/2} \cdot F_1$. Accordingly, we stop the at F_2 (rather than F_1) and estimate it directly. In summary,

$$E_k(s) \leqslant F_{k-1} \leqslant n^{-(k-3)/2} \cdot F_2$$

and it remains to upper-bound

$$F_2 = \sum_{w_1, w_2 \in W} \sqrt{\sum_{t \neq 0} \left|\widehat{S_{w_1}}(t)\right|^2 \left|\widehat{S_{w_2}}(t)\right|^2}$$

Theorem 9 proves that $F_2 \ll n^{-1/2} \cdot \log n$, which, upon substitution, yields Theorem 1.

3.1 Estimating F_2

Upper-bounding F_2 turns out to be fairly challenging. From Cauchy–Schwarz, we get $F_2 \leqslant A^2$, where

$$A \coloneqq \sum_{w \in W} \left(\sum_{t \neq 0} \left|\widehat{S_w}(t)\right|^4 \right)^{1/4}. \tag{10}$$

Theorem 9 proves that $A \ll n^{-1/4} \cdot \sqrt{\log n}$, and (from that) $F_2 \ll n^{-1/2} \cdot \log n$.[2] We prove:

Lemma 1 (Technical: Energy estimate)**.** *For any S_w, we have*

$$\sum_{t \neq 0} \left|\widehat{S_w}(t)\right|^4 \ll n^{-3}.$$

This quantity is closely connected to the (additive) energy of S_w.

$$E^+(S_w) \coloneqq \#\left\{ (a,b,c,d) \in S_w^4 \,:\, a+b = c+d \pmod N \right\}. \tag{11}$$

[2]This estimate holds for every n, with no primality assumption, in the Mersenne setting $N = 2^n - 1$.

Using the connection between the energy of a set and its Fourier coefficients, our technical lemma yields:

$$\frac{E^+(S_w)}{N^3} - \mu(S_w)^4 = \sum_{t\neq 0} \left|\widehat{S_w}(t)\right|^4 \leqslant n^{-3}, \tag{12}$$

where $\mu(S) = \#S/N$ denotes the density of the set S in $\mathbb{Z}/N\mathbb{Z}$. This estimate is the main quantitative input in the proof of Theorem 9, and it also feeds into the structural result summarized in Theorem 11.

Energy estimation challenge. The main obstacle is the arithmetic of carries. Addition modulo $N = 2^n - 1$ induces long-range dependencies across bit positions: the carry propagates and wraps around, so the constraint $a + b = c + d \pmod N$ does not decompose into independent local conditions. Thus, counting solutions in Equation 12 requires controlling a global constraint generated by a local finite-state process.

Moreover, it is not sufficient to estimate $E^+(S_w)$ at the level of the main term $\mu(S_w)^4$. We must resolve the deviation $N^{-3}E^+(S_w) - \mu(S_w)^4$ to accuracy $\mathcal{O}\big(n^{-3}\big)$, which forces us to track lower-order correlation created by the carry process.

Our approach. We encode the carry process using a finite-state automaton and analyze it via generating functions; see Appendix C.

Step 1: Local transition model. We first construct the generating function for the addition of two bits with prescribed incoming and outgoing carry bits; see Figure 4a. This yields a local transfer operator.

Step 2: Coupling two additions. We then construct a joint generating function that enforces the condition that the sum of the first pair of bits equals the sum of the second pair; see Figure 4b. This generating function is represented as a 4×4 matrix $B(\mathbf{u})$, where the indeterminate $\mathbf{u} = (u_1, u_2, u_3, u_4)$ tracks the four bits.

Step 3: Global composition. Iterating the transition n times and dovetailing the carry bits yields a cyclic composition of the automaton. Here, the identity $N = 2^n - 1$ is essential: The final carry wraps around and becomes the initial carry. Consequently, for odd n, the energy becomes as the coefficient extraction problem

$$E[S_w] = [u_1^w u_2^w u_3^w u_4^w] \operatorname{tr} B(\mathbf{u})^n, \tag{13}$$

see Proposition 14 in Appendix C.[3]

Step 4: Coefficient extraction. We recover the coefficient in Equation 13 using the Cauchy integral formula on the product contour (in our case, a circle in each coordinate); see Appendix D. This analysis reduces to upper-bounding the $\operatorname{tr} B(\mathbf{u})^n$ uniformly along the contour.

Step 5: Spectral analysis. The key here is a dichotomy based on the spectrum of $B(\mathbf{u})$:

1. *Near the base point* $\mathbf{u} = \mathbf{1}$. The matrix $B(\mathbf{u})$ has a unique maximum eigenvalue 8, with a spectral gap to the remaining eigenvalues. By analytic perturbation, this persists in the neighborhood of $\mathbf{1}$. In this region, $\operatorname{tr} B(\mathbf{u})^n$ is dominated by the top eigenvalue, yielding the main term.

[3] For even n there is a slight mismatch between $E[S_w]$ and $[u_1^w u_2^w u_3^w u_4^w] \operatorname{tr} B(\mathbf{u})^n$ because 0 and $2^n - 1$ are identical in G.

2. *Away from the base point.* Outside this neighborhood, direct control via trace identities is insufficient. Instead, we prove that the spectral radius of $B(\mathbf{u})$ is uniformly bounded away from 8. This uses structural properties of $B(\mathbf{u})$ together with the Frobenius-Wielandt comparison theorem (see Theorem 10). Consequently, the contribution of this region is exponentially small.

Combining the local expansion near $\mathbf{1}$ with the global spectral decay away from it yields the required $\mathcal{O}(n^{-3})$ control on the energy deviation.

4 Upper Bound: N close to a Power of Two

In this section, we extend the upper bound to near-dyadic moduli N, beyond Mersenne primes. Our argument works uniformly for all $|N - 2^n| \leqslant 2^n/n$.

Theorem 2. *There is an absolute positive constant c such that $E_k(s) \leqslant (cn)^{-k/2+5/4}$ for any N satisfying $|N - 2^n| \leqslant 2^n/n$, $k \in \{3, 4, \dots\}$, and $s \in \{0, 1, \dots, N-1\}$.*

At a high level, we again follow the scaffolding-down strategy from the proof of Theorem 1. However, nearly every step now requires a substantial rework. The first obstruction is that, for general N, the arithmetic of carries modulo N is no longer described by a small automaton. Because of this, the method from Section 3 does not yield a satisfactory estimate for F_2. We therefore push the recursion one step further, down to F_1. This is exactly where the loss of $1/4$ in the exponent reappears.

Next, the central difficulty is to recover an analogue of the $F_m \leqslant n^{-1/2}F_{m-1}$ reduction of Lemma 9. In the Mersenne case, that estimate relied crucially on the fact that the doubling map $x \mapsto 2x \pmod N$ has orbits of length n, for prime n. For a general near-dyadic modulus N, this exact orbit structure disappears. The heart of our proof is therefore to build a robust substitute for this orbit-averaging argument that survives under perturbations of size N/n.

Analysis inspiration. Our arithmetic takes place on the N-grid, namely in $\mathbb{Z}/N\mathbb{Z}$. On the other hand, it is natural to work with Hamming slices on the full dyadic cube, which we identify with $\{0, 1, \dots, Q-1\}$, where $Q = 2^n$ (read, Q for "qübe"). The guiding idea is therefore to sample this cube along the N-grid; Equation 14 elaborates it. We first analyze the model version of our quantities on the cube, where the combinatorial structure is cleaner, and then transfer the resulting estimates back to the N-grid by a perturbative argument. Since N is close to Q, our transference introduces only mild slack, and the main term remains dominant.

Model quantities. Introduce the auxiliary function $B_w \colon \mathbb{Z}_N \to \mathbb{C}$, for $w \in W$, defined below:

$$B_w(x) \;:=\; \#\Big\{0 \leqslant y < Q \;:\; y = x \pmod N, \text{ and } \mathrm{wt}(y) = w\Big\}.$$

To see our accounting, note that each $y \in \{0, 1, \dots, Q-1\}$ contributes $+1$ to the counter $B_{\mathrm{wt}(y)}(y \mod N)$. Since $|N - Q| \leqslant Q/2$, we have $Q/N \leqslant 2$. Therefore, $B_w(\cdot)$ can receive at most 2 contributions (possibly from $y = x$ and $y = N + x$); hence, $B_w(x) \in \{0, 1, 2\}$. In particular, for a fixed $x \in \mathbb{Z}_N$,

1. If $N \geqslant Q$ (that is: $Q \leqslant N \leqslant 3Q/2$), then $B_w(x) = 1$ if $\mathrm{wt}(x) = w$; otherwise $B_w(x) = 0$.
2. If $N < Q$ (that is: $Q/2 \leqslant N < Q$), then only for $x \in \{0, \dots, Q - N - 1\}$, the counter $B_w(x)$ may get an additional contribution from $y = (x + N)$

Next, consider its Fourier transform:

$$\widehat{B_w}(t) \coloneqq \frac{1}{N} \sum_{0 \leqslant x < N} B_w(x) \cdot \mathrm{e}_N(xt) = \frac{1}{N} \sum_{0 \leqslant y < Q \colon \mathrm{wt}(y) = w} \mathrm{e}_N(yt). \tag{14}$$

This right-most expression is the "full cube" (sum over all $0 \leqslant x < Q$) sampled at the "N-grid" (evaluation of the function $\mathrm{e}_N(\cdot)$). Next, define the companion model quantities: For $0 \leqslant s < N$ and $k \in \{3, 4, \dots\}$:

$$E_k^{\square}(N, s) \coloneqq \sum_{\mathbf{w} \in W^k} \left| \sum_{t \neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \widehat{B_{\mathbf{w}_j}}(t). \right| \tag{15}$$

For $m \in \{2, 3, \dots\}$ define:

$$F_m^{\square}(N) \coloneqq \sum_{\mathbf{w} \in W^m} \left(\sum_{t \neq 0} \prod_{j=1}^{m} \left| \widehat{B_{\mathbf{w}_j}}(t) \right|^2 \right)^{1/2}. \tag{16}$$

Scaffolding in model cube. These model quantities support the previous scaffolding strategy, albeit incurring constant slacks.

Lemma 2. *For every $0 \leqslant s < N$, we have $E_k^{\square}(N, s) \leqslant 2 \cdot F_{k-1}^{\square}(N)$.*

Appendix G.1 proves this lemma, an analog of Lemma 7. The slack of 2 arises from the fact that $B_w(x) \leqslant 2$.

Lemma 3. *For every $m \in \{2, 3, \dots\}$ $F_m^{\square}(N) \leqslant (Q/N)^{1/2} \cdot \alpha^{\square}(N)^{1/2} \cdot F_{m-1}^{\square}(N)$, where*

$$\alpha^{\square}(N) \coloneqq \max_{t \neq 0} \sum_{w \in W} \frac{\left| \widehat{B_w}(t) \right|^2}{\rho_w(N)} \tag{17}$$

$$\rho_w(N) \coloneqq \frac{1}{N} \binom{n}{w}. \tag{18}$$

Appendix G.2 proves this lemma, the analog of Lemma 9. The slack $Q/N \asymp 1$, so it is innocuous. A key technical challenge is to upper-bound $\alpha^{\square}(N)$; here, there are no doubling orbits to help us.

Lemma 4 (Key technical lemma)**.** $\alpha^{\square}(N) \ll n^{-1}$.

Appendix G.4 proves this lemma. Previously, when $N = 2^n - 1$ and n is prime, it follows from a rigid structure: the doubling map $x \mapsto 2x$ partitions S_w into length-n orbits. For general N, this exact orbit structure is no longer available. We replace it with a *dynamical system viewpoint*. Specifically, we study the system on the torus $\mathbb{R}/\mathbb{Z}$ induced by the Bernoulli shift (see Figure 5 for an example)

$$\{t/N\} \longmapsto \{2t/N\},$$

where $\{\cdot\}$ denotes the fractional part. This map serves as a soft substitute for the discrete orbit structure: while exact periodicity is lost, the iterates are sufficiently equidistributed to recover the necessary averaging.

Together, Lemma 3 and Lemma 4 yield the correct desired asymptotics $F_m^{\square}(N) \ll n^{-1/2} \cdot F_{m-1}^{\square}(N)$, just like Lemma 9. Finally, at the foundation of our scaffolding, we have the analog of Lemma 12:

Lemma 5. $F_1^{\square}(N) \ll n^{1/4}$.

This lemma is proven in Appendix G.3. From these results, upper-bounding $E_k^{\square}(N,s)$ is straightforward:

$$\begin{aligned} E_k^{\square}(N,s) &\ll F_{k-1}^{\square}(N) && \text{(by Lemma 2)} \\ &\ll n^{-1/2}\cdot F_{k-2}^{\square}(N) && \text{(by Lemma 3 and Lemma 4, and because } Q/N \leqslant 2) \\ &\ll_k n^{-(k-2)/2}\cdot F_1^{\square}(N) \\ &\ll n^{-(k-2)/2}\cdot n^{1/4}. && \text{(by Lemma 5)} \end{aligned}$$

So, we have the upper bound in the model cube.

Theorem 3. *For $k \in \{3,4,\dots\}$ and $s \in \{0,1,\dots,N-1\}$, we have: $E_k^{\square}(N,s) \ll_k n^{-k/2+5/4}$.*

Transference theorem. Here, the takeaway will be that the transference theorem acts like a highly economical union bound. The only loss comes from the perturbation created when one transfers between the cube model and the N-grid, and that loss is governed by $|N-2^n|$. A direct union bound would only tolerate $|N-2^n| \leqslant 2^n \cdot n^{-k/2}$ to retain the final $n^{-k/2}$-type bound. The transference theorem avoids this waste and extends the admissible regime to $|N-2^n| \leqslant 2^n \cdot n^{-1}$. Appendix F proves the following:

Theorem 4. *Let N satisfy $|N-2^n| \leqslant P$. Consider any $k \in \{3,4,\dots\}$ and $0 \leqslant s < N$, the following upper bound holds: $E_k(s) \leqslant E_k^{\square}(N,s) + \sum_{\ell=1}^{k-1}\binom{k}{\ell}(P/N)^{\ell/2}F_{k-\ell}^{\square}(N) + (P/N)^{k/2}\sqrt{n}$.*

We can use Lemma 3, Lemma 4, and Lemma 5 to upper bound $F_{k-\ell}^{\square}(N) \ll_k n^{-(k-\ell-1)/2}\cdot n^{1/4}$. When the perturbation is small, namely $P/N \leqslant 2n^{-1}$, using Theorem 3, we have the following specialization:

$$E_k(s) \ll_k E_k^{\square}(N,s) + \sum_{\ell=1}^{k-1}\binom{k}{\ell}\cancel{n^{-\ell/2}}\cdot n^{-(k-\cancel{\ell}-1)/2+1/4} + n^{-k/2+1/2} \ll_k n^{-k/2+5/4}.$$

This derivation proves Theorem 2.

4.1 Another Upper Bound: Statement and Proof of Theorem 5

Next, we state and prove Theorem 5, a specialization of our upper bound to moduli $N = 2^n - 1$, where n is an arbitrary positive integer (not necessarily a prime).

Theorem 5. *$E_k(s) \leqslant (cn)^{-k/2+1}\log n$ for any odd $n \geqslant 3$, $N = 2^n-1$, $k \geqslant 3$, and $s \in \{0,1,\dots,N-1\}$.*

Note that G and the cube $\{0,1,\dots,2^n-1\}$ differ only in one element that has weight n, and it occurs with probability $1/N$, which is exponentially small. So, we will transition from one to the other using naïve union bound and pay with a $1/N$ slack per share. Below, additive k/N terms account for the union bound.

$$\begin{aligned} E_k(s) &\leqslant E_k^{\square}(N,s) + k/N && \text{(union bound)} \\ &\leqslant 2\cdot F_{k-1}^{\square}(N) + k/N && \text{(by Lemma 2)} \\ &\leqslant 2\cdot (cn)^{-1/2}\cdot F_{k-2}^{\square}(N) + k/N && \text{(by Lemma 3 and Lemma 4, and because } Q/N \leqslant 2) \\ &\leqslant 2\cdot (cn)^{-(k-3)/2}\cdot F_2^{\square}(N) + k/N && \text{(stopping at } F_2^{\square}(N), \text{ instead of } F_1^{\square}(N)) \\ &\leqslant 2\cdot (cn)^{-(k-3)/2}\cdot F_2(N) + 2k/N && \text{(union bound)} \\ &\leqslant 2\cdot (cn)^{-(k-3)/2}\cdot n^{-1/2}\log n + 2k/N. && \text{(by Theorem 9)} \end{aligned}$$

5 Lower Bound: $N = 2^n - 1$, even k

Lower-bounding insecurity is threat assessment of side-channel attacks. This section will serve as a warm-up for our lower-bounding strategies, which are the first of their kind in this field.

Theorem 6. *$E_k(0) \geqslant (1/10)^k \cdot n^{-k/2+1}$ for any odd n, $N = 2^n - 1$, and $k \in \{4, 6, \dots\}$.*

We use a dual phase-selection argument: rewrite $E_k(0)$ as a supremum over phase choices, and then restrict attention to product phases that are coherently aligned with the canonical dyadic Fourier modes. Using this alignment and the doubling-orbit structure, the problem reduces to estimating a single frequency $\sum_{w \in W} \left|\widehat{S_w}(-1)\right|$, which is the ℓ_1-mass of an associated product; see Equation 19. In cryptographic interpretation, these canonical dyadic modes correspond to explicit distinguishers that break the scheme.

Proof of Theorem 6. Recall $E_k(0) = \sum_{\mathbf{w} \in W^k} \left|\sum_{t \neq 0} \prod_{j=1}^k \widehat{S_{\mathbf{w}_j}}(t)\right|$. Consider arbitrary phases $\mathbf{\Phi} = \left(\mathbf{\Phi}_{\mathbf{w}} : \mathbf{w} \in W^k\right)$. Then, by duality, we have the identity

$$E_k(0) = \max_{\mathbf{\Phi}} \left| \sum_{\mathbf{w} \in W^k} \mathbf{\Phi}_{\mathbf{w}} \sum_{t \neq 0} \prod_{j=1}^k \widehat{S_{\mathbf{w}_j}}(t) \right|.$$

Restrict to product phases $\mathbf{\Phi}_{\mathbf{w}} = \prod_{j=1}^k \phi_w$, where the appropriate phases ϕ_w are defined below:

$$\phi_w = \begin{cases} \overline{\widehat{S_w}(-1)} / \left|\widehat{S_w}(-1)\right|, & \text{if } \widehat{S_w}(-1) \neq 0 \\ 1, & \text{otherwise.} \end{cases}$$

Restricted to such phases, we have:

$$E_k(0) \geqslant \max_{(\phi_w \colon w \in W)} \left| \sum_{\mathbf{w} \in W^k} \sum_{t \neq 0} \prod_{j=1}^k \phi_{\mathbf{w}_j} \cdot \widehat{S_{\mathbf{w}_j}}(t) \right| = \max_{(\phi_w \colon w \in W)} \left| \sum_{t \neq 0} \left(\sum_{w \in W} \phi_w \cdot \widehat{S_w}(t) \right)^k \right|.$$

Recall, $\widehat{S_{n-w}}(t) = \overline{\widehat{S_w}(t)}$ (because $x \in S_w$ implies $-x \in S_{n-w}$). So, $\phi_w \widehat{S_w}(t) + \phi_{n-w} \widehat{S_{n-w}}(t) \in \mathbb{R}$. Furthermore, since k is even, $\left(\sum_{w \in W} \phi_w \widehat{S_w}(t)\right)^k \geqslant 0$. As a result, we conclude that

$$\begin{aligned}
E_k(0) &\geqslant \max_{(\phi_w \colon w \in W)} \sum_{t \neq 0} \left(\sum_{w \in W} \phi_w \widehat{S_w}(t) \right)^k \\
&\geqslant n \cdot \max_{(\phi_w \colon w \in W)} \left(\sum_{w \in W} \phi_w \widehat{S_w}(-1) \right)^k \quad \text{(because } \widehat{S_w}(2^j t) = \widehat{S_w}(t), \text{ for all } j \in \{0, 1, \dots, n-1\}) \\
&= n \cdot \left(\sum_{w \in W} \left|\widehat{S_w}(-1)\right| \right)^k \\
&\geqslant 10^{-k} \cdot n^{-k/2+1}. \qquad \text{(by the technical Lemma 6 mentioned below)}
\end{aligned}$$

Lemma 6 (Technical: Lower bound)**.** $\sum_{w \in W} \left|\widehat{S_w}(-1)\right| \geqslant (1/10) \cdot n^{-1/2}$.

Appendix H proves this result. For $w \neq n$, we begin with the observation:

$$\widehat{S_w}(t) = \frac{1}{N} \sum_{x \in S_w} \mathrm{e}_N(-xt) = \frac{1}{N} \cdot [z^w] \prod_{j=0}^{n-1} \left(1 + z \cdot \mathrm{e}_N(-2^j t)\right) \tag{19}$$

So, the technical lemma is equivalent to a lower bound on the sum of the absolute values of the coefficients of this product when $t = -1$. This lower bound matches the upper bound from Theorem 1. A subtlety is that $\widehat{S_w}(-2^j)$ are not the only dominant Fourier modes; other frequencies can contribute comparably. For example, any frequency t whose binary representation contains a short block of consecutive ones may carry significant spectral mass. Figure 2 illustrates this phenomenon by comparing the $t = 3$ and $t = 1$ cases.

6 Lower Bound: $|N - 2^n| \leqslant 2^{(1-\varepsilon)n}$

Now, we will prove a general lower bound for any N that is close to a power of 2.

Theorem 7. *For any N satisfying $|N - 2^n| \leqslant 2^m$, where $m < n$ and $n \geqslant 4$, the following bound holds.*

$$\max_{0 \leqslant s < N} E_k(s) \geqslant \sqrt{\frac{1}{N} \sum_{0 \leqslant s < N} E_k(s)^2} \geqslant L^{1/2} \cdot (1/25)^k \cdot n^{-k/2},$$

where $L = \left(n - m - \frac{1}{2}\log_2 n - \mathcal{O}(1)\right)$. In particular, when $m = (1-\varepsilon)n$, then (for sufficiently large n, as a function of ε) $\max_{0 \leqslant s < N} E_k(s) \geqslant \varepsilon^{1/2} \cdot (1/25)^k \cdot n^{-k/2+1/2}$.

Appendix I proves this result. Theorem 7 does *not* claim that $E_k(0)$ is large; it proves the existence by demonstrating that the (L^2-)average of $E_k(s)$ is large. Theorem 8 provides evidence that some non-zero secret may witness the maximum insecurity.

Like the proof of Theorem 6, restrict to a specific type of product phases $\mathbf{\Phi_w} := \prod_{j=1}^{k} \phi^{\mathbf{w}_j}$ – this choice is different from that in Theorem 6. For this restriction, the lower bound turns out to be

$$\sqrt{\sum_{t \neq 0} \underbrace{\left| \sum_{w \in W} \phi^w \cdot \widehat{S_w}(t) \right|^{2k}}_{T(t)}}$$

We will identify a subset H of candidate frequencies $H \subseteq \left\{-2^j : 0 \leqslant j < n\right\}$ such that $\#H = \varepsilon \cdot n$ and $T(t) \gg n^{-1/2}$, for every $t \in H$. To this end, because N is very close to 2^n, we argue that instead of the spectral properties of S_w, it suffices to investigate the "idealized set" of all weight-w elements of $\{0, 1, \ldots, 2^n - 1\}$. The analog of $T(t)$ for these idealized sets admits a closed-form expression:

$$\prod_{j=0}^{k-1} \left(1 + \phi \cdot \mathrm{e}_N\left(2^j t\right)\right).$$

We make a careful choice $\phi = \exp(-\imath/\sqrt{n})$ and prove that these idealized quantities are $\gg n^{-1/2}$. Finally, we present an attack on the $k = 2$ case.

Theorem 8. *Consider $|2^n - N| \leqslant \varepsilon \cdot N$ and $s = 2^n - 1 \pmod N$. Then, $E_2(s) \geqslant 1 - 2\varepsilon - \mathcal{O}\left(n^{-1/2}\right)$.*

Proof. Consider shares s_1, s_2 of the secret $s = 2^n - 1 \pmod N$. Let $w_1 = \mathrm{wt}(s_1)$ and $w_2 = \mathrm{wt}(s_2)$. All but an ε fraction of the shares satisfy $w_1 + w_2 = n$. Hence,

$$E_2(s) \geqslant \sum_{\substack{(w_1,w_2)\in W^2 \\ w_1+w_2=n}} D(s)(w_1,w_2) - D(U)(w_1,w_2) \geqslant \frac{N-\varepsilon N}{N} - \frac{1}{N^2}\binom{2n}{n} = 1 - \varepsilon - \mathcal{O}\Big(n^{-1/2}\Big). \quad \square$$

7 Open Problems

Our framework, based on generating functions, complex analysis, and matrix analysis, demonstrates significant potential for addressing general leakage problems and more sophisticated secret-sharing schemes. At the same time, even within additive sharing, several fundamental questions remain open; a few immediate ones are elaborated below.

General modulus. Extend the analysis beyond near-dyadic N. A candidate entry point is using the MSB-fixing decomposition of $\mathbb{Z}/N\mathbb{Z}$ into cube-like subsets [MNP+21]. For example, consider $N = 20$; the set $\mathbb{Z}_N = \{0, 1, \ldots, 19\}$ partitions into two cubes $\{0, \ldots, 15\} \dot\cup \{16, \ldots, 19\}$, all elements in the first cube have MSB 0 and all elements in the second cube have MSB 100. Restricted to each cube, the Hamming weight neatly splits into the sum of the Hamming weights of the prefix and the suffix (referred to as the q-additive property). This reduces the insecurity analysis to these structural components, yielding a recursive, smaller Hamming-weight leakage on the cube. Developing Fourier-analytic control for cubes in this non-uniform setting will be the natural path ahead.

F_2 estimation. Remove the logarithm loss in $F_2 \ll n^{-1/2} \cdot \log n$. This appears to be entirely an artifact of our contour-based argument. A refined saddle-point analysis, capturing Gaussian concentration near the saddle point, should yield the sharper $n^{-1/2}$ upper bound.

Analyze $N = 2^n$ and $N = 2^n + 1$ within the generating function framework. These cases are sufficiently structured that our analytical pathways developed for $N = 2^n - 1$ could accommodate them. The starting point will be to extend the generating function to account for the final carry in these cases. Overall, these may serve as a bridge to general N.

Tighter lower bounds. Eliminate the $1/2$ loss in the exponent of Theorem 7. The current L^2 averaging is too coarse. A weighted construction via Riesz products, concentrating spectral mass on controlled frequencies, may recover the optimal exponent or yield a tighter overall lower bound. Extending control beyond dyadic modes is a key obstacle.

Vulnerable witness. Identify the secret $s \in G$ maximizing $E_k(s)$, Experiments have been inconclusive here. Some suggest that $s = 0$ is the global witness, but Theorem 8 indicates a possible non-zero maximizer.

Exact insecurity for small k. Determine $E_3(s)$, starting with, say, $E_3(0)$. Tightness of insecurity estimation is particularly essential in the small-k regime, where the slack has a more pronounced impact. Empirically, $n \cdot E_3(0)$ appears affine in $1/n$, suggesting

$$E_3(0) \sim a \cdot n^{-1} + b \cdot n^{-2}.$$

Figure 3 illustrates this phenomenon. This matches the lower bound n^{-1} proved in Theorem 7 and highlights the slack in the upper bound of Theorem 1. Either $s = 0$ isn't the witness (unlikely, according to us), or our odd-k upper bound is off in Theorem 1.

Appendix

A A Unified Preliminaries and Notations

Basics. We work over the group $G \coloneqq \mathbb{Z}/N\mathbb{Z}$; also represented by $\mathbb{Z}_N$ for brevity. Let $W = \{0, 1, \ldots, n\}$, where n is the closest power of 2 to N. The weight of an element $x \in G$, denoted by $\mathrm{wt}(x)$, is the number of ones in its binary representation. Note that $\mathrm{wt}(G) \subseteq W$. For $w \in W$, let $S_w \subseteq G$ denote the set of all weight-w elements of G.

Boldface variables are vectors, for example $\mathbf{w} \in W^k$, and $\mathbf{w}_j$ represents the j-th element of this vector.

Fourier analysis. A phase is a uni-modular complex number, and $\overline{z}$ denotes the complex conjugate of z. We proceed by Fourier analysis over G. We define $\mathrm{e}_N(x) \coloneqq \exp(2\pi\imath \cdot x/N)$. Sets are equivalent to their characteristic functions. For $0 \leqslant t < N$, the corresponding (normalized) Fourier coefficient of $S \subseteq G$ is:

$$\widehat{S}(t) \coloneqq \frac{1}{N} \sum_{x \in S} \mathrm{e}_N(-xt).$$

The energy of a set $S \subseteq G$, denoted by $E(S)$, is the number of solutions to the equation $a + b = c + d$, where $(a, b, c, d) \in S^4$. It connects to (normalized) Fourier coefficients through the equation:

$$E(S) = N^3 \cdot \sum_t \left|\widehat{S_w}(t)\right|^4.$$

Cryptography. The *additive secret sharing* of a secret $s \in G$ into k shares chooses random $(s_1, s_2, \ldots, s_k) \in G^k$ satisfying $\sum_{j=1}^k s_i = s$. The adversary receives the leakage $(\mathrm{wt}(s_1), \ldots, \mathrm{wt}(s_k))$; let $D(s)$ denote this conditional distribution over W^k. For brevity, $D(U)$ denotes the leakage distribution when the secret is chosen uniformly at random $\in G$. The *insecurity* of a specific secret s is the total variational distance:

$$E_k(s) \coloneqq \left\| D(s) - D(U) \right\|_{\mathrm{TV}}.$$

By [BDIR18, BDIR21], it is known that

$$E_k(s) = \sum_{\mathbf{w} \in W^k} \left| \sum_{t \neq 0} \mathrm{e}_N(-st) \prod_{j=1}^k \widehat{S_{\mathbf{w}_j}}(t) \right|.$$

To prove security, one has to demonstrate an upper bound on all $E_k(s)$, for every $s \in G$. Identifying an attack needs a lower bound on $E_k(s)$ for some $s \in G$.

Asymptotic notations. We use standard Vinogradov notation $\gg$, $\asymp$, $\ll$, and asymptotic notations $\mathcal{O}(\cdot)$ and $\mathrm{o}(\cdot)$.

B Proofs for Analytical Proxies

B.1 Reduction to F_{k-1}

Lemma 7 (E_k to F_{k-1} reduction)**.** *For any integer N, $k \in \{2, 3, \ldots\}$, and $s \in \{0, 1, \ldots, N-1\}$, we have:*

$$E_k(s) \leqslant F_{k-1}.$$

Proof of Lemma 7. Recall that

$$E_k(s) = \sum_{\mathbf{w}\in W^k} \left| \sum_{t\neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \widehat{S_{w_j}}(t) \right| = \sum_{\mathbf{w}\in W^{k-1}} \sum_{w\in W} \left| \sum_{t\neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k-1} \widehat{S_{w_j}}(t) \cdot \widehat{S_w}(t) \right|.$$

To prove $E_k(s) \leqslant F_{m-1}$, it will suffice to prove the following statement for any $\mathbf{w}' \in W^{k-1}$:

$$\sum_{w\in W} \left| \sum_{t\neq 0} \underbrace{\mathrm{e}_N(st) \prod_{j=1}^{k-1} \widehat{S_{w'_j}}(t)}_{c_t \coloneqq} \cdot \widehat{S_w}(t) \right| \leqslant \sqrt{\sum_{t\neq 0} \prod_{j=1}^{k-1} \left|\widehat{S_{w_j}}(t)\right|^2}.$$

This, in turn, will follow immediately from the technical Claim 8 below, instantiated with $f_w = S_w$. Since $(S_w)_{w\in W}$ partitions $\mathbb{Z}/N\mathbb{Z}$, we have $\left\| \sum_{w\in W} |f_w| \right\|_{L^\infty} = 1$.

Claim 8. *For $w \in W$, consider functions $f_w \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$. For any complex numbers $(z_t \colon 0 < t < N)$, we have*

$$\sum_{w\in W} \left| \sum_{t\neq 0} z_t \cdot \widehat{f_w}(t) \right| \leqslant \left\| \sum_{w\in W} |f_w| \right\|_{L^2} \cdot \sqrt{\sum_{t\neq 0} |z_t|^2} \leqslant \left\| \sum_{w\in W} |f_w| \right\|_{L^\infty} \cdot \sqrt{\sum_{t\neq 0} |z_t|^2}.$$

Proof of Claim 8. Consider the dual characterization. We remind the reader that phases are unimodular complex numbers. Over phases $\mathbf{\Phi} = (\mathbf{\Phi}_w \colon w \in W)$ we have the following guarantee:

$$\begin{aligned}
\sum_{w\in W} \left| \sum_{t\neq 0} z_t \cdot \widehat{f_w}(t) \right| &= \sup_{\mathbf{\Phi}} \left| \sum_{w\in W} \mathbf{\Phi}_w \sum_{t\neq 0} z_t \cdot \widehat{f_w}(t) \right| \\
&= \sup_{\mathbf{\Phi}} \left| \sum_{t\neq 0} z_t \cdot \left(\sum_{w\in W} \mathbf{\Phi}_w \widehat{f_w}(t) \right) \right| \\
&= \sup_{\mathbf{\Phi}} \left| \sum_{t\neq 0} z_t \cdot \widehat{f_{\mathbf{\Phi}}}(t) \right| && (\text{define } f_{\mathbf{\Phi}} \coloneqq \sum_{w\in W} \mathbf{\Phi}_w \cdot f_w) \\
&\leqslant \sup_{\mathbf{\Phi}} \sqrt{\sum_{t\neq 0} |z_t|^2} \cdot \|f_{\mathbf{\Phi}}\|_{L^2}. && (\text{by Cauchy-Schwarz and Parseval's})
\end{aligned}$$

By the triangle inequality, the first inequality of the lemma follows. The second inequality follows from the monotonicity of norms. □

B.2 Reduction from F_m to F_{m-1}

Lemma 9 (F_m to F_{m-1} reduction)**.** *For prime n, $N = 2^n - 1$, and $m \in \{2, 3, \dots\}$, we have:*

$$F_m \leqslant n^{-1/2} \cdot F_{m-1}.$$

Proof of Lemma 9. We begin with two technical claims.

Claim 10. *For any $t \neq 0$, $\sum_{w\in W} \left|\widehat{S_w}(t)\right|^2 / \rho_w \leqslant n^{-1}$, where $\rho_w = |S_w|/N$.*

Proof. Consider the function $f_t\colon G \to \mathbb{C}$ defined by $f_t = \sum_{w\in W} z_{w,t}\cdot S_w$, where $z_{w,t} \coloneqq \overline{\widehat{S_w}(t)}/\rho_w$. Note that $\widehat{f_t} = \sum_{w\in W} z_{w,t}\cdot \widehat{S_w}$. In particular, $\widehat{f_t}(t) = \sum_{w\in W}\left|\widehat{S_w}(t)\right|^2/\rho_w \in \mathbb{R}_{\geqslant 0}$.

By rotation symmetry and n being prime, we have $\#\{t, 2t, \dots, 2^{n-1}t\} = n$ and $\widehat{f_t}(t) = \widehat{f_t}(2t) = \dots = \widehat{f_t}(2^{n-1}t)$. By Parseval's, we get

$$n\widehat{f_t}(t)^2 = \sum_{0\leqslant j<n}\widehat{f_t}(2^j t)^2 \leqslant \sum_u\left|\widehat{f_t}(u)\right|^2 = \frac{1}{N}\sum_x |f_t(x)|^2 = \frac{1}{N}\sum_{w\in W}\rho_w N\cdot|z_{w,t}|^2 = \sum_{w\in W}\left|\widehat{S_w}(t)\right|^2/\rho_w = \widehat{f_t}(t).$$

From the extreme LHS and RHS expressions, we conclude that $\widehat{f_t}(t) \leqslant n^{-1}$. □

Claim 11. *Consider arbitrary*

1. *non-negative real numbers a_t, for $0 < t < N$,*
2. *non-negative real numbers $b_{w,t}$, for $0 < t < N$ and $w \in W$,*
3. *positive real numbers μ_w, for $w \in W$, and*
4. *$\alpha \geqslant \sum_{w\in W} b_{w,t}/\mu_w$ for all $0 < t < N$*

Then, the following bound holds:

$$\sum_{w\in W}\sqrt{\sum_{t\neq 0} a_t\cdot b_{w,t}} \leqslant \alpha^{1/2}\cdot\sqrt{\sum_{w\in W}\mu_w}\cdot\sqrt{\sum_{t\neq 0} a_t}.$$

Proof.

$$\begin{aligned}
\sum_{w\in W}\sqrt{\sum_{t\neq 0} a_t\cdot b_{w,t}} &= \sum_{w\in W}\sqrt{\mu_w}\cdot\sqrt{\sum_{0<t<N} a_t\cdot b_{w,t}/\mu_w} \\
&\leqslant \sqrt{\sum_{w\in W}\mu_w}\cdot\sqrt{\sum_{0<t<N} a_t\sum_{w\in W} b_{w,t}/\mu_w} && \text{(by Cauchy-Schwarz)} \\
&\leqslant \left(\max_{0<t<N}\sum_{w\in W} b_{w,t}/\mu_w\right)^{1/2}\cdot\sqrt{\sum_{w\in W}\mu_w}\cdot\sqrt{\sum_{t\neq 0} a_t}.
\end{aligned}$$

whence the claim follows. □

Now, we use these two technical claims.

$$\begin{aligned}
F_m &= \sum_{\mathbf{w}\in W^m}\sqrt{\sum_{t\neq 0}\prod_{j=1}^{m}\left|\widehat{S_{w_j}}(t)\right|^2} \\
&= \sum_{\mathbf{w}\in W^{m-1}}\sum_{w\in W}\sqrt{\sum_{t\neq 0}\underbrace{\prod_{j=1}^{m-1}\left|\widehat{S_{w_j}}(t)\right|^2}_{a_t\,\coloneqq}\cdot\underbrace{\left|\widehat{S_w}(t)\right|^2}_{b_{w,t}}} \\
&\leqslant \sum_{\mathbf{w}\in W^{m-1}} n^{-1/2}\cdot\sqrt{1}\cdot\sqrt{\sum_{t\neq 0}\prod_{j=1}^{m-1}\left|\widehat{S_{w_j}}(t)\right|^2} = n^{-1/2}\cdot F_{m-1}. \\
&\qquad\qquad \text{(by Claim 11 and } \mu_w = \#S_w/N \text{ and } \alpha = n^{-1} \text{ from Claim 10)}
\end{aligned}$$

This completes the proof of Lemma 9.

B.3 Estimating F_1

Lemma 12 (Estimating F_1)**.** *For any integer $n \in \{2, 3, \dots\}$ and $N = 2^n - 1$ or $N = 2^n$, we have*

$$F_1 \ll n^{1/4}.$$

Proof of Lemma 12.

$$\begin{aligned}
F_1 &= \sum_{w \in W} \sqrt{\sum_{t \neq 0} \left|\widehat{S_w}(t)\right|^2} \\
&\asymp \sum_{w \in W} \sqrt{\binom{n}{w} \cdot 2^{-n}} && \text{(Parseval's identity and accommodating some edge terms)} \\
&\ll \frac{1}{n^{1/4}} \sum_{w \in W} \exp\left(-\frac{(w - n/2)^2}{n+1}\right) && \text{(see [BHMY25, Corollary 4])} \\
&\ll n^{1/4}.
\end{aligned}$$

C Generating Function for Carry Automata

Refer to Figure 4a for the presentation below. For $a, b, c, c', o \in \{0, 1\}$ and indeterminate u_1, u_2, let us construct the generating function for the finite automata for carry addition. Suppose the incoming carry is c. Suppose a and b are two bits at the current position. The resulting output is o, with outgoing carry c'. Therefore, these bits satisfy the following equation over $\mathbb{Z}$:

$$a + b + c = o + 2c'.$$

Towards constructing the generating function, we construct a 2×2 matrix $M^{(o)}$ as follows:

$$M^{(o)}(u_1, u_2)[c, c'] \coloneqq \sum_{a,b:\ a+b+c=o+2c'} u_1^a u_2^b.$$

So, for example, we have:

$$M^{(0)}(u_1, u_2) = \begin{pmatrix} 1 & u_1 u_2 \\ 0 & u_1 + u_2 \end{pmatrix}, \qquad \text{and} \qquad M^{(1)}(u_1, u_2) = \begin{pmatrix} u_1 + u_2 & 0 \\ 1 & u_1 u_2 \end{pmatrix}.$$

Next, our objective is to construct the generating function of the following "collision-in-addition" automata (see Figure 4b): Suppose we have two incoming carry bits $c, d \in \{0, 1\}$. Suppose there are two pairs of bits $(a, b), (g, h) \in \{0, 1\}^2$. The addition of a, b, c produces output o and outgoing carry bit c'. The addition of g, h, d produces the *same* output o and outgoing carry bit d'. We want to construct a 4×4 generating function matrix B in indeterminate $\mathbf{u} = (u_1, u_3, u_3, u_4)$ with the following semantics:

$$B(\mathbf{u})[cd, c'd'] \coloneqq \sum_{\substack{a,b,g,h,o \in \{0,1\} \\ a+b+c=o+2c' \\ g+h+d=o+2d'}} u_1^a u_2^b u_3^g u_4^h.$$

Here $cd \in \{00, 01, 10, 11\}$ and $c'd' \in \{00, 01, 10, 11\}$.

Proposition 13.

$$B = M^{(0)}(u_1, u_2) \otimes M^{(0)}(u_3, u_4) + M^{(1)}(u_1, u_2) \otimes M^{(1)}(u_3, u_4).$$

Specifically,

$$B(\mathbf{u}) = \begin{pmatrix} 1 & u_3u_4 & u_1u_2 & u_1u_2 \cdot u_3u_4 \\ 0 & u_3+u_4 & 0 & u_1u_2 \cdot (u_3+u_4) \\ 0 & 0 & (u_1+u_2) & (u_1+u_2) \cdot u_3u_4 \\ 0 & 0 & 0 & (u_1+u_2) \cdot (u_3+u_4) \end{pmatrix} + \begin{pmatrix} (u_1+u_2) \cdot (u_3+u_4) & 0 & 0 & 0 \\ (u_1+u_2) & (u_1+u_2) \cdot u_3u_4 & 0 & 0 \\ (u_3+u_4) & 0 & u_1u_2 \cdot (u_3+u_4) & 0 \\ 1 & u_3u_4 & u_1u_2 & u_1u_2 \cdot u_3u_4 \end{pmatrix}.$$

Note that $B(\mathbf{u})^n$ denotes the generating function of the additions of n-bit strings with the semantics that $B(\mathbf{u})^n[cd, c'd'] = \sum_{\mathbf{w} \in W^4} \nu(\mathbf{w}) \cdot u_1^{\mathbf{w}_1} u_2^{\mathbf{w}_2} u_3^{\mathbf{w}_3} u_4^{\mathbf{w}_4}$, where $\nu(\mathbf{w})$ denotes the *number* of n-bit strings $\mathbf{a}, \mathbf{b}, \mathbf{g}, \mathbf{h} \in \{0,1\}^n$ such that

1. Their respective Hamming weights are $\mathbf{w}_1$, $\mathbf{w}_2$, $\mathbf{w}_3$, and $\mathbf{w}_4$.
2. Starting with carry bit c, the addition of $\mathbf{a}$ and $\mathbf{b}$ produces some output $\mathbf{o} \in \{0,1\}^n$ and outgoing carry bit c'.
3. Starting with carry bit d, the addition of $\mathbf{g}$ and $\mathbf{h}$ produces the *same* output $\mathbf{o}$ and outgoing carry bit d'.

Fix arbitrary weights $\mathbf{w} \in W^4$. For brevity, $\mathbf{u}^{\mathbf{w}}$ will denote $u_1^{\mathbf{w}_1} u_2^{\mathbf{w}_2} u_3^{\mathbf{w}_3} u_4^{\mathbf{w}_4}$. Our objective is to count the cardinality of the following set:

$$\left\{ (\mathbf{a}, \mathbf{b}, \mathbf{g}, \mathbf{h}) \in S_{\mathbf{w}_1} \times S_{\mathbf{w}_2} \times S_{\mathbf{w}_3} \times S_{\mathbf{w}_3} \,:\, \mathbf{a} + \mathbf{b} = \mathbf{g} + \mathbf{h} \pmod{N} \right\}.$$

Since $N = 2^n - 1$, note that here the starting and outgoing carries must be identical, i.e., $cd = c'd'$. So, we are interested in the quantity

$$[\mathbf{u}^{\mathbf{w}}] \operatorname{tr} B(\mathbf{u})^n.$$

However, $[\mathbf{u}^{\mathbf{w}}] \operatorname{tr} B(\mathbf{u})^n$ *may not be identical to the cardinality of the set above*; there is a subtle disconnect.

Note that in $\mathbb{Z}/(2^n-1)\mathbb{Z}$ there are two representations of 0, one is $\underbrace{00\cdots0}_{n\text{-times}}$ and another is $\underbrace{11\cdots1}_{n\text{-times}}$. However, if $\underbrace{11\cdots1}_{n\text{-times}} \notin (S_{\mathbf{w}_1} + S_{\mathbf{w}_2}) \cap (S_{\mathbf{w}_3} + S_{\mathbf{w}_4})$, then this disconnect is entirely circumvented.

Keeping our downstream applications in mind, consider the special case $\mathbf{w} = (w, w, w, w)$ for some $w \in W$. Let $\mathbf{u}^w$ represent $\mathbf{u}^{(w,w,w,w)}$. Note that $S_w + S_w$ cannot contain $2^n - 1$ when n is odd. In this context, we have

Proposition 14. $[\mathbf{u}^w] \operatorname{tr} B(\mathbf{u})^n$ *is identical to the* energy *of the set S_w, denoted by $E(S_w)$, when n is odd.*

The plan ahead. Our objective is to prove that

$$[\mathbf{u}^w] \operatorname{tr} B(\mathbf{u})^n = \frac{1}{N} \cdot \binom{n}{w}^4 \pm \mathcal{O}\big(N^3 \cdot n^{-3}\big).$$

To that end, note that

$$[\mathbf{u}^w]\Big(\underbrace{\frac{1}{2}\cdot(1+\mathbf{u}_1)(1+\mathbf{u}_2)(1+\mathbf{u}_3)(1+\mathbf{u}_4)}_{=:\,\Lambda_0(\mathbf{u})}\Big)^n = \frac{1}{2^n}\cdot\binom{n}{w}^4. \tag{20}$$

Interpret $\Lambda_0(\mathbf{u})$ as the "ideal baseline polynomial" and our aim is to prove that the "actual polynomial" $B(\mathbf{u})$ only deviates slightly from it. In other words, for any $w \in W$, our target objective is to prove:

$$\Big|\ [\mathbf{u}^w]\ (\mathrm{tr}\ \ B(\mathbf{u})^n - \Lambda_0(\mathbf{u})^n)\ \Big| \ll N^3\cdot n^{-3}.$$

We will proceed using Cauchy's coefficient estimation technique by integrating along the torus $\mathbf{u} = (\exp(\imath\theta_1),\ldots,\exp(\imath\theta_4))$, where $\boldsymbol{\theta} = (\theta_1,\ldots,\theta_4) \in [-\pi,\pi]^4$. Of specific interest would be the behavior of our polynomial in a small disc around $\boldsymbol{\theta} = \mathbf{0}$. Keeping this end objective in mind, for brevity, we introduce a slight abuse of notation: $\mathrm{tr}\ B(\boldsymbol{\theta})^n - \Lambda_0(\boldsymbol{\theta})^n$ will denote the polynomial with $\mathbf{u}_i = \exp(\imath\boldsymbol{\theta}_i)$ substitution, for every $i \in \{1,2,3,4\}$.

D Tighter F_2 Upper Bound

Theorem 9. *Let $N = 2^n - 1$ for an odd n.*

$$A \coloneqq \sum_{w\in W}\left(\sum_{t\neq 0}\left|\widehat{S_w}(t)\right|^4\right)^{1/4} \ll n^{-1/4}\cdot\sqrt{\log n}.$$

In particular, as a consequence, $F_2 \ll n^{-1/2}\cdot\log n$.

Proof. From the upper bound on A, the bound $F_2 \leqslant A^2 \ll n^{-1/2}\cdot\log n$ is straightforward by the Cauchy-Schwarz inequality.

For the first bound, we will use the following technical lemma:

Lemma 15 (Technical lemma)**.** *For any $w \in W$*

$$\sum_{t\neq 0}\left|\widehat{S_w}(t)\right|^4 \ll n^{-3}.$$

Appendix D.1 proves Lemma 15. From this technical lemma, the proof of the theorem follows directly. Consider the contribution to A by the central weights $W_{\mathrm{cent}} \coloneqq \left\{w \in W\colon |n/2 - w| \leqslant \sqrt{n\log n}\right\}$.

$$Q_1 = \sum_{w\in W_{\mathrm{cent}}}\left(\sum_{t\neq 0}\left|\widehat{S_w}(t)\right|^4\right)^{1/4} \leqslant \#W_{\mathrm{cent}}\cdot n^{-3/4} \ll n^{-1/4}\cdot\sqrt{\log n}.$$

The contribution from the remaining weights is

$$\begin{aligned}
Q_2 &= \sum_{w\in W\setminus W_{\text{cent}}} \left(\sum_{t\neq 0}\left|\widehat{S_w}(t)\right|^4\right)^{1/4} \\
&= \sum_{w\in W\setminus W_{\text{cent}}} \ell_4\left(\widehat{S_w}\right) \\
&\leqslant \sum_{w\in W\setminus W_{\text{cent}}} \ell_2\left(\widehat{S_w}\right) && (\ell_k(\cdot) \text{ norm decreases with increasing } k) \\
&< \sum_{w\in W\setminus W_{\text{cent}}} \sqrt{\rho_w} && (\text{by Parseval's, where } \rho_w = \tbinom{n}{w}\cdot N^{-1} \text{ is the density of } S_w) \\
&\overset{(*)}{\ll} n^{-1/4}\cdot\frac{1}{n}\cdot\sqrt{n/\log n} = \mathrm{o}\left(n^{-3/4}\right).
\end{aligned}$$

The $(*)$ inequality follows from the following derivation:

$$\text{Fact 1:}\qquad N^{-1}\binom{n}{n/2+i} \ll n^{-1/2}\exp\left(-2\frac{i^2}{n+1}\right).$$

$$\text{Fact 2:}\qquad \sum_{x\geqslant u}\exp(-x^2/m) \leqslant \exp(-iu^2/m)\left(1+\frac{m}{2u}\right).$$

$$\text{(because } \sum_{x\geqslant u}\exp(-x^2/m) \leqslant \exp(-u^2/m) + \tfrac{\sqrt{\pi m}}{2}\cdot\operatorname{erfc}(u/\sqrt{m})\text{)}$$

$$\text{(and } \operatorname{erfc}(x) \leqslant \exp(-x^2)/x\sqrt{\pi}\text{)}$$

$$\text{So,}\qquad 2^{-n/2}\sum_{i\geqslant u}\binom{n}{n/2+i}^{1/2} \ll n^{-1/4}\cdot\exp\left(-\frac{u^2}{n+1}\right)\cdot\frac{n}{u}.$$

After this, $A = Q_1 + Q_2 \ll n^{-1/4}\cdot\sqrt{\log n}$ upper bound is immediate. □

D.1 Proof of Lemma 15

In this section, we will prove:

$$\left|E_w - \binom{n}{w}^4\cdot N^{-1}\right| \ll N^3\cdot n^{-3}, \tag{21}$$

which is equivalent to Lemma 15's upper bound

$$\sum_{t\neq 0}\left|\widehat{S_w}(t)\right|^4 \ll n^{-3}.$$

One innocuous modification moving forward: Instead of proving $\left|E_w - \binom{n}{w}^4\cdot N^{-1}\right| \ll N^3\cdot n^{-3}$, it would suffice to prove that $\left|E_w - \binom{n}{w}^4\cdot 2^{-n}\right| \ll N^3\cdot n^{-3}$ because $N = 2^n - 1$. Let us proceed with this estimation now.

We have set up a generating function

$$G(\mathbf{u}) = \operatorname{tr} B(\mathbf{u})^n - \Lambda_0(\mathbf{u})^n,$$

where $\mathbf{u} = (u_1, u_2, u_3, u_4)$, the matrix B is defined by Equation 23 and Λ_0 is defined by Equation 20.

Claim 16.

$$E_w - \binom{n}{w}^4 \cdot 2^{-n} \;=\; [u_1^w u_2^w u_3^w u_4^w] G(\mathbf{u}).$$

This claim was proven in Appendix C as Proposition 14 for odd n. By the Cauchy integral formula (or, in this specific case, the orthogonality relation), we have:

$$E_w - \binom{n}{w}^4 \cdot 2^{-n} = \frac{1}{(2\pi)^4} \int_{[-\pi,\pi]^4} G(\boldsymbol{\theta}) \exp\left(-\imath w(\boldsymbol{\theta}_1 + \cdots + \boldsymbol{\theta}_4)\right) \mathrm{d}\boldsymbol{\theta},$$

where $\boldsymbol{\theta} = (\theta_1, \theta_2, \theta_3, \theta_4)$ and $G(\boldsymbol{\theta}) = G\left(\exp(\imath\theta_1), \ldots, \exp(\imath\theta_4)\right)$. By the triangle inequality, we have

$$\left| E_w - \binom{n}{w}^4 \cdot 2^{-n} \right| \ll \int_{[-\pi,\pi]^4} |G(\boldsymbol{\theta})| \mathrm{d}\boldsymbol{\theta}.$$

We split the contour into two different parts and estimate this integral separately. Let us partition the set $[-\pi, \pi]^4$ into two sets.

$$\boldsymbol{\Theta}_{\text{close}} = \left\{ \boldsymbol{\theta} \in [-\pi,\pi]^4 \,:\, |\theta_1|, |\theta_2|, |\theta_3|, |\theta_4| \leqslant \tau \right\} \quad \text{and} \quad \boldsymbol{\Theta}_{\text{far}} = [-\pi,\pi]^4 \setminus \boldsymbol{\Theta}_{\text{close}}$$

for some parameter τ.

Claim 17.

$$\int_{\boldsymbol{\Theta}_{\text{close}}} |G(\boldsymbol{\theta})| \mathrm{d}\boldsymbol{\theta} \ll N^3 \cdot n^{-3}.$$

Claim 18. *For some positive constant $c = c(\tau)$*

$$\int_{\boldsymbol{\Theta}_{\text{far}}} |G(\boldsymbol{\theta})| \mathrm{d}\boldsymbol{\theta} \ll N^3 \cdot \exp(-cn).$$

Below, Appendix D.2 proves Claim 17 and Appendix D.3 proves Claim 18. From these two claims, we immediately conclude Equation 21.

D.2 Proof of Claim 17

We will show that there is a function $\Lambda(\boldsymbol{\theta})$ such that

$$|G(\boldsymbol{\theta})| \leqslant |\Lambda(\boldsymbol{\theta})^n - \Lambda_0(\boldsymbol{\theta})^n| + \mathcal{O}(5^n) \leqslant n \cdot |\Lambda(\boldsymbol{\theta}) - \Lambda_0(\boldsymbol{\theta})| \cdot \left(|\Lambda(\boldsymbol{\theta})|^{n-1} + |\Lambda_0(\boldsymbol{\theta})|^{n-1} \right) + \mathcal{O}(5^n).$$

Then, we will claim (proven in Appendix D.4):

Claim 19.

$$\begin{aligned} |\Lambda(\boldsymbol{\theta}) - \Lambda_0(\boldsymbol{\theta})| &\ll \|\boldsymbol{\theta}\|_2^4 && (\text{for } \boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{close}}) \\ |\Lambda_0(\boldsymbol{\theta})| &\leqslant 8 \exp\left(-\|\boldsymbol{\theta}\|_2^2/\pi^2\right) \\ |\Lambda(\boldsymbol{\theta})| &\leqslant 8 \exp\left(-c\|\boldsymbol{\theta}\|_2^2\right). && (\text{for } \boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{close}}) \end{aligned}$$

From this claim, we get

$$\int_{\boldsymbol{\Theta}_{\text{close}}} |G(\boldsymbol{\theta})| \mathrm{d}\boldsymbol{\theta} \ll N^3 \int_{\boldsymbol{\Theta}_{\text{close}}} n \cdot \|\boldsymbol{\theta}\|_2^4 \cdot \exp(-cn\|\boldsymbol{\theta}\|_2^2) \mathrm{d}\boldsymbol{\theta} \asymp N^3 \cdot n \cdot n^{-4} = N^3 \cdot n^{-3}.$$

D.3 Proof of Claim 18

This claim will be immediate from $|\text{tr } B(\boldsymbol{\theta})^n| \ll N^3 \cdot \exp(-cn)$ and $|\Lambda_0(\boldsymbol{\theta})|^n \ll N^3 \cdot \exp(-cn)$. These are argued below.

Smallness of Λ_0. Suppose $|\theta_1| \geqslant \tau$. Then,

$$|1 + \exp(\imath\theta_1)| \leqslant 2\cos(\theta_1/2) \leqslant 2\cos(\tau/2) \leqslant 2 \cdot \exp(-\tau^2/8).$$

From this, it is immediate that

$$|\Lambda_0(\boldsymbol{\theta})|^n \leqslant N^3 \cdot \exp\left(-(\tau^2/8) \cdot n\right).$$

This argument works for any $\boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{far}}$.

Smallness of tr $B(\boldsymbol{\theta})^n$. We will prove the following claim in Appendix D.5:

Claim 20. *For $\boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{far}}$, there is a positive constant $c = c(\tau)$ such that the spectral radius is upper-bounded:*

$$\rho(B(\boldsymbol{\theta})) \leqslant 8 \cdot \exp(-c).$$

After this claim, we know that

$$\text{tr } B(\boldsymbol{\theta})^n = \mu_1^n + \mu_2^n + \mu_3^n + \mu_4^n,$$

where, for all eigenvalues, one has $|\mu_1|, |\mu_2|, |\mu_3|, |\mu_4| \leqslant 8\exp(-c)$. So, we conclude $|\text{tr } B(\boldsymbol{\theta})^n| \ll N^3 \cdot \exp(-cn)$.

D.4 Proof of Claim 19

Part 1. From Equation 22, we have

$$|\Lambda(\boldsymbol{\theta}) - \Lambda_0(\boldsymbol{\theta})| \ll \left|\prod_{j=1}^{4}(1 - \exp(\imath\boldsymbol{\theta}_j))\right| \leqslant 16\prod_{j=1}^{4}\sin(\boldsymbol{\theta}_j/2) \leqslant \prod_{j=1}^{4}\boldsymbol{\theta}_j \ll \|\boldsymbol{\theta}\|_2^4.$$

Part 2. Note that $|1 + \exp(\imath\theta)| = 2\cos(\theta/2) \leqslant 2\exp(-\theta^2/\pi^2)$, because $\cos t \leqslant \exp(-4t^2/\pi^2)$. So, we have

$$|\Lambda_0(\boldsymbol{\theta})| \leqslant 8 \cdot \exp(-\|\boldsymbol{\theta}\|_2^2/\pi^2).$$

Part 3. From Parts 1 and 2, we know that

$$|\Lambda(\boldsymbol{\theta})| \leqslant |\Lambda_0(\boldsymbol{\theta})| + |\Lambda(\boldsymbol{\theta}) - \Lambda_0(\boldsymbol{\theta})| \leqslant 8 \cdot \exp(-\|\boldsymbol{\theta}\|_2^2/\pi^2) + \mathcal{O}\Big(\|\boldsymbol{\theta}\|_2^4\Big).$$

Given the threshold τ, $\|\boldsymbol{\theta}\|_2^4$ is radially-symmetric and bounded. So, we can upper-bound the RHS by $\leqslant 8\cdot\exp(-c\|\boldsymbol{\theta}\|_2^2)$, a sufficiently weaker Gaussian with parameter c that depends on the threshold τ.

D.5 Spectral Properties

In this section, we will prove spectral properties of the matrix $B(\boldsymbol{\theta})$.

1. When $\boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{close}}$, its largest eigenvalue behaves as:

$$|\Lambda(\boldsymbol{\theta}) - \Lambda_0(\boldsymbol{\theta})| \ll \left| \prod_{j=1}^{4} \left(1 - \exp(\imath \boldsymbol{\theta}_j)\right) \right|. \tag{22}$$

2. Its spectral radius is separated from 8 when $\boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{far}}$ (that is Claim 20).

In the sequel, we use $\mathbf{u} = (u_1, \ldots, u_4)$ defined by $u_j \coloneqq \exp(\imath \boldsymbol{\theta}_j)$, for $j \in \{1, 2, 3, 4\}$. Recall from Appendix C, we have:

$$B(\mathbf{u}) = \begin{pmatrix} (u_1+u_2)\cdot(u_3+u_4)+1 & u_3u_4 & u_1u_2 & u_1u_2 \cdot u_3u_4 \\ (u_1+u_2) & (u_1+u_2)\cdot u_3u_4 + (u_3+u_4) & 0 & u_1u_2 \cdot (u_3+u_4) \\ (u_3+u_4) & 0 & u_1u_2 \cdot (u_3+u_4) + (u_1+u_2) & (u_1+u_2)\cdot u_3u_4 \\ 1 & u_3u_4 & u_1u_2 & u_1u_2 \cdot u_3u_4 + (u_1+u_2)\cdot(u_3+u_4) \end{pmatrix}. \tag{23}$$

Our objective is to investigate the dominant eigenvalue $\Lambda(\mathbf{u})$ of this matrix.

Consider a sufficiently small neighborhood parameterized by $\tau > 0$:

$$\mathcal{N} \coloneqq \left\{ \mathbf{u} : \ |1 - \mathbf{u}_j| \leqslant \tau, \text{ for every } j \in \{1, 2, 3, 4\} \right\}.$$

Note that $B(\mathbf{1})$ has eigenvalues $8, 4, 4, 2$. There is an analytic function $\Lambda(\mathbf{u})$ such that its magnitude is > 7 and is the largest eigenvalue of $B(\mathbf{u})$, for any $\mathbf{u} \in N$. All other eigenvalues of $B(\mathbf{u})$ are < 5 in magnitude.

Consider the auxiliary polynomial $P(\mathbf{u}; z) \coloneqq \det(\text{diag}\,(z, z, z, z) - B(\mathbf{u}))$, the roots represent the eigenvalues corresponding to $\mathbf{u}$. Note that $P(\mathbf{u}; z)$ is a function such that the partial derivative with respect to z at $(\mathbf{1}, 8)$ is not equal to 0. Therefore, by the implicit function theorem, there exists an analytic function $\Lambda(\mathbf{u})$ such that

$$P(\mathbf{u}; \Lambda(\mathbf{u})) = 0, \text{ and } \Lambda(\mathbf{1}) = 8$$

in a small neighborhood of $\mathbf{1}$.

Let us choose two contours:

$$\Gamma_{\text{high}} \coloneqq \{z : |z - 8| = 1\}, \text{ and } \Gamma_{\text{rest}} \coloneqq \{z : |z| = 5\}.$$

Now, on both these contours, $|P(\mathbf{1}; z)| = \left|(z-8)(z-4)^2(z-2)\right| > 0$. Therefore, for $\mathbf{u}$ very close to $\mathbf{1}$, since $P(\mathbf{u}; z)$ changes continuously with $\boldsymbol{u}$, we can make

$$|P(\mathbf{u}; z) - P(\mathbf{1}; z)| < |P(\mathbf{1}; z)|$$

on each contour. Then, by Rouché's theorem, inside both the contours, $P(\mathbf{u}; z)$ and $P(\mathbf{1}; z)$ have the same number of roots, counted with multiplicity. Therefore, together with the continuity of spectral radius and the fact that $\Lambda(\mathbf{1}) = 8$, we can assume, without loss of generality, by contracting the neighborhood of $\mathbf{u}$ around $\mathbf{1}$ appropriately (if necessary) that

1. We have an analytic function $\Lambda(\mathbf{u})$ denoting the largest eigenvalue of $B(\mathbf{u})$ which remains in the proper interior of Γ_{high}.

2. All remaining eigenvalues of $B(\mathbf{u})$ are in the proper interior of Γ_{rest}.

Therefore, we get that $\operatorname{tr} B(\mathbf{u})^n = \Lambda(\mathbf{u})^n + \mathcal{O}(5^n)$.

Recall that $\Lambda_0(\mathbf{u}) = \frac{1}{2}\prod_{j=1}^4 (1+\mathbf{u}_j)$. Define $\mathbf{u}'$ as $\mathbf{u}$ restricted to $\mathbf{u}_1 = 1$. Note that we have the identity:

$$B(\mathbf{u}') \cdot \mathbf{1} = \Lambda_0(\mathbf{u}') \cdot \mathbf{1}.$$

So, $\Lambda_0(\mathbf{u}')$ is a eigenvalue of $B(\mathbf{u}')$. At $\mathbf{u}' = \mathbf{1}$, we have $\Lambda_0(\mathbf{1}) = 8$, which coincides with $\Lambda(\mathbf{1})$. In the neighborhood $\mathcal{N}$, because $\Lambda(\mathbf{u})$ is the only eigenvalue, it must be the case that $\Lambda(\mathbf{u}') = \Lambda_0(\mathbf{u}')$.

From this, we conclude that $(1-\mathbf{u}_1)$ divides $\Lambda(\mathbf{u}) - \Lambda_0(\mathbf{u})$. Likewise, by symmetry $\prod_{j=1}^4 (1-\mathbf{u}_j)$ divides $\Lambda(\mathbf{u}) - \Lambda_0(\mathbf{u})$. So, we conclude that

$$\Lambda(\mathbf{u}) - \Lambda_0(\mathbf{u}) = \left(\prod_{j=1}^4 (1-\mathbf{u}_j)\right) \cdot H(\mathbf{u}),$$

for some analytic function $H(\mathbf{u})$. The maximum magnitude of $H(\mathbf{u})$ is bounded in the neighborhood $\mathcal{N}$, whence we get Equation 22.

Next, we will prove the spectral gap when $\mathbf{u} \in \mathbf{\Theta}_{\text{far}}$. For this, we will need the following result.

Theorem 10 (Frobenius-Wielandt comparison theorem, [BP94, Theorem 2.14, p. 31])**.** *Let A be an irreducible non-negative matrix, and let B be a complex matrix satisfying $|B_{i,j}| \leqslant A_{i,j}$, entrywise. Then*

$$\rho(B) \leqslant \rho(A).$$

More generally, every eigenvalue γ of B satisfies $|\gamma| \leqslant \rho(A)$. If equality holds for some eigenvalues γ of B, that is, if $|\gamma| = \rho(A)$, then there exists a diagonal unitary matrix D and a real number ϕ such that

$$B = \exp(\imath\phi) DAD^{-1}, \text{ and } \exp(\imath\phi) = \gamma/\rho(A).$$

In particular, if $\rho(B) = \rho(A)$, then $B = \exp(\imath\phi)DAD^{-1}$ for some real ϕ and diagonal unitary D.

We emphasize that this result proves that $\rho(B(\mathbf{u}))$ is far from 8 for *any* $\mathbf{u}$ far away from $\mathbf{1}$.

Let $A \coloneqq B(\mathbf{1})$. Note that A is non-negative and irreducible (because A^2 has all non-zero entries). So, $\rho(B(\mathbf{u})) \leqslant \rho(A) = 8$. If the inequality becomes strict in a sufficiently small neighborhood around $\mathbf{1}$, then the proof of Claim 20 is complete.

So, it suffices to prove that it is impossible to achieve equality for $\mathbf{u} \neq \mathbf{1}$. If possible, let the equality hold in the theorem at $\mathbf{u} \neq 1$. Then, $B(\mathbf{u}) = \exp(\imath\phi)DAD^{-1}$, for some real ϕ and $D = \operatorname{diag}(d_1, d_2, d_3, d_4)$. In particular, $|B(\mathbf{u})_{i,j}| = A_{i,j}$.

Comparing $(2,1)$ elements of A and $B(\mathbf{u})$, we conclude that $\mathbf{u}_1 = \mathbf{u}_2$. Likewise, comparing $(3,1)$ elements, we conclude that $\mathbf{u}_3 = \mathbf{u}_4$. Next, comparing $(1,1)$ elements, we conclude that $\mathbf{u}_1 = \mathbf{u}_2 = \overline{\mathbf{u}_3} = \overline{\mathbf{u}_4}$. From this, we conclude that $B(\mathbf{u})_{1,4} = 1$.

After that, observe that

$$1 = B(\mathbf{u})_{1,4} = \exp(\imath\phi) d_1 \overline{d_4} A_{1,4} = \exp(\imath\phi) d_1 \overline{d_4}$$
$$1 = B(\mathbf{u})_{4,1} = \exp(\imath\phi) d_4 \overline{d_1} A_{4,1} = \exp(\imath\phi) d_4 \overline{d_1}.$$

These two constraints imply that $\exp(\imath\phi) \in \{\pm 1\}$; i.e., $\exp(\imath 2\phi) = 1$.

Now, compare $(1,2)$ and $(2,1)$ elements of A and $B(\mathbf{u})$. We have $B(\mathbf{u})_{1,2} = \overline{\mathbf{u}_1}^2$ and $B(\mathbf{u})_{2,1} = 2\mathbf{u}_1$. We also have $B(\mathbf{u})_{1,2} = \exp(\imath\phi) d_1 \overline{d_2} A_{1,2}$ and $B(\mathbf{u})_{2,1} = \exp(\imath\phi) d_2 \overline{d_1} A_{2,1}$. Multiplying them, we get: $\overline{\mathbf{u}_1} = \exp(\imath 2\phi)$, which we know is 1.

This proves that $\mathbf{u}_1 = 1 = \mathbf{u}_2 = \overline{\mathbf{u}_3} = \overline{\mathbf{u}_4}$; i.e., $\mathbf{u} = \mathbf{1}$, a contradiction.

Next, for a positive constant τ, we need to upgrade this strict inequality into a spectral separation. For simplicity, let us revert to the $\boldsymbol{\theta}$ notation. Consider the set

$$S_\tau \;\coloneqq\; \left\{\boldsymbol{\theta} \in [-\pi,\pi]^4 \;:\; \|\boldsymbol{\theta}\|_\infty \geqslant \tau\right\}.$$

Note that because $[-\pi,\pi]^4$ is compact, the set S_τ is also compact and does not contain $\mathbf{0}$. Since the spectral radius is a continuous function, the spectral radius of $B(\boldsymbol{\theta})$ on S_τ is strictly smaller than 8. This continuous function attains a maximum at some point in the compact set S_τ. Denote this maximum spectral radius in S_τ by $8 \cdot \exp(-c)$, for some positive constant c. This completes the proof that $\rho(B(\mathbf{u})) \leqslant 8 \cdot \exp(-c)$ for $\boldsymbol{\theta} \in \boldsymbol{\Theta}_{\text{far}}$

E Structural Results

This section proves the following theorem:

Theorem 11. diam $\text{Cay}(G, S_w) \leqslant 3$, *where* $G = \mathbb{Z}/N\mathbb{Z}$, $N = 2^n - 1$, *odd* n, *and* $\#S_w/N \gg n^{-3/5}$.

The proof is immediate from Lemma 1 and Claim 21 (stated and proved below); Lemma 1 proves $c = 3$ in Claim 21 for our case.

Claim 21. *Consider a group* G *of order* N *and* $c > 0$. *If* $S \subseteq G$ *satisfies*

$$\#S > a^{1/5} \cdot Nn^{-c/5} \qquad \textit{and} \qquad E(S) \leqslant \frac{(\#S)^4}{N} + a \cdot N^3 n^{-c},$$

then $S + S + S = G$.

Proof. Suppose not, then there is $x \in G$ such that $x \notin S + S + S$. That is, $T \coloneqq x - S$ and $S + S$ are disjoint. Let $r_S(x)$ denote the number of pairs (u, v) such that $u + v = x$ and $u, v \in S$. From elementary definitions, we have that $\sum_{x\in G} r_S(x)^2 = E(S)$ and

$$\sum_{x\in G}\left(\frac{(\#S)^2}{N} - r_S(x)\right)^2 = N^3 \sum_{t\neq 0}\left|\widehat{S}(t)\right|^4 \leqslant aN^3n^{-c}.$$

On the other hand, we know that $r_S(y) = 0$, for $y \in T$. So, we get

$$\frac{\#T(\#S)^4}{N^2} \leqslant \sum_{y\in T}\left(\frac{(\#S)^2}{N} - r_S(y)\right)^2 \leqslant \sum_{x\in G}\left(\frac{(\#S)^2}{N} - r_S(x)\right)^2 \leqslant aN^3n^{-c}.$$

Comparing the extreme LHS and RHS, we have

$$\#S \leqslant a^{1/5} Nn^{-c/5},$$

a contradiction. Therefore, $S + S + S = G$. □

F Transference: Proof of Theorem 4

Our aim is to express S_w, the actual Hamming slice restricted to $\{0, \ldots, N-1\}$, as a mild perturbation of B_w, a function that samples the N-grid at the Hamming slice restricted to the model cube $\{0, \ldots, Q-1\}$.

1. First, suppose $N > Q$. Consider the set $P_w := \{Q \leqslant y < N : \mathrm{wt}(y) = w\}$. $B_w = S_w \cap \{0, 1, \ldots, Q-1\}$. Therefore, $S_w = B_w + P_w$.
2. Next, suppose $N \leqslant Q$. Consider the set $P_w := \{N \leqslant y < Q : \mathrm{wt}(y) = w\}$. $y \in P_w$ gets accounted at $x = y - N$. Therefore, $S_w = B_w - P_w$.

As a result, in general, we have $S_w = B_w + \sigma \cdot P_w$. And, the sets $(P_w : w \in W)$ are pairwise disjoint and their cumulative density is

$$\sum_{w \in W} \frac{\#P_w}{N} \leqslant \frac{P}{N}.$$

Now, for $\mathbf{w} \in W^k$, let us compute the product of the Fourier coefficient that appears in our target quantity $E_k(N, s)$. Recall that

$$E_k(N, s) = \sum_{\mathbf{w} \in W^k} \left| \sum_{t \neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \widehat{S_{\mathbf{w}_j}}(t) \right|$$

The terms in the summand can be expanded as:

$$\begin{aligned} \prod_{j=1}^{k} \widehat{S_{\mathbf{w}_j}}(t) &= \prod_{j=1}^{k} \left(\widehat{B_{\mathbf{w}_j}}(t) + \sigma \cdot \widehat{P_{\mathbf{w}_j}}(t) \right) \\ &= \sum_{J \subseteq \{1,2,\ldots,k\}} \sigma^{\#J} \left(\prod_{j \notin J} \widehat{B_{\mathbf{w}_j}}(t) \right) \left(\prod_{j \in J} \widehat{P_{\mathbf{w}_j}}(t) \right) \end{aligned}$$

For $J \subseteq \{1, 2, \ldots, k\}$, define the restriction:

$$E_k(N, s)|_J := \sum_{\mathbf{w} \in W^k} \left| \sum_{t \neq 0} \mathrm{e}_N(st) \cdot \left(\prod_{j \notin J} \widehat{B_{\mathbf{w}_j}}(t) \right) \cdot \left(\prod_{j \in J} \widehat{P_{\mathbf{w}_j}}(t) \right) \right|$$

By the triangle inequality, we have $E_k(N, s) \leqslant \sum_J E_k(N, s)|_J$. So, it will suffice to upper bound the individual $E_k(N, s)|_J$ contributions from the restrictions.

Case $J = \emptyset$. Note that $E_k(N, s)|_J = E_k^{\square}(N, s)$

Case $J = \{1, 2, \ldots, k\}$. In this case, we have

$$E_k(N, s)|_J = \sum_{\mathbf{w} \in W^k} \left| \sum_{t \neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \widehat{P_{\mathbf{w}_j}}(t) \right|$$

We will use the L^2 version of the Claim 8's upper bound. Fix $\mathbf{w} \in W^{k-1}$ (the first $(k-1)$ indices) and we will perform summation over the last index $\mathbf{w}_k \in W$ with the following setup:

1. $f_w = P_w$
2. $z_t = \mathrm{e}_N(st) \cdot \prod_{1 \leqslant j < k} \widehat{P_{\mathbf{w}_j}}(t)$

After this use, we will have:

$$\begin{aligned} E_k(N,s)|_J &\leqslant \sum_{\mathbf{w}\in W^{k-1}} \left\| \sum_{\mathbf{w}_k\in W} P_{\mathbf{w}_k} \right\|_{L^2} \cdot \sqrt{\sum_{t\neq 0} \prod_{1\leqslant j<k} \left|\widehat{P_{\mathbf{w}_j}}(t)\right|^2} \\ &\leqslant \sqrt{P/N} \sum_{\mathbf{w}\in W^{k-1}} \sqrt{\sum_{t\neq 0} \prod_{1\leqslant j<k} \left|\widehat{P_{\mathbf{w}_j}}(t)\right|^2} \\ &\qquad \text{(because } P_w \text{ are pairwise disjoint and } \textstyle\sum_{w\in W} P_w \text{ has density } \leqslant P/N\text{)} \end{aligned}$$

Roughly speaking its the density-sensitive version of Lemma 7.

Next, we plan to use Claim 11. Fix $\mathbf{w} \in W^{k-2}$, the first $(k-2)$ indices, and we will perform summation over the last index $\mathbf{w}_{k-1} \in W$ with the following setup:

1. $a_t = \prod_{1\leqslant j<k-1} \left|\widehat{P_{\mathbf{w}_j}}(t)\right|^2$
2. $b_{w,t} = \left|\widehat{P_w}(t)\right|^2$
3. $\mu_w = \#P_w/N$, i.e., P_w's density
4. $\alpha = 1$

After using Claim 11, because $\sum_{w\in W} \mu_w \leqslant P/N$, we have the inequality:

$$E_k(N,s)|_J \leqslant (P/N)^{1/2} \cdot (P/N)^{1/2} \sum_{\mathbf{w}\in W^{k-2}} \sqrt{\sum_{t\neq 0} \prod_{1\leqslant j<k-1} \left|\widehat{P_{\mathbf{w}_j}}(t)\right|^2}$$

Repeatedly applying this step eliminates one index from the end. We stop when we have one index left over.

$$\begin{aligned} E_k(N,s)|_J &\leqslant (P/N)^{(k-1)/2} \sum_{w\in W} \sqrt{\sum_{t\neq 0} \left|\widehat{P_w}(t)\right|^2} \\ &\leqslant (P/N)^{(k-1)/2} \cdot \sqrt{n} \cdot \sqrt{P/N}. && \text{(by Parseval and Cauchy-Schwarz)} \\ &= (P/N)^{k/2} \cdot \sqrt{n}. \end{aligned}$$

Case $\emptyset \neq J \subsetneq \{1,2,\ldots,k\}$. This case covers all remaining cases. In this case, we have

$$E_k(N,s)|_J \coloneqq \sum_{\mathbf{w}\in W^k} \left| \sum_{t\neq 0} \mathrm{e}_N(st) \cdot \left(\prod_{j\notin J} \widehat{B_{\mathbf{w}_j}}(t) \right) \cdot \left(\prod_{j\in J} \widehat{P_{\mathbf{w}_j}}(t) \right) \right|.$$

Next, we use the upper-bounding strategy we used above for $J = \{1,2,\ldots,k\}$. Denote $\overline{J} \coloneqq \{1,2,\ldots,k\} \setminus J$. We will get the inequality:

$$E_k(N,s)|_J \leqslant (P/N)^{\#J/2} \sum_{\mathbf{w}_{\overline{J}}\in W^{k-\#J}} \sqrt{\sum_{t\neq 0} \left(\prod_{j\in \overline{J}} \left|\widehat{B_{\mathbf{w}_j}}(t)\right|^2 \right)} = (P/N)^{\#J/2} \cdot F^{\square}_{k-\#J}(N).$$

After this, Theorem 4 is immediate:

$$E_k(N,s) \leqslant \sum_{J\subseteq\{1,2,\dots,k\}} E_k(N,s)|_J \leqslant E_k(N,s)|_\emptyset + E_k(N,s)|_{\{1,2,\dots,k\}} + \sum_{\emptyset\neq J\subsetneq\{1,2,\dots,k\}} E_k(N,s)|_J$$
$$\leqslant E_k^\square(N,s) + (P/N)^{k/2}\sqrt{n} + \sum_{0<\ell<k}\binom{k}{\ell}(P/N)^{\ell/2}F_{k-\ell}^\square(N).$$

This completes the proof of Theorem 4.

G Cube Model

G.1 Proof of Lemma 2

We will use Claim 8 with $f_w = B_w$. In that claim, we will use the fact that $\left\| \sum_{w\in W} |B_w| \right\|_{L^\infty} \leqslant 2$. Lemma 2 is immediate at this point:

$$\begin{aligned}
E_k^\square(N,s) &= \sum_{\mathbf{w}\in W^k}\left|\sum_{t\neq 0}\mathrm{e}_N(st)\prod_{j=1}^k \widehat{B_{\mathbf{w}_j}}(t)\right| \\
&= \sum_{\mathbf{w}'\in W^{k-1}}\sum_{\mathbf{w}_k\in W}\left|\sum_{t\neq 0}\underbrace{\mathrm{e}_N(st)\prod_{j=1}^{k-1}\widehat{B_{\mathbf{w}'_j}}(t)}_{z_t\,:=}\cdot\widehat{B_{\mathbf{w}_k}}(t)\right| && \text{(rearranging)} \\
&\leqslant \sum_{\mathbf{w}'\in W^{k-1}} 2\cdot\left(\sum_{t\neq 0}\prod_{j=1}^{k-1}\left|\widehat{B_{\mathbf{w}'_j}}(t)\right|^2\right)^{1/2} && \text{(by Claim 8)} \\
&= 2\cdot F_{k-1}^\square(N).
\end{aligned}$$

G.2 Proof of Lemma 3

$$\begin{aligned}
F_m^\square(N) &= \sum_{\mathbf{w}'\in W^{m-1}}\sum_{\mathbf{w}_m\in W}\left(\underbrace{\sum_{t\neq 0}\prod_{j=1}^{m-1}\left|\widehat{B_{\mathbf{w}'_j}}(t)\right|^2}_{a_t}\cdot\underbrace{\left|\widehat{B_{\mathbf{w}_m}}(t)\right|^2}_{b_{\mathbf{w}_m,t}}\right)^{1/2} \\
&\leqslant \sum_{\mathbf{w}'\in W^{m-1}}\alpha^\square(N)^{1/2}\cdot(Q/N)^{1/2}\cdot\left(\sum_{t\neq 0}\prod_{j=1}^{m-1}\left|\widehat{B_{\mathbf{w}'_j}}(t)\right|^2\right)^{1/2} \\
&\quad \text{(By Claim 11, with } \mu_w = \rho_w(N),\ \alpha = \alpha^\square(N), \text{ and } \textstyle\sum_{w\in W}\rho_w(N) = Q/N) \\
&= (Q/N)^{1/2}\cdot\alpha^\square(N)^{1/2}\cdot F_{m-1}^\square(N).
\end{aligned}$$

G.3 Proof of Lemma 5

$$\begin{aligned}
F_1^{\square}(N) &= \sum_{w\in W}\left(\sum_{t\neq 0}\left|\widehat{B_w}(t)\right|^2\right)^{1/2} \\
&< \sum_{w\in W}\left(\frac{1}{N}\sum_{0\leqslant x<N} B_w(x)^2\right)^{1/2} && \text{(by Parseval's identity)} \\
&\leqslant \sum_{w\in W}\left(\frac{2}{N}\cdot\binom{n}{w}\right)^{1/2} && \text{(because } \sum_{0\leqslant x<N} B_w(x) = \tbinom{n}{w} \text{ and } B_w(x)\leqslant 2\text{)} \\
&\ll \frac{1}{N^{1/2}}\cdot Q^{1/2}n^{1/4} \asymp n^{1/4}. && \text{(see [BHMY25, Corollary 4] and because } Q/N\leqslant 2\text{)}
\end{aligned}$$

G.4 Proof of Lemma 4

Recall that our target is to prove that

$$\alpha^{\square}(N) = \max_{t\neq 0}\sum_{w\in W}\frac{\left|\widehat{B_w}(t)\right|^2}{\rho_w(N)} \ll \frac{1}{n}.$$

First, we will reduce the target to proving this result when the summation is restricted to $w\in W_{\text{cent}}$ defined below

$$W_{\text{cent}} \coloneqq \left\{\, w\in W \,:\, |w-n/2|\leqslant\sqrt{2n\log n}\,\right\}.$$

To that end, consider any $w\notin W_{\text{cent}}$. For such a w, we have

$$\left|\widehat{B_w}(t)\right| \leqslant N^{-1}\cdot\binom{n}{w} \ll \frac{1}{\sqrt{n}}\cdot\frac{1}{n^2}.$$

Moreover,

$$\frac{\left|\widehat{B_w}(t)\right|}{\rho_w(N)} \leqslant \frac{\left|\widehat{B_w}(t)\right|}{N^{-1}\binom{n}{w}} \leqslant 1.$$

From this observation, we conclude that

$$\sum_{w\notin W_{\text{cent}}}\frac{\left|\widehat{B_w}(t)\right|^2}{\rho_w(N)} \ll \#\left(W\setminus W_{\text{cent}}\right)\cdot\frac{1}{n^{2.5}} \leqslant n^{-1.5} = \mathrm{o}\big(n^{-1}\big).$$

Therefore, for any $t\neq 0$, it will suffice to prove that

$$\sum_{w\in W_{\text{cent}}}\frac{\left|\widehat{B_w}(t)\right|^2}{\rho_w(N)} \ll \frac{1}{n}. \tag{24}$$

We will prove the following technical claim.

Claim 22. *For any $0<t<N$, we have:*

$$\left|\widehat{B_w}(t)\right| \ll N^{-1}\binom{n}{w}\cdot\left(\frac{|n-2w|}{n}+\frac{1}{\sqrt{n}}\right).$$

This is a Krawtchouk-type upper bound over $\mathbb{Z}_N$. First, let us demonstrate that starting from this claim, we can prove our target Equation 24.

$$\begin{aligned}
\sum_{w\in W_{\mathrm{cent}}} \frac{\left|\widehat{B_w}(t)\right|^2}{\rho_w(N)} &\ll \sum_{w\in W_{\mathrm{cent}}} \frac{N^{-2}\binom{n}{w}^2}{N^{-1}\binom{n}{w}} \cdot \left(\frac{(n-2w)^2}{n^2}+\frac{1}{n}\right) \\
&\ll \sum_{w\in W_{\mathrm{cent}}} N^{-1}\binom{n}{w} \cdot \left(\frac{(n-2w)^2}{n^2}+\frac{1}{n}\right) \\
&\asymp \sum_{w\in W_{\mathrm{cent}}} Q^{-1}\binom{n}{w} \cdot \left(\frac{(n-2w)^2}{n^2}+\frac{1}{n}\right) \\
&\leqslant \frac{4}{n^2}\cdot \mathrm{Var}(X)+\frac{1}{n} \ll \frac{1}{n}. && (X\sim \mathrm{Bin}(n,1/2))
\end{aligned}$$

This concludes the proof that $\alpha^{\square}(N) \ll n^{-1}$. All that remains is to prove Claim 22; below Appendix G.5 does that.

G.5 Proof of Claim 22

Recall that

$$\widehat{B_w}(t) = \frac{1}{N} \sum_{0\leqslant x<Q\colon \mathrm{wt}(x)=w} \mathrm{e}_N(xt).$$

Note that this expression is identical to the following coefficient.

$$\widehat{B_w}(t) = \frac{1}{N}\cdot [z^w] \prod_{j=0}^{n-1} \left(1+z\cdot \mathrm{e}_N(2^j t)\right).$$

We will estimate this coefficient using the Cauchy integral method. Let us set up the machinery. Define $p \coloneqq w/n$ and $r \coloneqq p/(1-p)$. We will integrate along the contour of radius r centered at 0. We have the following upper bound:

$$\left|\widehat{B_w}(t)\right| \leqslant \frac{1}{2\pi N p^w (1-p)^{n-w}} \cdot \underbrace{\int_{-\pi}^{\pi} \left|\prod_{j=0}^{n-1} (1-p)+p\cdot \exp\left(\imath\cdot\left(\theta+\frac{2\pi\cdot 2^j t}{N}\right)\right)\right| \mathrm{d}\theta}_{I\coloneqq}.$$

We will prove the following technical lemma in Appendix G.6.

Lemma 23. *For $w\in W_{\mathrm{cent}}$ we have:*

$$I \ll \frac{|1-2p|}{\sqrt{n}}+\frac{1}{n}.$$

Once we have this lemma, Claim 22 is immediate:

$$\begin{aligned}
\left|\widehat{B_w}(t)\right| &\ll \frac{1}{2\pi N p^w (1-p)^{n-w}} \cdot \left(\frac{|1-2p|}{\sqrt{n}}+\frac{1}{n}\right) \\
&\asymp \frac{1}{N}\cdot\binom{n}{w}\cdot\left(|1-2p|+\frac{1}{\sqrt{n}}\right),
\end{aligned}$$

G.6 Integral Estimation: Proof of Lemma 23

Recall that $W_{\text{cent}} = \left\{w \in W : \ |w - n/2| \leqslant \sqrt{2n \log n}\right\}$. Here $p = w/n$. Recall that

$$I = \int_{-\pi}^{\pi} \prod_{j=0}^{n-1} \Big|(1-p) + p \exp(\imath\theta + \imath \cdot 2\pi\phi_j)\Big| \mathrm{d}\theta,$$

where $\phi_j = 2^j t/N$. We are going to pick two parameters $\ell_0 = \frac{1}{2}\log_2 n$ and $\theta_0 = \frac{1}{40}$ (a small angle less than $1/10\pi$).

Case: Arc $|\theta| > \theta_0$. This arc will contribute negligibly to the integral. This is because:

$$\begin{aligned}\prod_{j=0}^{n-1} \Big|(1-p) + p \exp(\imath\theta + \imath \cdot 2\pi\phi_j)\Big| &\leqslant \exp\left(-\frac{4}{9}\sum_{j=0}^{n-1} \sin^2\left(\frac{\theta}{2} + \frac{\pi 2^j t}{N}\right)\right) \qquad \text{(by Claim 24)} \\ &\leqslant \exp\left(-\frac{2}{45}\sin^2(\theta/2)\cdot(n-1)\right) \leqslant \exp(-cn). \\ &\qquad \text{(by the Dispersion Lemma 25 and } \sin^2(\theta/2) \geqslant \sin^2(\theta_0/2) > 0)\end{aligned}$$

The integral on this arc is $\ll \exp(-cn)$.

Case: Arc $|\theta| \leqslant \theta_0$. Recall that $\phi_0 = t/N$ and $\phi_j = \left\{2^j t/N\right\} \pmod 1$, where $\{x\}$ denotes the fractional part of x. Write down the (possibly infinite) binary representation of t/N. The indexing of the bits after the decimal place starts with $0, 1, 2, \ldots$. Two definitions are required for our case analysis:

1. We say that *the head has length h* if the binary representation begins with 0^h1 or 1^h0. Among the first n bits, the remaining bits are called the *tail*; its length is denoted by $h' = (n-h)$. In our case, $h \leqslant n$ because $t/N \geqslant \frac{1}{2}\cdot 2^{-n}$.

2. We say *a run of length ℓ starts at j* if the binary presentation at the j-th position after the decimal point is either 01^ℓ or 10^ℓ. Roughly speaking, if a long run starts at j in ϕ_0, then ϕ_j is $\ll 2^{-\ell}$ close to $1/2$.

Without loss of generality, we can assume that

$$A(\theta) \ \coloneqq \ |1-2p| + |\theta| \leqslant A \ \coloneqq \ \frac{1}{10}.$$

This is because, when $|n/2 - w| \leqslant \sqrt{2n\log n}$ and $|\theta| \leqslant \theta_0$, $A(\theta) \leqslant \theta_0 + \mathcal{O}\Big(\sqrt{n^{-1}\log n}\Big)$.

Next, by symmetry, we can assume that the binary expansion of ϕ_0 starts with a 0. This is because we can replace the variable t with $(N-t)$, and the integral remains unchanged.

Summary of our sub-cases.

1. Short tail: $h' \leqslant \ell_0$
2. Medium tail: $\ell_0 < h' \leqslant n/2$
3. One long run: A run of length $\geqslant \ell_0$

4. Long tail with no long run: $h' > n/2$ and all runs have length $< \ell_0$.

These cases are *exhaustive*. Cases 3 and 4 together cover the long tail case. After that, the remaining cases for short and medium tails are covered in 1 and 2, respectively. The choice of ℓ_0 ensures that $2^{-\ell_0} \asymp n^{-1/2}$.

1. Short tail: $h' \leqslant \ell_0$. Write $t = 2^a \cdot b$, for an odd b. Here, the binary expansion of ϕ_0 starts with $h = (n - h')$ zeroes. Observe that $b \leqslant t \leqslant N \cdot 2^{-h} \ll 2^{h'} \ll n^{1/2}$. Define $j^* = n - a - 1$. Now, ϕ_{j^*} is close to $1/2$.

$$\phi_{j^*} = \left\{\frac{2^{j^*} t}{N}\right\} = \left\{\frac{2^{n-1} b}{N}\right\}$$

After that

$$\|\phi_{j^*} - 1/2\|_{\mathbb{R}/\mathbb{Z}} = \|\phi_{j^*} - b/2\|_{\mathbb{R}/\mathbb{Z}} \leqslant \frac{b}{2}\left|\frac{2^n}{N} - 1\right| \ll \frac{b}{n} \ll n^{-1/2}.$$

So, we get

$$\left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_{j^*})\right| \ll A(\theta) + \frac{1}{\sqrt{n}} \qquad \text{(by Claim 24.3.)}$$

Now, we proceed to upper-bound the product:

$$\begin{aligned}
\prod_{j=0}^{n-1}\left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right| &\leqslant \left(A(\theta) + \frac{1}{\sqrt{n}}\right) \cdot \exp\left(-\frac{4}{9}\sum_{j \neq j^*} \sin^2\left(\frac{\theta}{2} + \frac{\pi 2^j t}{N}\right)\right) \\
&\qquad \text{(by Claim 24.1.)} \\
&\leqslant \left(A(\theta) + \frac{1}{\sqrt{n}}\right) \cdot \exp(4/9) \cdot \exp\left(-\frac{2}{45} \cdot \sin^2(\theta/2) \cdot (n-1)\right) \\
&\qquad \text{(by Lemma 25)} \\
&\ll \left(A(\theta) + \frac{1}{\sqrt{n}}\right) \cdot \exp(-cn\theta^2)
\end{aligned}$$

By integrating over the arc (and adding the exponentially small contribution from the arc $|\theta| \geqslant \theta_0$), we get $I \ll \frac{|1-2p|}{\sqrt{n}} + \frac{1}{n}$.

2. Sub-case: Medium tail: $\ell_0 \leqslant h' < n/2$. The integral I will be very small in this case.

First, observe that if there is a run of length ℓ starting at ϕ_j, then the following bound holds:

$$\left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right| \leqslant |1-2p| + |\theta| + 2^{-\ell} \leqslant A(\theta) + 2^{-\ell}.$$

(by Claim 24.3., because $2\pi \cdot \phi_j$ is $\left(2^{-\ell} + |\theta|\right)$ close to π)

Suppose the lengths of the maximal runs in the tail are $\ell_1, \ldots, \ell_r$. Note that $\ell_1 + \cdots + \ell_r = h'$. Now consider the product restricted to the tail[4]

$$\prod_{j=h-1}^{n-1}\left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right|$$

[4] A clarification: Suppose the binary representation of ϕ_0 is 0.000110... The head consists of zeros at indices 0, 1, and 2. The head length is $h = 3$ here. The first run (011) in the tail begins at index $h - 1 = 2$.

The indices that witness the start of the maximal runs contribute

$$\leqslant \prod_{j'=1}^{r} \left(A(\theta) + 2^{-\ell_{j'}}\right) \leqslant 2 \cdot \left(A(\theta) + 2^{-h'}\right).$$

(by our compression Lemma 26 proved in Appendix G.7)

Next, all remaining terms are trivially upper-bounded by 1. Therefore, we conclude with the following upper bound:

$$\prod_{j=h-1}^{n-1} \left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right| \leqslant 2 \cdot \left(A(\theta) + 2^{-h'}\right).$$

Next, let us look at the remaining contribution from the head

$$\begin{aligned}\prod_{j=0}^{h-2} \left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right| &\leqslant \exp\left(-\frac{4}{9}\sum_{j=0}^{h-2} \sin^2\left(\frac{\theta}{2} + \frac{\pi 2^j t}{N}\right)\right) && \text{(by Claim 24)}\\ &\leqslant \exp\left(-\frac{2}{45}\sin^2(\theta/2)\cdot(h-2)\right) \leqslant \exp(-ch\theta^2).\\ &&& \text{(by the dispersion Lemma 25 and } \sin^2(\theta/2) \gg \theta^2)\end{aligned}$$

Putting the head and tail contributions together, we have:

$$\begin{aligned}\prod_{j=0}^{n-1} \left|(1-p) + p\exp(\imath\theta + \imath \cdot 2\pi\phi_j)\right| &\leqslant 2 \cdot \left(A(\theta) + 2^{-h'}\right) \cdot \exp(-ch\theta^2)\\ &\ll (A(\theta) + n^{-1/2}) \cdot \exp(-c'n\theta^2).\end{aligned}$$

Just like in the previous case, integration of this Gaussian gives $I \ll \frac{|1-2p|}{\sqrt{n}} + \frac{1}{n}$.

3. Sub-case: a run of length $\geqslant \ell_0$. Let the run start at j^*. In this arc, we have:

$$\left|(1-p) + p\cdot\exp(\imath\cdot\theta + \imath\cdot 2\pi\phi_{j^*})\right| \leqslant |1-2p| + |\theta| + 2^{-\ell_0}.$$

(by Claim 24.3., because $2\pi\cdot\phi_{j^*}$ is $2^{-\ell_0} + |\theta|$ close to π)

The rest of the contribution is bounded by

$$\begin{aligned}\prod_{j\neq j^*} \left|(1-p) + p\cdot\exp(\imath\cdot\theta + \imath\cdot 2\pi\phi_j)\right| &\leqslant \exp\left(-\frac{4}{9}\sum_{j\neq j^*} \sin^2\left(\frac{\theta + 2\pi\phi_j}{2}\right)\right) && \text{(by Claim 24.1.)}\\ &\leqslant \exp(4/9)\cdot\exp\left(-\frac{4}{9}\sum_{j=0}^{n-1} \sin^2\left(\frac{\theta + 2\pi\phi_j}{2}\right)\right)\\ &\ll \exp\left(-\frac{4}{9}\cdot\frac{n-1}{10}\sin^2(\theta/2)\right) && \text{(by Lemma 25)}\\ &\ll \exp(-c'n\theta^2).\\ &&& \text{(because } \sin^2 x \gg x^2 \text{ when } x \in [-\pi/2, \pi/2])\end{aligned}$$

After this, we have

$$\int_{-\theta_0}^{\theta_0} \prod_j \Big|(1-p)+p\cdot\exp(\imath\cdot\theta+\imath\cdot 2\pi\phi_j)\Big|\mathrm{d}\theta \ll \int_{-\theta_0}^{\theta_0}\left(|1-2p|+|\theta|+2^{-\ell_0}\right)\cdot\exp(-c'n\theta^2)\mathrm{d}\theta$$
$$\ll \frac{|1-2p|}{\sqrt{n}}+\frac{1}{n}+\frac{2^{-\ell_0}}{\sqrt{n}}.$$

So, overall, this sub-case also leads to $I \ll \frac{|1-2p|}{\sqrt{n}}+\frac{1}{n}$.

4. Sub-case: Long tail $h' \geqslant n/2$ with no length-ℓ_0 runs. In this case, ϕ_0 has runs of length (ℓ_0-1) or shorter, and ϕ_0 has a long tail, $h' \geqslant n/2$. Break the tail bits into ℓ_0-bit blocks. Within each block, there must be at least one occurrence of 01 or 10. If 01 or 10 occurs at the j-th position of ϕ_0's binary representation, then $\phi_j \in [1/4, 3/4]$. Therefore, there are at least $B \gg n/\ell_0$ indices j satisfying $\phi_j \in [1/4, 3/4]$. In this arc, using the fact that $|\theta| \leqslant \theta_0 \leqslant \pi/3$, we have

$$\frac{\theta+2\pi\phi_j}{2} \in [\pi/12, 11\pi/12].$$

For such angles

$$\sin^2\left(\frac{\theta+2\pi\phi_j}{2}\right) \geqslant \sin^2(\pi/12)$$

Next, the product is upper-bounded as follows:

$$\prod_j\Big|(1-p)+p\cdot\exp(\imath\cdot\theta+\imath\cdot 2\pi\phi_j)\Big| \leqslant \exp(-dB) \qquad \text{(by Claim 24.1)}$$
$$\leqslant \frac{1}{n}.$$

So, the integral on this arc is $\ll 1/n$. Again, for this case, $I \ll 1/n$.

G.7 Technical Results for Integral Estimation

Define:

$$L(p,\varphi) \;\coloneqq\; \Big|(1-p)+p\cdot\exp(\imath\varphi)\Big|. \tag{25}$$

Claim 24. *For $1/3 \leqslant p \leqslant 2/3$ and every $\varphi \in [-\pi, \pi]$ the following bounds hold:*

1. $L(p,\varphi) \leqslant \exp\left(-\frac{4}{9}\sin^2(\varphi/2)\right)$.
2. $L(p,\varphi) \leqslant |1-2p| + \cos(\varphi/2)$.
3. *If $|\pi-\varphi| \leqslant \varepsilon$, then $L(p,\varphi) \leqslant |1-2p|+\varepsilon$.*

Proof. We have:

$$\begin{aligned}
L(p,\varphi)^2 &= (1-p)^2+p^2+2(1-p)p\cdot\cos\varphi \\
&= 1-4p(1-p)\cdot\sin^2(\varphi/2) \\
&\leqslant \exp\left(-4p(1-p)\cdot\sin^2(\varphi/2)\right) && \text{(because } 1-t\leqslant\exp(-t)\text{)} \\
&\leqslant \exp\left(-\frac{8}{9}\cdot\sin^2(\varphi/2)\right). && \text{(because } 1/3\leqslant p\leqslant 2/3\text{)}
\end{aligned}$$

We rewrite

$$\begin{aligned} L(p,\varphi)^2 &= \cos^2(\varphi/2) + (1-2p)^2 \cdot \sin^2(\varphi/2) \\ &\leqslant \cos^2(\varphi/2) + |1-2p|^2. \end{aligned}$$

By Minkowski, the second bound follows. For the last one, note that $\cos^2(\varphi/2) = \sin^2((\pi-\varphi)/2) \leqslant \varepsilon^2$. □

Lemma 25 (Dispersion Lemma)**.** *The following bound holds for any n, α, β*

$$S_n(\alpha,\beta) \;\coloneqq\; \sum_{j=0}^{n-1} \sin^2\left(\alpha + 2^j\beta\right) \geqslant \frac{n-1}{10}\sin^2\alpha.$$

Proof. Define $\theta_j = \alpha + 2^j\beta$. Note that $\theta_{j+1} = 2\theta_j - \alpha \pmod{\pi}$. So, $|\sin(\alpha)| = |\sin(2\theta_j - \theta_{j+1})|$. Next, note that

$$|\sin(2\theta_j - \theta_{j+1})| \leqslant |\sin(2\theta_j)| + |\sin\theta_{j+1}| \leqslant 2|\sin\theta_j| + |\sin\theta_{j+1}|.$$

From this, we conclude that

$$\sin^2(2\theta_j - \theta_{j+1}) \leqslant 4\sin^2\theta_j + \sin^2\theta_{j+1} + 4\sin\theta_j\sin\theta_{j+1} \leqslant 5(\sin^2\theta_j + \sin^2\theta_{j+1}).$$

We conclude:

$$\sin^2(\alpha) \leqslant 5\left(\sin^2\theta_j + \sin^2\theta_{j+1}\right)$$

Adding over all $j \in \{0, 1, \ldots, n-1\}$, we get:

$$(n-1)\sin^2\alpha \leqslant 5\sum_{j=0}^{n-2}\left(\sin^2\theta_j + \sin^2\theta_{j+1}\right) \leqslant 10\sum_{j=0}^{n-1}\sin^2\theta_j.$$ □

Lemma 26 (Compression)**.** *Let $0 \leqslant A \leqslant \frac{1}{10}$. Consider arbitrary integers $\ell_1, \ldots, \ell_r \geqslant 1$. Then, the following bound holds.*

$$\prod_{u=1}^{r}\left(A + 2^{-\ell_u}\right) \leqslant 2\cdot\left(A + 2^{-\sum_{u=1}^{r}\ell_u}\right).$$

Proof. The case of $r = 1$ is trivial.

Consider the remaining case $r \geqslant 2$. Suppose there is one index u such that $\ell_u \geqslant 2$. In this case, for any index $v \neq u$, we have:

$$\begin{aligned} \left(A + 2^{-\ell_u}\right)\cdot\left(A + 2^{-\ell_v}\right) &= A^2 + A\left(2^{-\ell_u} + 2^{-\ell_v}\right) + 2^{-\ell_u-\ell_v} \\ &\leqslant \frac{A}{10} + A\left(\frac{1}{4} + \frac{1}{2}\right) + 2^{-\ell_u-\ell_v} \\ &\leqslant A + 2^{-\ell_u-\ell_v}. \end{aligned}$$

Because $\ell_u + \ell_v \geqslant \ell_u \geqslant 2$, we can continue this process and upper-bound the product by $A + 2^{-\sum_u \ell_u}$, thereby proving the compression lemma.

The only remaining case is that $\ell_u = 1$, for all u. Since $r \geqslant 2$, we consider the first two indices:

$$\left(A + \frac{1}{2}\right)\cdot\left(A + \frac{1}{2}\right) \leqslant \frac{1}{10}\cdot A + A + \frac{1}{4} \leqslant 2\cdot\left(A + 2^{-2}\right)$$

So, we got a term of the form "A plus a $\geqslant 2$-power of two," this can now help us jump-start the previous process. We can now proceed along the $\ell_u \geqslant 2$ case to complete the proof. □

H Lower Bound: Proof of Technical Lemma 6

Note that $N \cdot \widehat{S_w}(-1) = [z^w] \prod_{j=0}^{n-1} \left(1 + z \cdot \mathrm{e}_N(2^j)\right)$. Denote $c_w = [z^w] \prod_{j=0}^{n-1} \left(1 + z \cdot \mathrm{e}_N(2^j)\right)$. So, our target is to prove:

$$\sum_{w \in W} |c_w| \geqslant \frac{1}{10} \cdot N \cdot n^{-1/2}.$$

We will handle the two (exhaustive) cases $n = 3$ and $n \geq 5$ separately.

Case 1: $n = 3$: Let $\zeta = \mathrm{e}_7(1)$ and set $s := \zeta + \zeta^2 + \zeta^4 = c_1$. Then

$$s^2 = \zeta^2 + \zeta^4 + \zeta^8 + 2(\zeta^3 + \zeta^5 + \zeta^6) = \zeta + \zeta^2 + \zeta^4 + 2(-1 - \zeta - \zeta^2 - \zeta^4) = -2 - s.$$

Thus $s^2 + s + 2 = 0$, and hence $|s| = \sqrt{2}$. Therefore,

$$\sum_{w \in W} |c_w| \geq |c_1| = \sqrt{2} > \frac{7}{10\sqrt{3}} = \frac{1}{10} \cdot \frac{N}{\sqrt{n}}.$$

Case 2: $n \geqslant 5$: We first introduce the following auxiliary variables:

$$a_w \ := \sum_{0 \leqslant x < 2^{n-1} \colon \mathrm{wt}(x) = w} \mathrm{e}_N(x).$$

Note that

$$c_w = a_w + \mathrm{e}_N(2^{n-1}) \cdot a_{w-1} = a_w - \mathrm{e}_N(1/2) \cdot a_{w-1} = (a_w - a_{w-1}) + (1 - \mathrm{e}_N(1/2)) \cdot a_{w-1}.$$

So, we get the following lower bound:

$$\sum_{w \in W} |c_w| \geqslant \underbrace{\left(\sum_{w \in W} |a_w - a_{w-1}| \right)}_{\text{main term}} - \underbrace{\left(|1 - \mathrm{e}_N(1/2)| \sum_{w \in W} |a_{w-1}| \right)}_{\text{perturbation}}$$

First, we will show that the perturbation is small. Note that

1. $|1 - \mathrm{e}_N(1/2)| \leqslant \pi/N$
2. $|a_{w-1}| \leqslant \binom{n-1}{w-1}$

From these, the perturbation is upper-bounded as follows:

$$\text{perturbation} \leqslant \frac{\pi}{N} \cdot 2^{n-1} < \pi.$$

Next, we lower bound the main term. Let $t := \frac{n-1}{2}$. Note that a_w is the sum of $e_N(x)$, where $0 \leq x < 2^{n-1}$. For these values of x, the argument of $e_N(x)$ lies in $[0, \pi)$. So,

$$|a_w - a_{w-1}| \geq |\Im a_w - \Im a_{w-1}|.$$

Using the triangle inequality, we have

$$\sum_{w=0}^{t} |a_w - a_{w-1}| \geq |a_t - a_{-1}| \geq \Im a_t,$$

$$\sum_{w=t+1}^{n-1} |a_w - a_{w-1}| \geq |a_t - a_{n-1}| \geq \Im a_t - \Im a_{n-1} \geq \Im a_t - 1.$$

Therefore,main term $> 2\Im a_t - 1$. So, it will suffice to lower bound $\Im a_t$. Let us denote the j-th octant we mean the interval

$$\left[\frac{(j-1)\pi}{4}, \frac{j\pi}{4}\right), \qquad j = 1, \ldots, 8.$$

Our strategy will be to show that the $\Im\, \mathrm{e}_N(x)$ contributions whose arguments are in octants 2 and 3 already help us reach our target lower bound. We proceed with the following observations.We record the following observations.

- If the binary representation of x begins with 010 or 001, then $2^{n-3} \leq x < 3 \cdot 2^{n-3}$. Hence $\frac{\pi}{4} < \frac{2\pi x}{N} < \frac{3\pi}{4}$, and therefroe we have $\Im e_N(x) \geq \frac{1}{\sqrt{2}}$.
- The total number of such x with $\mathrm{wt}(x) = t$ is exactly $2\binom{n-3}{\frac{n-3}{2}}$.

Therefore,

$$\Im\ a_t \geq \sqrt{2}\binom{n-3}{\frac{n-3}{2}}.$$

Hence, considering the perturbation, we have

$$\sum_{w \in W} |c_w| \geq 2\sqrt{2}\binom{n-3}{\frac{n-3}{2}} - (\pi + 1) > 2\sqrt{2}\binom{n-3}{\frac{n-3}{2}} - \frac{29}{7}. \qquad \text{(Since } \pi <= \tfrac{22}{7}\text{)}$$

Now, we will use the exact value for the binomial coefficient for $n = 5, 7$ and then for $n \geqslant 9$ we will use the general lower bound for the binomail coefficient to obtain the desired result. From the above bound, for $n = 5$, we have

$$\sum_{w \in W} |c_w| > 4\sqrt{2} - \frac{29}{7} > \frac{31}{10\sqrt{5}} = \frac{1}{10} \cdot \frac{N}{\sqrt{n}}.$$

For $n = 7$, we obtain

$$\sum_{w \in W} |c_w| > 12\sqrt{2} - \frac{29}{7} > \frac{127}{10\sqrt{7}} = \frac{1}{10} \cdot \frac{N}{\sqrt{n}}.$$

Now, consider the cases where $n \geqslant 9$. Since,

$$\begin{aligned}\binom{n-3}{\frac{n-3}{2}} &\geqslant \frac{2^{n-3}}{\sqrt{\pi\left(n + \frac{1}{4} + \frac{1}{16(n-3)}\right)}} = \frac{1}{8\sqrt{\pi}} \cdot \frac{2^n - 1}{\sqrt{\left(n + \frac{1}{4} + \frac{1}{16(n-3)}\right)}} \quad \text{(see [BBM+21, Section J.2.2])} \\ &\geqslant \frac{\sqrt{10}}{32\sqrt{\pi}} \cdot \frac{N}{\sqrt{n}} \qquad \left(\text{since } \frac{1}{\sqrt{\left(n+\frac{1}{4}+\frac{1}{16(n-3)}\right)}} \geqslant \frac{\sqrt{10}}{4} \cdot \frac{1}{\sqrt{n}}\right)\end{aligned}$$

Therefore, using $\pi \leqslant 22/7$, we have

$$\sum_{w \in W} |c_w| \geqslant \frac{\sqrt{70}}{16\sqrt{11}} \cdot \frac{N}{\sqrt{n}} - \frac{29}{7} \geqslant \frac{1}{8} \cdot \frac{N}{\sqrt{n}} - \frac{29}{7} \geqslant \frac{1}{10} \cdot \frac{N}{\sqrt{n}},$$

where the last inequality true for $n \geqslant 9$.

I Lower Bound: Proof of Theorem 7

Recall $W = \{0, 1, \ldots, n\}$. Since $m < n$, this will capture all possible weights. Let $\delta := |2^n - N|/N \leq 2^m/N$ denote the distortion from the ideal behavior. In our proof, in fact, we will use the quantity

$$L := \#\left\{0 \leqslant j < n : 2^j\delta \leqslant (1/10\pi) \cdot n^{-1/2}\right\}.$$

Note that set above is an interval and that its cardinality $L \geqslant \left(n - m - \frac{1}{2} \cdot \log_2 n - \mathcal{O}(1)\right)$.

For phases $\mathbf{\Phi} := \left(\, \mathbf{\Phi}_{\mathbf{w}} : \mathbf{w} \in W^k \,\right)$, we know that

$$E_k(s) = \max_{\mathbf{\Phi}} \left| \sum_{\mathbf{w} \in W^k} \mathbf{\Phi}_{\mathbf{w}} \sum_{t \neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \widehat{S_{\mathbf{w}_j}}(t) \right|$$

We will restrict to $\mathbf{\Phi}_{\mathbf{w}} := \prod_{j=1}^{k} \phi^{\mathbf{w}_j}$ for some appropriately chosen phase ϕ. Then, for this restriction, we have

$$E_k(s) \geqslant \left| \sum_{\mathbf{w} \in W} \sum_{t \neq 0} \mathrm{e}_N(st) \prod_{j=1}^{k} \phi^{\mathbf{w}_j} \widehat{S_{\mathbf{w}_j}}(t) \right| = \Bigg| \underbrace{\sum_{t \neq 0} \left(\sum_{w \in W} \phi^w \widehat{S_w}(t) \right)^k}_{=: f} \cdot \chi_t(s) \Bigg|$$

Note that

$$\widehat{f}(t) = \left(\sum_{w \in W} \phi^w \widehat{S_w}(t) \right)^k.$$

Define the set $H := \left\{-2^j : 0 \leqslant j < L\right\}$. We have:

$$\begin{aligned}
\max_{0 \leqslant s < N} E_k(s) &\geqslant \max_{0 \leqslant s < N} |f(s)| \\
&\geqslant \sqrt{\frac{1}{N} \sum_{0 \leqslant s < N} |f(s)|^2} && \text{(monotonicity of norms)} \\
&= \sqrt{\sum_{t} \left|\widehat{f}(t)\right|^2} && \text{(Parseval's identity)} \\
&\geqslant \sqrt{\sum_{t \in H} \left|\widehat{f}(t)\right|^2} \\
&\geqslant L^{1/2} \cdot \min_{t \in H} \left|\widehat{f}(t)\right| = L^{1/2} \min_{t \in H} \left| \sum_{w} \phi^w \widehat{S_w}(t) \right|^k.
\end{aligned}$$

So, to prove Theorem 7, it will suffice to show that: There is a choice of phase ϕ such that for all $0 \leqslant j < L$, the following estimate is satisfied.

$$\left| \sum_{w \in W} \phi^w \widehat{S_w}(-2^j) \right| \geqslant \left(\frac{1}{25}\right) \cdot n^{-1/2}. \tag{26}$$

Let us begin towards lower-bounding this target expression. We begin by observing that our target expression (inside the $|\cdot|$) is the following polynomial.

$$T(t) := \sum_{w \in W} \phi^w \widehat{S_w}(-t) = \frac{1}{N} \sum_{w \in W} \phi^w \sum_{x \in S_w} \mathrm{e}_N(xt) = \frac{1}{N} \sum_{0 \leqslant x < N} \phi^{\mathrm{wt}(x)} \mathrm{e}_N(xt).$$

We will compare this expression against an ideal baseline:

$$I(t) \coloneqq \frac{1}{N}\sum_{0\leqslant x<2^n} \phi^{\mathrm{wt}(x)}\mathrm{e}_N(xt) = \frac{1}{N}\prod_{\ell=0}^{n-1}\left(1+\phi\cdot \mathrm{e}_N\left(2^\ell t\right)\right).$$

By the union bound, we have

$$|T(t)| \geqslant |I(t)| - \frac{|2^n-N|}{N} = |I(t)| - \delta.$$

Thus, it would suffice to choose ϕ such that for every $t \in \left\{\, 2^j \,:\, 0\leqslant j < \min\{L, n-1\}\,\right\}$, we have $|I(t)| \geqslant \frac{21}{275}\cdot n^{-1/2}$ and it can absorb δ into it, which has magnitude at most $\frac{1}{10\pi}\cdot n^{-1/2}$.

Let us substitute $\phi = \exp(-\imath\theta)$, where $\theta = n^{-1/2}$ is a positive angle. Fix j and let us begin on our new target of proving the lower bound:

$$\left|I(2^j)\right| = \frac{1}{N}\prod_{\ell=0}^{n-1}\left|1+\exp\left(-\imath\theta + 2\pi\imath\cdot 2^{\ell+j}/N\right)\right| \geqslant \frac{21}{275}\cdot n^{-1/2}. \tag{27}$$

Our aim is to lower-bound the RHS terms separately based on which of the three conditions it satisfies below.

Case 1: $\ell + j \geqslant n$. Define the gap $g = \ell + j - n$. Note that $0 \leqslant g < j$. For this analysis, we will need the signed version of δ defined as

$$\Delta \coloneqq \frac{2^n - N}{N}.$$

Using this, we can write:

$$\exp\left(2\pi\imath\cdot\frac{2^{\ell+j}}{N}\right) = \exp\left(2\pi\imath\cdot\frac{2^{n+g}}{N}\right) = \exp\left(2\pi\imath\cdot 2^g\cdot(1+\Delta)\right) = \exp\left(2\pi\imath\cdot 2^g\Delta\right)$$

Note that the magnitude of this angle

$$|2\pi\cdot 2^g\Delta| \leqslant \pi\cdot 2^j\delta \leqslant \frac{1}{10}\cdot n^{-1/2},$$

because $g < j$ and $2^j\delta \leqslant \frac{1}{10\pi}\cdot n^{-1/2}$ by the definition of the quantity L. These angles will be significantly small in magnitude compared to $\theta = n^{-1/2}$. As a consequence, we will have:

$$\left|1+\exp\left(-\imath\theta + 2\pi\imath 2^{\ell+j}/N\right)\right| \geqslant 2\cos\left(\frac{n^{-1/2}+\frac{1}{10}\cdot n^{-1/2}}{2}\right)$$

Now, we estimate the cumulative contribution of all j satisfying $\ell + j \geqslant n$.

$$\begin{aligned}
\prod_{\substack{0\leqslant\ell<j:\\ \ell+j\geqslant n}}\left|1+\exp\left(-\imath\theta+2\pi\imath 2^{\ell+j}/N\right)\right| &= \prod_{g=0}^{j-1}\left|1+\exp\left(-\imath\theta+2\pi\imath 2^{n+g}/N\right)\right| \\
&\geqslant \left(2\cos\left(\frac{11\cdot n^{-1/2}}{20}\right)\right)^j \\
&\geqslant 2^j\cdot\exp\left(-\frac{2}{\pi}\cdot\left(\frac{11}{20}\right)^2\cdot n^{-1}j\right) \\
&\qquad \text{(using technical Lemma 27, a Gaussian lower bound on cosine)} \\
&\geqslant 2^j\cdot\frac{4}{5}. \qquad \text{(because } j\leqslant n \text{ and } \exp(-1/5)\geqslant 1-1/5.)
\end{aligned}$$

Case 2: $\ell + j = n - 1$**.** In this case, we have

$$\exp\left(2\pi\imath \cdot \frac{2^{\ell+j}}{N}\right) = \exp\left(2\pi\imath \cdot \frac{2^{n-1}}{N}\right) = \exp\left(\pi\imath \cdot \frac{2^n}{N}\right) = \exp\left(\pi\imath \cdot (1+\Delta)\right) = -\exp\left(\pi\imath \cdot \Delta\right)$$

Our concern is that the magnitude of the term $\left|1 + \phi \cdot \mathrm{e}_N(2^{\ell+j})\right|$ may become too small. However, the magnitude of Δ being much smaller than $\theta = n^{-1/2}$ will save us. Indeed,

$$\begin{aligned}
\left|1 + \exp\left(-\imath\theta + 2\pi\imath 2^{\ell+j}/N\right)\right| &= \left|1 - \exp\left(-\imath\theta + \pi\imath \cdot \Delta\right)\right| \\
&\geqslant \left|1 - \exp\left(-\imath\theta + \pi\imath \cdot \delta\right)\right| = 2\sin\left(\frac{\theta - \pi\delta}{2}\right) \\
&\geqslant 2\sin\left(\frac{n^{-1/2} - \frac{1}{10}\cdot n^{-1/2}}{2}\right) \\
&\geqslant \frac{9}{5\pi} \cdot n^{-1/2}. \qquad \text{(because } \sin t \geqslant \tfrac{2}{\pi} \cdot t\text{)}
\end{aligned}$$

Case 3: $\ell + j < n - 1$**.** Again, we write the gap $g = n - (\ell + j)$. Note that $2 \leqslant g \leqslant n - j$. As before, we rewrite:

$$\exp\left(2\pi\imath \cdot \frac{2^{\ell+j}}{N}\right) = \exp\left(2\pi\imath \cdot \frac{2^{n-g}}{N}\right) = \exp\left(2\pi\imath \cdot 2^{-g} \cdot \frac{2^n}{N}\right) = \exp\left(2\pi\imath \cdot 2^{-g} \cdot (1+\Delta)\right)$$

Now, we will lower-bound the magnitude of the term

$$\left|1 + \exp\left(-\imath\theta + 2\pi\imath 2^{\ell+j}/N\right)\right| = 2\cos\left(\frac{-\theta + 2\pi \cdot 2^{-g}(1+\Delta)}{2}\right) = 2\cos\left(-\frac{\theta}{2} + \pi 2^{-g} + \pi 2^{-g}\Delta\right).$$

Now, let us consider the cumulative contributions of these terms:

$$\begin{aligned}
\prod_{\substack{0 \leqslant \ell < j: \\ \ell + j < n-1}} \left|1 + \exp\left(-\imath\theta + 2\pi\imath 2^{\ell+j}/N\right)\right| &= \prod_{g=2}^{n-j} 2\cos\left(-\frac{\theta}{2} + \pi 2^{-g} + \pi 2^{-g}\Delta\right) \\
&= 2^{n-j-1} \prod_{g'=0}^{n-j-2} \cos\left(\frac{\pi}{4} \cdot 2^{-g'} - \left(\frac{\theta}{2} - \frac{\pi}{4}\Delta \cdot 2^{-g'}\right)\right).
\end{aligned}$$

Note that $\pi 2^{-g} \in (0, \pi/4]$. The angle $\pi 2^{-g}\Delta = \frac{\pi}{4}\Delta \cdot 2^{-g'}$ will have magnitude $\leqslant \pi\delta/4$, which will be much smaller than $\theta/2$. The argument of the cosine is always $\leqslant \pi/4$ (in magnitude) and is the difference of two positive angles. We will use the fact that for positive u, v, we have $(u-v)^2 \leqslant u^2 + v^2$.

We continue simplifying the RHS.

$$\prod_{\substack{0\leqslant \ell<j:\\ \ell+j<n-1}} \left|1+\exp\left(-\imath\theta+2\pi\imath 2^{\ell+j}/N\right)\right| \geqslant 2^{n-j-1}\prod_{g'=0}^{n-j-2}\exp\left(-\frac{2}{\pi}\cdot\underbrace{\left(\frac{\pi}{4}\cdot 2^{-g'}\right)^2}_{u^2}-\frac{2}{\pi}\cdot\underbrace{\left(\frac{\theta}{2}-\frac{\pi}{4}\Delta 2^{-g'}\right)^2}_{v^2}\right)$$

(by the Gaussian lower bound on cosine, Lemma 27)

$$\geqslant 2^{n-j-1}\prod_{g'=0}^{n-j-2}\exp\left(-\frac{2}{\pi}\cdot\left(\frac{\pi}{4}\cdot 2^{-g'}\right)^2-\frac{2}{\pi}\cdot\left(\frac{\theta}{2}+\frac{\pi}{4}\delta 2^{-g'}\right)^2\right)$$

$$\geqslant 2^{n-j-1}\exp\left(-\frac{\pi}{6}-\frac{1}{2\pi}\quad\underbrace{-\frac{\theta\delta}{2}\cdot 2-\frac{\pi}{8}\delta^2\cdot\frac{4}{3}}_{\mathcal{O}(n^{-1})}\right)$$

$$\geqslant 2^{n-j}\cdot\frac{1}{4}.$$

(Used calculation: $\exp(-\pi/6-1/2\pi)>1/2$ and the bound holds for $n\geqslant 4$)

Putting together the three pieces. We can substitute the three lower bounds to obtain a lower bound on our ideal polynomial.

$$\begin{aligned}\left|I(2^j)\right| &= \frac{1}{N}\prod_{\ell=0}^{n-1}\left|1+\exp(-\imath\theta+2\pi\imath\cdot 2^{\ell+j}/N)\right| \\ &\geqslant \frac{2^n}{N}\cdot\frac{4}{5}\cdot\frac{9}{5\pi}\cdot\frac{1}{4}\cdot n^{-1/2} \\ &\geqslant \frac{2}{3}\cdot\frac{9}{25\pi}\cdot n^{-1/2} > \frac{21}{275}\cdot n^{-1/2}. \qquad \text{(because } 2^n/N\geqslant 2/3 \text{ and } \pi<22/7)\end{aligned}$$

This is what we set ourselves out to achieve in Equation 27.

Conclusion. We have proved that $\left|I(2^j)\right|\geqslant\frac{21}{275}\cdot n^{-1/2}$. This implies the following lower bound for our target polynomial:

$$\left|T(2^j)\right|\geqslant\left(\frac{21}{275}-\frac{1}{10\pi}\right)\cdot n^{-1/2}>\frac{12}{275}\cdot n^{-1/2}>\frac{1}{25}\cdot n^{-1/2}.$$

Here we use $\pi>3.1$. This was our target from Equation 26. So, overall, we proved that

$$\max_{0\leqslant s<N}E_k(s)\geqslant\sqrt{\frac{1}{N}\sum_{0\leqslant s<N}E_k(s)^2}\geqslant L^{1/2}\cdot\left(\frac{1}{25}\right)^k\cdot n^{-k/2}.$$

This proves the theorem.

I.1 A technical result

Lemma 27 (Gaussian Lower bound on Cosine)**.** *For all $|x|\leqslant\pi/4$, we have*

$$\cos x\geqslant\exp\left(-\frac{2}{\pi}x^2\right).$$

Proof. We need to prove that the following function is non-negative for $x \in [0, \pi/4]$.

$$f(x) = \ln \cos x + \frac{2}{\pi} \cdot x^2.$$

The result follows from the fact that $f'(x) = -\tan x + \frac{4}{\pi} \cdot x \geqslant 0$ when $x \in [0, \pi/4]$. The equality holds at $x = 0$ and $x = \pi/4$, and between those extremes $\tan x \leqslant \frac{4}{\pi} x$. □

J Broader Context of our Research Question

Additive secret sharing is best viewed as an operational primitive for splitting trust, extending beyond its traditional role in cryptography and privacy. It is a cornerstone of threshold cryptography and secure computation, and increasingly serves as a system-level tool for privacy-preserving data use, federated learning, large-scale telemetry, and browser measurements. Across these settings, whether the underlying data are gradients, counters, health data, or records, the core question remains the same: *what information is revealed by simple functions of all the shares?*

The groups. In practice, additive/arithmetic secret sharing is most commonly instantiated over two kinds of algebraic domain. Over prime fields $\mathbb{F}_p$ (or small extensions), as in Shamir's scheme [Sha79] and its descendants in threshold cryptography and MPC [Des88, BGW88, DF92, Sho00, CDN01, DPSZ12, BDOZ11, DPSZ12]. Or, over rings $\mathbb{Z}/2^n\mathbb{Z}$, which align with native word arithmetic and enable highly efficient implementations [CDN01, ADEN21, DEF+19, CDE+18]. The latter setting is also standard in masking and mixed Boolean/arithmetic countermeasures against side-channel leakage, where arithmetic shares modulo 2^n interact naturally with machine-word operations and conversion routines [CG00, ISW03, CPRR14, CGV14, CGTV15, Cor17, CGMZ22]. This ambient group choice is tightly coupled to concrete design tradeoffs in real systems.

Small number of shares. While asymptotics in the number of shares arise in virtualization techniques (for example, MPC in the head, cut-and-choose, or watchlists), practical deployments overwhelmingly operate in the constant-party regime. For example, aggregation and telemetry may involve millions of clients, yet only a few servers hold the shares. This is the dominant setting in secure computation, threshold cryptography, or (software/hardware) masking countermeasures [NRR06, GM11, NRS11, GMK16, CGV14]. Thus, whether driven by efficiency or trust boundaries, the small-party regime is the norm, and analysis must capture the exact combinatorics of a few correlated shares rather than depend on asymptotic smoothening.

Hamming weight leakage. Since the foundational work of Kocher and of Kocher–Jaffe–Jun, side-channel attacks have shown that cryptographic devices can leak secret information through runtime behavior and power consumption [Koc96, KJJ99]. A central leakage model posits that measured power correlates with the Hamming weight, or with the Hamming distance from a reference state, of manipulated data; this is the basis of classical DPA/CPA attacks and of much of the modern masking literature [Mes00, CG00, BCO04, MOP07]. So, the goal is to keep the shares uninformative even under leakage [ISW03, CPRR14, CGV14, Cor17, CGZ20, CGC+21, CGMZ22]. Hamming-weight leakage more is not merely convenient, but a mathematically tractable proxy for a central engineering constraint.

Leakage resilience. Leakage resilience is a broad area; we refer to [KR19] for a comprehensive overview. There is extensive literature on protecting computation from leakage [ISW03, MR04, DP08, Rot12, PR13, MV13, FRR+14, GR15, GIM+16, GIW17, BIS19, IS24, IS25]. For secret sharing, a large portion of the literature is devoted to the construction of new schemes that are built to be resilient to leakage attacks [BPRW16, GK18, KMS19, BS19, BIS19, ADN+19, CGG+20, FY19, SV19, FY20, HVW20, MSV20, CKOS22]. Here, we instead characterize the inherent resilience of standard, linear schemes, such as additive and Shamir secret sharing [BDIR18, BDIR21, MNP+21, MPSW21, MNP+22a, MNP+22b, MNPCW22, KK23, MNPY24, Ngu25, HMNY25].

Summary of [FMM+24] analysis. For completeness, let us summarize the analysis pathway of [FMM+24] below. Their analysis will only use the fact that the doubling map $x \mapsto 2x$ induces length-n orbits in S_w, and the densities of the sets S_w in $\mathbb{Z}/N\mathbb{Z}$. Recall N is a Mersenne prime and $N = 2^n - 1$. Define $\rho_w := N^{-1}\binom{n}{w}$. Note that $\max_{t\neq 0}\left|\widehat{S_w}(t)\right| \leqslant \sqrt{\rho_w/n}$ because of Parseval's identity and $\widehat{S_w}(t) = \widehat{S_w}(2^j t)$, for $t \neq 0$ and $j \in \{0, 1, \ldots, n-1\}$, when $N = 2^n - 1$ and n is a prime.

$$
\begin{aligned}
E_k(s) &\leqslant \sum_{\mathbf{w}\in W^k} \sum_{t\neq 0} \prod_{j=1}^{k} \left|\widehat{S_{\mathbf{w}_j}(t)}\right| && \text{(triangly inequality proxy of Equation 28)} \\
&\leqslant \sum_{\mathbf{w}\in W^k} \left(\sum_{t\neq 0} \prod_{j=1}^{2} \widehat{S_{\mathbf{w}_j}(t)}\right) \left(\prod_{j=3}^{k} \sqrt{\rho_{\mathbf{w}_j}/n}\right) && (\ell^2\text{-}\ell^\infty \text{ interpolation}) \\
&\leqslant n^{-(k-2)/2} \cdot \left(\sum_{w\in W} \sqrt{\rho_w}\right)^2 \cdot \left(\sum_{w\in W} \sqrt{\rho_w}\right)^{k-2} \\
&\qquad \text{(by Cauchy-Schwarz on } j = 1, 2 \text{ product part, followed by Parseval's itentity)} \\
&\ll_k n^{-(k-2)/2} n^{k/4} && \text{(by standard Gaussian upper bound } \textstyle\sum_{w\in W} \sqrt{\rho_w} \ll n^{1/4}) \\
&= n^{-k/4+1}.
\end{aligned}
$$

Therefore, their insecurity $\to 0$ only for $k \geqslant 5$.

Connection with code repair literature. A similar challenge arises in the code-repair literature [GW16], a conceptual dual in which one seeks to reconstruct a secret from small pieces of information across many shares, whereas here we aim to ensure that such distributed leakage remains uninformative (see also [CT22a, Section 6]). Non-linear repair strategies have only recently emerged there and remain technically challenging to design and analyze [CT22b, CT22a, CSTW24], foreshadowing the difficulty of our research questions.

K Collection of Useful Figures

K.1 Comparison of our Proxy

The triangle inequality proxy is defined as follows:

$$
\text{Triangle proxy:} \qquad T_k := \sum_{\mathbf{w}\in W^k} \sum_{t\neq 0} \prod_{j=1}^{k} \left|\widehat{S_{\mathbf{w}_j}(t)}\right|. \tag{28}
$$

We know that $E_k(s) \leqslant T_k$. However, it is unclear how our proxy F_{k-1} compares to T_k. Figure 1 illustrates this comparison.

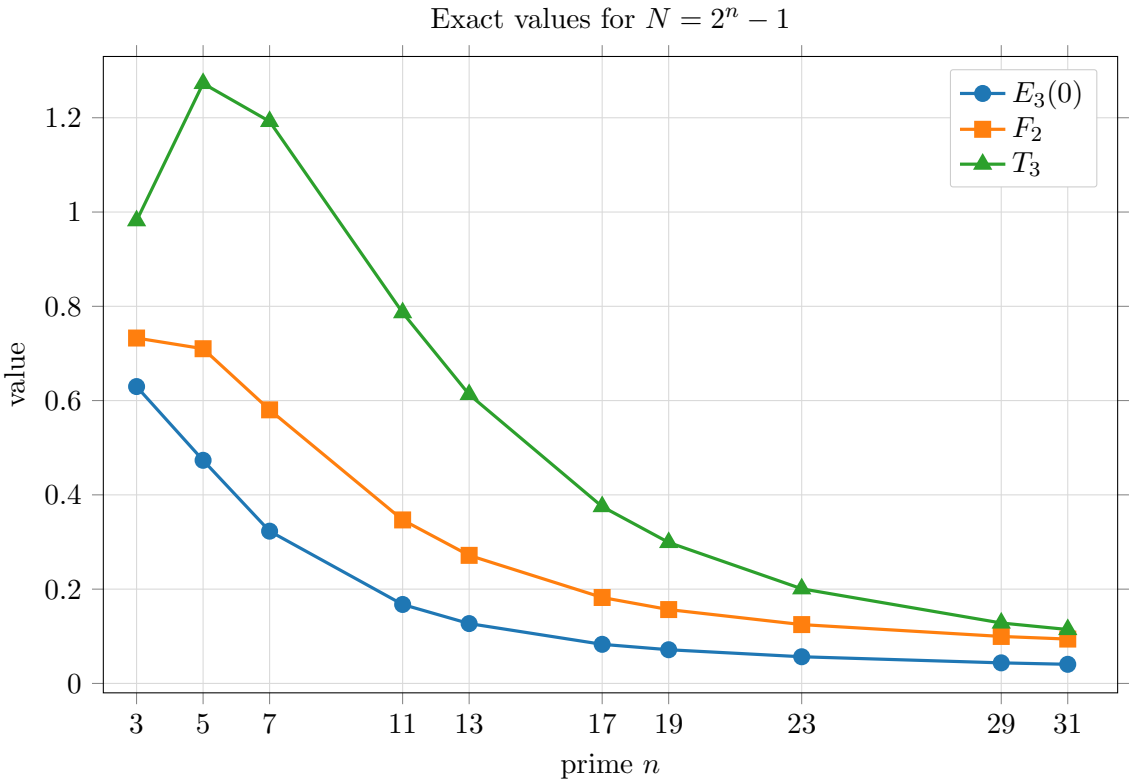


Figure 1: Comparison of $E_3(0)$, F_2, and T_3 for primes $3 \leqslant n < 32$ and $N = 2^n - 1$.

K.2 Comparison of $\sum_{w \in W} \left|\widehat{S_w}(1)\right|$ and $\sum_{w \in W} \left|\widehat{S_w}(3)\right|$

Define

$$A \coloneqq \sum_{w \in W} \left|\widehat{S_w}(1)\right| \qquad\qquad B \coloneqq \sum_{w \in W} \left|\widehat{S_w}(3)\right|$$

Figure 2 plots the ratio of B/A for moduli $N = 2^n - 1$, and prime $n \leqslant 31$. It illustrates that the ratio does not decay as n grows, it tends to a constant, remaining comparable.

K.3 Plot of $E_3(0)$

Experimentally, it seems that $E_3(0)$ behaves like $a \cdot n^{-1}$, where $a = \mathrm{E}\left[\,\left|\,\Psi(X, Y.Z)\,\right|\,\right]$ where X, Y, Z are i.i.d. $N(0,1)$ distributions, and $\Psi(x,y,z) = \sum_{\text{cyc}}(x^2 - 1)yz$.

Figure 3 indicates that $n \cdot E_3(0)$ is an affine function of $1/n$. For $N = 2^n - 1$ and primes $41 \leqslant n \leqslant 256$, we have the plot for $n \cdot E_3(0)$ versus $1/n$.

K.4 Upper Bound Figures

Figure 4a represents a bit-wise addition $a + b$ as an automaton that takes the incoming carry bit c, then returns the output bit o along with the outgoing carry bit c' such that $a + b + c = o + 2c'$. Figure 4b then shows the automaton that represents $a+b = g+h$ as the composition of two automata

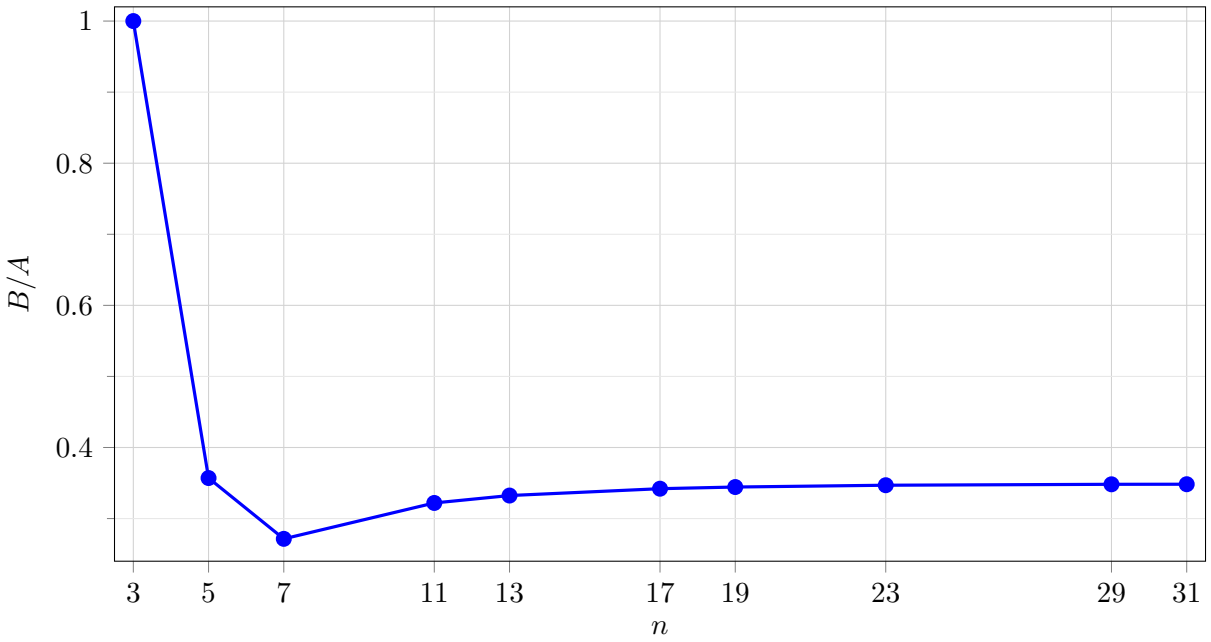


Figure 2: For $N = 2^n - 1$ and prime $3 \leqslant n \leqslant 31$, plot of $\left|\widehat{S_w}(3)\right| / \left|\widehat{S_w}(1)\right|$.

(Figure 4a), one for $a + b$ and the other for $g + h$. Figure 5 provides an example illustrating that multiplication by a power of 2 is equivalent to bitshifting.

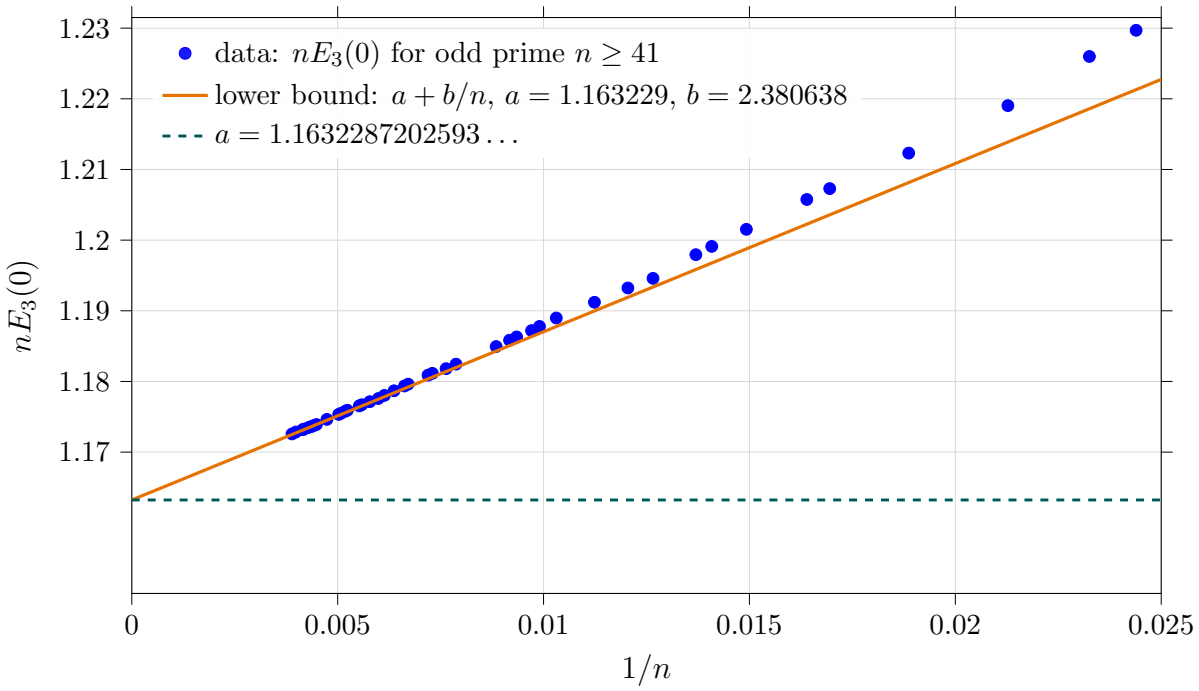
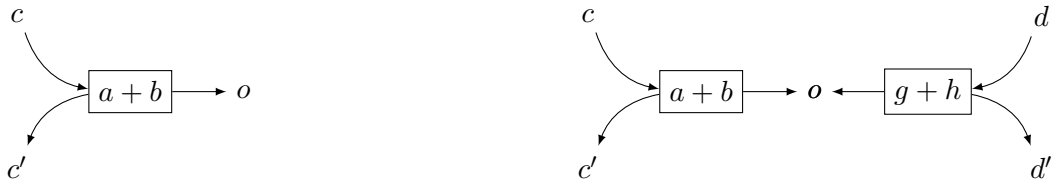


Figure 3: For $41 \leqslant n \leqslant 257$ and $N = 2^n - 1$, plots $n \cdot E_3(0)$ versus $1/n$ plot, along with an asymptotic lower bound line.



(a) Bitwise addition as an automaton

(b) Composition of two automata

Figure 4: Carry automata

$$0.001011\ldots \xrightarrow{\times 8} \square\square\square.011\ldots$$

Figure 5: Bernoulli shift (multiplication by a power of 2) as a bitshift

References

[AB14] Noga Alon and Jean Bourgain. Additive patterns in multiplicative subgroups. *Geometric and Functional Analysis*, 24(3):721–739, 2014. 3

[ADEN21] Mark Abspoel, Anders P. K. Dalskov, Daniel Escudero, and Ariel Nof. An efficient passive-to-active compiler for honest-majority MPC over rings. In Kazue Sako and Nils Ole Tippenhauer, editors, *ACNS 2021: 19th International Conference on Applied Cryptography and Network Security, Part II*, volume 12727 of *Lecture Notes in Computer Science*, pages 122–152, Kamakura, Japan, June 21–24, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-78375-4_6. 43

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 510–539, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Cham, Switzerland. doi:10.1007/978-3-030-26951-7_18. 44

[BBM+21] Alexander R. Block, Simina Brânzei, Hemanta K. Maji, Himanshi K. Mehta, Tamalika Mukherjee, and Hai H. Nguyen. P_4-free partition and cover numbers & applications. In Stefano Tessaro, editor, *ITC 2021: 2nd Conference on Information-Theoretic Cryptography*, volume 199 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:25, Seattle, WA, USA, July 23–26, 2021. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITC.2021.16. 38

[BCO04] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29, Cambridge, Massachusetts, USA, August 11–13, 2004. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-540-28632-5_2. 1, 43

[BDIR18] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 531–561, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Cham, Switzerland. doi:10.1007/978-3-319-96884-1_18. 1, 5, 15, 44

[BDIR21] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34(2):10, April 2021. doi:10.1007/s00145-021-09375-2. 1, 5, 15, 44

[BDOZ11] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic encryption and multiparty computation. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 169–188, Tallinn, Estonia, May 15–19, 2011. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-20465-4_11. 43

[BGW88] M BenOr, S Goldwasser, and A Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *Proceedings of the 20th Annual Symposium on the Theory of Computing (STOC'88)*, pages 1–10, 1988. 43

[BHMY25] Aniruddha Biswas, Jihun Hwang, Hemanta K. Maji, and Xiuyu Ye. Resilience of inner-product masking scheme against hamming weight leakage, October 2025. Available at https://www.cs.purdue.edu/homes/hmaji/papers/BHMY25.pdf. 18, 30

[BIS19] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 387–416, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Cham, Switzerland. doi:10.1007/978-3-030-26951-7_14. 44

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of AFIPS 1979 National Computer Conference*, 48:313–317, 1979. 1

[BMV19] Luís T. A. N. Brandão, Nicky Mouha, and Apostol Vassilev. NIST IR 8214: Threshold schemes for cryptographic primitives: Challenges and opportunities in standardization and validation of threshold cryptography. Technical Report NIST IR 8214, National Institute of Standards and Technology, 2019. doi:10.6028/NIST.IR.8214. 1

[BP94] Abraham Berman and Robert J Plemmons. *Nonnegative Matrices in the Mathematical Sciences*, volume 9 of *Classics in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1994. 25

[BP26] Luís T. A. N. Brandão and Rene Peralta. NIST IR 8214C: Nist first call for multiparty threshold schemes. Technical Report NIST IR 8214C, National Institute of Standards and Technology, 2026. doi:10.6028/NIST.IR.8214C. 1

[BPRW16] Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, and Daniel Wichs. Essentially optimal robust secret sharing with maximal corruptions. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 58–86, Vienna, Austria, May 8–12, 2016. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-49890-3_3. 44

[BS19] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 593–622, Darmstadt, Germany, May 19–23, 2019. Springer, Cham, Switzerland. doi:10.1007/978-3-030-17653-2_20. 44

[CDE+18] Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing. SPD $\mathbb{Z}_{2^k}$: Efficient MPC mod 2^k for dishonest majority. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 769–798, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Cham, Switzerland. doi:10.1007/978-3-319-96881-0_26. 43

[CDN01] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. Multiparty computation from threshold homomorphic encryption. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 280–299, Innsbruck, Austria, May 6–10, 2001. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-44987-6_18. 43

[CG00] Jean-Sébastien Coron and Louis Goubin. On Boolean and arithmetic masking against differential power analysis. In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2000*, volume 1965 of *Lecture Notes in Computer Science*, pages 231–237, Worcester, Massachusetts, USA, August 17–18, 2000. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-44499-8_18. 43

[CGC+21] Wei Cheng, Sylvain Guilley, Claude Carlet, Jean-Luc Danger, and Sihem Mesnager. Information leakages in code-based masking: A unified quantification approach. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(3):465–495, 2021. URL: https://tches.iacr.org/index.php/TCHES/article/view/8983, doi:10.46586/tches.v2021.i3.465-495. 43

[CGG+20] Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1226–1242. IEEE, 2020. 44

[CGMZ22] Jean-Sébastien Coron, François Gérard, Simon Montoya, and Rina Zeitoun. High-order table-based conversion algorithms and masking lattice-based encryption. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(2):1–40, 2022. doi:10.46586/tches.v2022.i2.1-40. 43

[CGTV15] Jean-Sébastien Coron, Johann Großschädl, Mehdi Tibouchi, and Praveen Kumar Vadnala. Conversion from arithmetic to Boolean masking with logarithmic complexity. In Gregor Leander, editor, *Fast Software Encryption – FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 130–149, Istanbul, Turkey, March 8–11, 2015. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-48116-5_7. 43

[CGV14] Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala. Secure conversion between Boolean and arithmetic masking of any order. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems – CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 188–205, Busan, South Korea, September 23–26, 2014. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-44709-3_11. 43

[CGZ20] Jean-Sébastien Coron, Aurélien Greuet, and Rina Zeitoun. Side-channel masking with pseudo-random generator. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 342–375, Zagreb, Croatia, May 10–14, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-45727-3_12. 43

[CKOS22] Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Short leakage resilient and non-malleable secret sharing schemes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology –*

CRYPTO 2022, Part I, volume 13507 of *Lecture Notes in Computer Science*, pages 178–207, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-15802-5_7. 44

[Cor17] Jean-Sébastien Coron. High-order conversion from Boolean to arithmetic masking. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, volume 10529 of *Lecture Notes in Computer Science*, pages 93–114, Taipei, Taiwan, September 25–28, 2017. Springer, Cham, Switzerland. doi:10.1007/978-3-319-66787-4_5. 43

[CPRR14] Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Higher-order side channel security and mask refreshing. In Shiho Moriai, editor, *Fast Software Encryption – FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 410–424, Singapore, March 11–13, 2014. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-43933-3_21. 43

[CSTW24] Roni Con, Noah Shutty, Itzhak Tamo, and Mary Wootters. Repairing reed-solomon codes over prime fields via exponential sums. *IEEE Transactions on Information Theory*, 70(12):8587–8594, 2024. 44

[CT22a] Roni Con and Itzhak Tamo. Nonlinear repair of reed-solomon codes. *IEEE Transactions on Information Theory*, 68(8):5165–5177, 2022. 44

[CT22b] Roni Con and Itzhak Tamo. Nonlinear repair schemes of reed-solomon codes. In Mark Braverman, editor, *ITCS 2022: 13th Innovations in Theoretical Computer Science Conference*, volume 215, pages 50:1–50:1, Berkeley, CA, USA, January 31 – February 3, 2022. Leibniz International Proceedings in Informatics (LIPIcs). doi:10.4230/LIPIcs.ITCS.2022.50. 44

[DDF14] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440, Copenhagen, Denmark, May 11–15, 2014. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-55220-5_24. 1

[DEF+19] Ivan Damgård, Daniel Escudero, Tore Kasper Frederiksen, Marcel Keller, Peter Scholl, and Nikolaj Volgushev. New primitives for actively-secure MPC over rings with applications to private machine learning. In *2019 IEEE Symposium on Security and Privacy*, pages 1102–1120, San Francisco, CA, USA, May 19–23, 2019. IEEE Computer Society Press. doi:10.1109/SP.2019.00078. 43

[Des88] Yvo Desmedt. Society and group oriented cryptography: A new concept. In Carl Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 120–127, Santa Barbara, CA, USA, August 16–20, 1988. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-48184-2_8. 43

[DF92] Yvo Desmedt and Yair Frankel. Shared generation of authenticators and signatures (extended abstract). In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469,

Santa Barbara, CA, USA, August 11–15, 1992. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-46766-1_37. 43

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th Annual Symposium on Foundations of Computer Science*, pages 293–302, Philadelphia, PA, USA, October 25–28, 2008. IEEE Computer Society Press. doi:10.1109/FOCS.2008.56. 44

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 643–662, Santa Barbara, CA, USA, August 19–23, 2012. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_38. 43

[FMM+24] Sebastian Faust, Loïc Masure, Elena Micheli, Maximilian Orlt, and François-Xavier Standaert. Connecting leakage-resilient secret sharing to practice: Scaling trends and physical dependencies of prime field masking. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 316–344, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58737-5_12. 2, 3, 5, 44

[FRR+14] Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from computationally bounded and noisy leakage. *SIAM Journal on Computing*, 43(5):1564–1614, 2014. 44

[FY19] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 472–499, Darmstadt, Germany, May 19–23, 2019. Springer, Cham, Switzerland. doi:10.1007/978-3-030-17659-4_16. 44

[FY20] Serge Fehr and Chen Yuan. Robust secret sharing with almost optimal share size and security against rushing adversaries. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020: 18th Theory of Cryptography Conference, Part III*, volume 12552 of *Lecture Notes in Computer Science*, pages 470–498, Durham, NC, USA, November 16–19, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-64381-2_17. 44

[GBTP08] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442, Washington, DC, USA, August 10–13, 2008. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-540-85053-3_27. 1

[Gel68] A Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arithmetica*, 13(3):259–265, 1968. 3

[GIM+16] Vipul Goyal, Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Alexander A. Sherstov. Bounded-communication leakage resilience via parity-resilient circuits. In Irit Dinur, editor, *57th Annual Symposium on Foundations of Computer Science*, pages 1–10,

New Brunswick, NJ, USA, October 9–11, 2016. IEEE Computer Society Press. doi:10.1109/FOCS.2016.10. 44

[GIW17] Daniel Genkin, Yuval Ishai, and Mor Weiss. How to construct a leakage-resilient (stateless) trusted party. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part II*, volume 10678 of *Lecture Notes in Computer Science*, pages 209–244, Baltimore, MD, USA, November 12–15, 2017. Springer, Cham, Switzerland. doi:10.1007/978-3-319-70503-3_7. 44

[GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th Annual ACM Symposium on Theory of Computing*, pages 685–698, Los Angeles, CA, USA, June 25–29, 2018. ACM Press. doi:10.1145/3188745.3188872. 44

[GM11] Louis Goubin and Ange Martinelli. Protecting AES with Shamir's secret sharing scheme. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 79–94, Nara, Japan, September 28 – October 1, 2011. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-23951-9_6. 43

[GMK16] Hannes Gross, Stefan Mangard, and Thomas Korak. Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. In *Proceedings of the 2016 ACM Workshop on Theory of Implementation Security*, TIS '16, page 3, New York, NY, USA, 2016. Association for Computing Machinery. doi:10.1145/2996366.2996426. 43

[GR15] Shafi Goldwasser and Guy N Rothblum. How to compute in the presence of leakage. *SIAM Journal on Computing*, 44(5):1480–1549, 2015. 44

[GW16] Venkatesan Guruswami and Mary Wootters. Repairing reed-solomon codes. In Daniel Wichs and Yishay Mansour, editors, *48th Annual ACM Symposium on Theory of Computing*, pages 216–226, Cambridge, MA, USA, June 18–21, 2016. ACM Press. doi:10.1145/2897518.2897525. 44

[HMNY25] Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye. Leakage-resilience of shamir's secret sharing: Identifying secure evaluation places. In Niv Gilboa, editor, *ITC 2025: 6th Conference on Information-Theoretic Cryptography*, volume 343 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:20, Santa Barbara, CA, USA, August 16–17, 2025. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITC.2025.3. 44

[HVW20] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. The price of active security in cryptographic protocols. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 184–215, Zagreb, Croatia, May 10–14, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-45724-2_7. 44

[IK21] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2021. 4

[IS24] Yuval Ishai and Yifan Song. Leakage-tolerant circuits. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 196–225, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58737-5_8. 44

[IS25] Yuval Ishai and Yifan Song. Protecting computations against continuous bounded-communication leakage. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1887–1897, 2025. 44

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481, Santa Barbara, CA, USA, August 17–21, 2003. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-540-45146-4_27. 1, 43, 44

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397, Santa Barbara, CA, USA, August 15–19, 1999. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-48405-1_25. 1, 43

[KK23] Ohad Klein and Ilan Komargodski. New bounds on the local leakage resilience of Shamir's secret sharing scheme. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023, Part I*, volume 14081 of *Lecture Notes in Computer Science*, pages 139–170, Santa Barbara, CA, USA, August 20–24, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-38557-5_5. 44

[KMS19] Ashutosh Kumar, Raghu Meka, and Amit Sahai. Leakage-resilient secret sharing against colluding parties. In David Zuckerman, editor, *60th Annual Symposium on Foundations of Computer Science*, pages 636–660, Baltimore, MD, USA, November 9–12, 2019. IEEE Computer Society Press. doi:10.1109/FOCS.2019.00045. 44

[Koc96] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO'96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113, Santa Barbara, CA, USA, August 18–22, 1996. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-68697-5_9. 1, 43

[KR19] Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. 2019. 44

[KS99] Sergei V. Konyagin and Igor E. Shparlinski. *Character sums with exponential functions and their applications*, volume 136 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1999. doi:10.1017/CBO9780511542930. 3

[Mes00] Thomas S. Messerges. Using second-order power analysis to attack DPA resistant software. In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2000*, volume 1965 of *Lecture Notes in Computer Science*, pages 238–251, Worcester, Massachusetts, USA, August 17–18, 2000. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-44499-8_19. 1, 43

[MNP+21] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Leakage-resilience of the Shamir secret-sharing scheme against physical-bit leakages. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 344–374, Zagreb, Croatia, October 17–21, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-77886-6_12. 13, 44

[MNP+22a] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu. Leakage-resilient linear secret-sharing against arbitrary bounded-size leakage family. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022: 20th Theory of Cryptography Conference, Part I*, volume 13747 of *Lecture Notes in Computer Science*, pages 355–383, Chicago, IL, USA, November 7–10, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-22318-1_13. 44

[MNP+22b] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu. Tight estimate of the local leakage resilience of the additive secret-sharing scheme & its consequences. In Dana Dachman-Soled, editor, *ITC 2022: 3rd Conference on Information-Theoretic Cryptography*, volume 230 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:19, Cambridge, MA, USA, July 5–7, 2022. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITC.2022.16. 44

[MNPCW22] Hemanta K Maji, Hai H Nguyen, Anat Paskin-Cherniavsky, and Mingyuan Wang. Improved bound on the local leakage-resilience of shamir's secret sharing. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 2678–2683. IEEE, 2022. 44

[MNPY24] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Constructing leakage-resilient Shamir's secret sharing: Over composite order fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 286–315, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58737-5_11. 44

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007. 43

[MPSW21] Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 779–808, Virtual Event, August 16–20, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-84252-9_26. 44

[MR04] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296, Cambridge, MA, USA, February 19–21, 2004. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-540-24638-1_16. 44

[MR09] Christian Mauduit and Joel Rivat. La somme des chiffres des carrés. *Acta Mathematica*, 203(1):107–148, 2009. 3

[MS97] Christian Mauduit and András Sárközy. On the arithmetic structure of the integers whose sum of digits is fixed. *Acta Arithmetica*, 81(2):145–173, 1997. 3

[MSV20] Pasin Manurangsi, Akshayaram Srinivasan, and Prashant Nalini Vasudevan. Nearly optimal robust secret sharing against rushing adversaries. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 156–185, Santa Barbara, CA, USA, August 17–21, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-56877-1_6. 44

[MV13] Eric Miles and Emanuele Viola. Shielding circuits with groups. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th Annual ACM Symposium on Theory of Computing*, pages 251–260, Palo Alto, CA, USA, June 1–4, 2013. ACM Press. doi:10.1145/2488608.2488640. 44

[Ngu25] Hai H. Nguyen. Physical-bit leakage resilience of linear code-based secret sharing. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology – EUROCRYPT 2025, Part VIII*, volume 15608 of *Lecture Notes in Computer Science*, pages 64–93, Madrid, Spain, May 4–8, 2025. Springer, Cham, Switzerland. doi:10.1007/978-3-031-91101-9_3. 44

[NIS26] National Institute of Standards and Technology, NIST. Masked circuits for block ciphers. https://csrc.nist.gov/projects/masked-circuits, 2026. Project page, accessed March 28, 2026. 1

[NRR06] Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold implementations against side-channel attacks and glitches. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *ICICS 06: 8th International Conference on Information and Communication Security*, volume 4307 of *Lecture Notes in Computer Science*, pages 529–545, Raleigh, NC, USA, December 4–7, 2006. Springer Berlin Heidelberg, Germany. doi:10.1007/11935308_38. 1, 43

[NRS11] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *Journal of Cryptology*, 24(2):292–321, April 2011. doi:10.1007/s00145-010-9085-7. 1, 43

[PR13] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159, Athens, Greece, May 26–30, 2013. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-38348-9_9. 44

[Rot12] Guy N. Rothblum. How to compute under AC^0 leakage without secure hardware. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 552–569, Santa Barbara, CA, USA, August 19–23, 2012. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-32009-5_32. 44

[Sha79] Adi Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979. doi:10.1145/359168.359176. 1, 43

[Sho00] Victor Shoup. Practical threshold signatures. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 207–220, Bruges, Belgium, May 14–18, 2000. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-45539-6_15. 43

[SMY09] François-Xavier Standaert, Tal Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In Antoine Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461, Cologne, Germany, April 26–30, 2009. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-01001-9_26. 1

[SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 480–509, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Cham, Switzerland. doi:10.1007/978-3-030-26951-7_17. 44

[TV06] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006. URL: https://proxy.library.spbu.ru:2060/10.1017/CBO9780511755149, doi:10.1017/CBO9780511755149. 3

[Yat90] Samuel Yates. *Digital Sum Sets*, pages 627–634. De Gruyter, Berlin, Boston, 1990. URL: https://doi.org/10.1515/9783110848632-045 [cited 2026-04-01], doi:doi:10.1515/9783110848632-045. 2