Resilience of Inner-Product Masking Scheme against Hamming Weight Leakage

Aniruddha Biswas
Department of Computer Science, Purdue University, USA

Jihun Hwang
Department of Computer Science, Purdue University, USA

Hemanta K. Maji
Department of Computer Science, Purdue University, USA

Xiuyu Ye
Department of Computer Science, Purdue University, USA

Abstract

Additive masking is a widely used countermeasure against side-channel attacks in which a secret is additively split into multiple random shares. However, over binary fields, the number of 1's in the binary representation (i.e., the Hamming weight) of the shares reveals information about the original secret. Inner-product masking scheme has been proposed as a promising alternative that is secure against such information leakage.

In this work, we establish that inner-product masking over a binary extension field is provably secure against Hamming weight leakage, and it translates into security against arbitrary symmetric function leakage from the shares. In addition, we present an efficiently computable score function that quantifies its security against leakages, enabling users to test and certify its security. Finally, we derive a relationship between the leakage resilience of inner-product masking and additive masking over arbitrary fields; roughly speaking, they are at least as secure as additive masking. Our approach is Fourier-analytic and involves estimating spectral norms of the Hamming slice by studying Krawtchouk polynomials.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives; Security and privacy → Cryptanalysis and other attacks

Keywords and phrases Local leakage resilience, additive masking, inner product masking, Hamming weight leakage, Fourier analysis, Krawtchouk polynomials.

Digital Object Identifier 10.4230/LIPIcs.ITC.2026.9

Related Version This is the full version of the paper that appeared in ITC 2026.

Funding *Hemanta K. Maji*: Partly supported by CNS–2055605 and CCF–2327981

Acknowledgements Authors thank Yuval Filmus for discussions on the Krawtchouk polynomial.

Contents

1 Introduction

Side-channel attacks have repeatedly compromised cryptographic secrets by exploiting observable side effects of a device's physical operation. *Masking* [12,24] is a widely prevalent and effective countermeasure; it splits the secret into shares, relying on the noise in measurements from individual shares to accumulate quickly and obscure the secret.

Additive masking, a prominent masking strategy, splits a secret s into random $(s_1, s_2, \ldots, s_n)$ shares satisfying $s_1+s_2+\cdots+s_n = s$. The security provided by this scheme has its limitations; even with noisy measurements, a carefully chosen attack can still reveal partial information about the secret. For example, over any finite field, single-bit probes into the devices storing the shares reveal information about the secret [1,38,39,41]. *Over binary extension fields, even power analysis and timing attacks* [33,34] *that reveal only the number of set bits of shares (a.k.a., their Hamming weight) compromise this masking – the secret's Hamming weight and the sum of all the leaked Hamming weights always have the same parity.* However, over exceptionally specialized and rare Mersenne-prime fields, weak security guarantees are known against such attacks [20].

In comparison, *inner-product masking* [3,4], a mild generalization of additive masking, has demonstrated significant potential for achieving greater security across all finite fields. Such a scheme is parameterized by its *reconstruction multipliers* $\vec{\beta} \in (F^*)^n$, where F is the ambient finite field, and the corresponding shares $(s_1, s_2, \ldots, s_n)$ satisfy $\beta_1 \cdot s_1 + \beta_2 \cdot s_2 + \cdots + \beta_n \cdot s_n = s$. Observe that $\vec{\beta} = (1, 1, \ldots, 1)$ reduces it to additive masking; however, carefully selecting these multipliers $\vec{\beta}$ can significantly enhance security. For instance, over any field, nearly all multipliers $\vec{\beta}$ offer strong security guarantees when the number of set bits of each share is revealed [21]. While nearly all multipliers offer strong security, we cannot identify them, nor can we determine the level of security provided by a specific multiplier.

This work contributes to the ongoing investigations into the security of inner product masking and, by extension, provides guidelines for NIST's ongoing standardization efforts for more secure secret-sharing schemes [10].

Summary of our results. As in [20, 21], we investigate the *local leakage resilience* [6, 7] of inner-product masking against *Hamming weight leakage* from shares, where the number of set bits in each share is revealed. This is a strong security metric, requiring statistical independence between the secret and the leakage, and it implies other security metrics in the literature, such as statistical bias [16], mutual information [22], and guessing entropy [52].

In this work, we establish that inner-product masking is *always* as secure as additive masking over any field, thereby ruling out the possibility of "vulnerable" multipliers that could undermine security – a gap left open in the analysis of [21]. Over binary extension fields, while additive masking is vulnerable, as indicated above, we prove that it is (essentially) the *only* vulnerable scheme; all other inner product masking schemes are secure. We present an efficiently computable *score function* for multipliers, where a higher score indicates greater security of the corresponding inner-product masking. Our score function enables *certifying* the security achieved by a specific multiplier, facilitating efforts similar to those in [17–19]. It helps explicitly identify multipliers with strong security, whose existence was proven in [21]. From a randomness extractor perspective: the inner product with random (public) multipliers is already a strong extractor; our contribution is to deterministically identify multipliers that yield a good inner-product extractor.

The results above stem from more general technical findings, also applicable to the local leakage resilience of secret-sharing schemes and polynomial masking [23, 49]. Our approach is Fourier-analytic and relies on spectral-norm estimates of the Hamming slice, which, in turn, require the asymptotic properties of Krawtchouk polynomials [37, 55].

1.1 Preliminary Notations

Basic notions. Here $x = a \pm c$ denotes $x \in [a-c, a+c]$, for reals x and a with $c > 0$. $\mathrm{card}(S)$ denotes the cardinality of the set S. Let F_q denote the finite field of order (cardinality) q and $F_q^* := F_q \setminus \{0\}$. Let $\lambda \in \{1, 2, \dots\}$ satisfy $2^{\lambda-1} < q \leqslant 2^\lambda$, the number of bits needed to represent the finite field elements.

Field extensions. Elements of an extension field F_{2^λ} are represented as $F_2[Z]/\Pi(Z)$ elements, where $\Pi(Z)$ is a monic irreducible polynomial of degree λ. We can view F_{2^λ} as a vector space F_2^λ after choosing a basis $\mathcal{B} = (b_1, \dots, b_\lambda)$. The *Hamming weight* $\mathrm{wt}_\mathcal{B}(\zeta) \in \{0, 1, \dots, \lambda\}$ is the number of 1's in the vector representation of $\zeta \in F_{2^\lambda}$ in F_2^λ under $\mathcal{B}$; we omit $\mathcal{B}$ unless it has to be specified. Let $\mathsf{Tr}_{F_{2^\lambda}/F_2} \colon F_{2^\lambda} \to F_2$ be the field trace of the field extension F_{2^λ}/F_2. The *trace-dual coordinate vector* of $\zeta \in F_{2^\lambda}$ is $\zeta^\vee := (\mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_1), \dots, \mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_\lambda)) \in F_2^\lambda$ and its Hamming weight $\mathrm{wt}(\zeta^\vee) =: \mathrm{wt}^\vee(\zeta)$ is called the *trace-dual Hamming weight* of ζ.

Secret sharing and masking. Let Add_n denote the *additive secret sharing* among n parties; to share a secret $s \in F$, it provides random shares $(s_1, s_2, \dots, s_n) \in F^n$ conditioned on $s_1 + s_2 + \cdots + s_n = s$. The *generalized additive secret sharing* $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is parameterized by $\vec{\beta} = (\beta_1, \dots, \beta_n) \in (F^*)^n$ and its shares satisfy $\beta_1 \cdot s_1 + \beta_2 \cdot s_2 + \cdots + \beta_n \cdot s_n = s$ instead (β_i's need not be all distinct); the additive scheme corresponds to $\vec{\beta} = (1, \dots, 1)$. The additive and generalized additive secret sharing are equivalent to additive and inner-product masking, respectively.

Leakage resilience. Fix a secret sharing scheme $\mathcal{S}$. Let $\tau_i \colon F \to \Omega_i$ be a leakage function, and let $\vec{\tau}(s)$ denote the joint leakage distribution $(\tau_1(s_1), \dots, \tau_n(s_n))$, where $\mathcal{S}$ generates shares $(s_1, \dots, s_n)$ of s. $\vec{\tau}(U_F)$ will denote the leakage distribution when the secret is chosen uniformly at random from F.

The *local leakage resilience* of $\mathcal{S}$ against the leakage attack $\vec{\tau}$ is defined by [6, 7]:

$$\varepsilon(\mathcal{S}; \vec{\tau}) \;:=\; \max_{s \in F} \mathrm{SD}(\vec{\tau}(s)\ ,\ \vec{\tau}(U_F)) \tag{1}$$

In local leakage resilience context, the insecurity of $\mathsf{Gen}(\mathsf{Add}_n,\ (c, \dots, c)\ )$, for $c \in F^*$, is identical to the Add_n's insecurity; hence, they are *essentially equivalent*.

Our score function. Define $\sigma\colon \{0, 1, \dots, \lambda\} \to \mathbb{R}$ as follows[1]

$$\sigma(w) \;:=\; \begin{cases} 0, & \text{if } w \in \{0, \lambda\} \\ \dfrac{1}{2}\log\dbinom{\lambda}{w} - \dfrac{\log \lambda}{4}, & \text{otherwise} \end{cases}. \tag{2}$$

Note that this function can be computed efficiently [8, 11].

▶ Remark 1 (Behavior of σ). Since $\binom{\lambda}{w} \geqslant (\lambda/w)^w$, we have

$$\sigma(w) \geqslant \frac{w^*}{2} \cdot \log\left(\frac{\lambda}{w^*}\right) - \frac{1}{4} \cdot \log \lambda$$

where $w^* = \min\{w, \lambda - w\}$ and $w \in \{1, 2, \dots, \lambda - 1\}$. Consequently, either $\sigma(w) = 0$ or $\sigma(w) \geqslant (1/4) \cdot \log \lambda$.

Asymptotically, by central limit theorem, $\binom{\lambda}{\frac{\lambda}{2} \pm x}$ behaves like $\frac{2^\lambda}{\sqrt{\pi\lambda/2}} \cdot \exp\left(-\frac{2x^2}{\lambda}\right)$. So, $\sigma(\lambda/2 \pm x)$ behaves like $\frac{\log 2}{2}\lambda - \frac{1}{2}\log\lambda - \frac{x^2}{\lambda}$. When w is drawn according to the binomial distribution, the expected value of $\sigma(w)$ is roughly $\frac{\log 2}{2}\lambda$, a consequence of the entropy of the binomial distribution. △

For $\vec{\beta} \in (F^*)^n$ and $\zeta \in F$, we define $\mathsf{Score}\colon F \times (F^*)^n \to \mathbb{R}$ as follows.

$$\mathsf{Score}(\zeta; \vec{\beta}) \;:=\; \sum_{i=1}^{n} \sigma\big(\ \mathrm{wt}^\vee(\beta_i \cdot \zeta)\ \big). \tag{3}$$

Let $\zeta^* \in F$ be the unique element satisfying ${\zeta^*}^\vee = (1, \dots, 1)$, equivalently $\mathrm{wt}^\vee(\zeta^*) = \lambda$. For a tuple $\vec{\beta} = (\beta_1, \beta_2, \dots, \beta_n) \in (F^*)^n$, define

$$\mathcal{S}_{\vec{\beta}} \;:=\; \left\{\ \zeta^* \cdot \beta_1^{-1},\ \zeta^* \cdot \beta_2^{-1},\ \dots,\ \zeta^* \cdot \beta_n^{-1}\ \right\} \subseteq F^*. \tag{4}$$

Looking ahead, our security characterization will depend on the minimum 'score' $\mathsf{Score}(\zeta; \vec{\beta})$ over $\zeta \in \mathcal{S}_{\vec{\beta}}$; insecurity will be small when $\vec{\beta}$ has a *large minimum score*.

1.2 Our Results

Over binary extension fields. Over $F = F_{2^\lambda}$, the attack in the introduction demonstrates the vulnerability of additive secret sharing to Hamming weight leakage. We begin by showing that transitioning to the generalized setting eliminates this vulnerability.

Informal Theorem 1. *For $n \in \{3, 4, \dots\}$ parties, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is $\lambda^{-1/4}$-insecure, unless $\vec{\beta} = (b, b, \dots, b)$ for $b \in F^*$.*

[1] For intuition, https://www.desmos.com/calculator/zerikstukw graphs the $\sigma(\cdot)$ function for a representative λ.

Except for those inner product masking that are essentially equivalent to the additive masking in the local leakage resilience context, everyone else is secure. Theorem 1 states this result formally. Next, we characterize choices of $\vec{\beta} \in (F^*)^n$ that allow us to derive stronger security bounds for $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$, where insecurity decays $\lambda^{-\Theta(n)}$. This characterization builds on the following technical result.

Informal Theorem 2. *For $n \in \{3, 4, \dots\}$ parties and $\vec{\beta} \in (F^*)^n$, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is λ^{-cn}-insecure, where $c \in (0, 1/2 - 1/n)$ satisfies*

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}\left(\zeta; \vec{\beta}\right) \geqslant cn \cdot \log \lambda. \tag{5}$$

and the Score *function is defined in Equation 3.*

We leave the case $n = 2$ as an open problem for both results. For clarity of presentation, we ignore additive $\log \log \lambda$ terms in the right-hand side of the expression above (Equation 5). See Theorem 2 for the full expression.

Given $\vec{\beta}$, one can efficiently compute its trace-dual weights and test whether the minimum score is $\geqslant cn \log \lambda$ or not, i.e. verify Equation 5 (see for example [56]). For example, if all elements of $\vec{\beta}$ are identical, we know already that the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is insecure. In this case, the minimum score is 0 and our technical result cannot upper bound the insecurity by a small quantity.

▶ Remark 2 (Consequences of Theorem 1 and 2). The following corollaries are immediate:

1. If every element in $\vec{\beta}$ occurs at most m times, then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ satisfies Equation 5 with $c = (n - m)/4n$. This is because for $\zeta \in \mathcal{S}_{\vec{\beta}}$, $\beta_i \zeta$ is either equal to ζ^* or has dual weight $\in \{1, 2, \dots, \lambda - 1\}$.
   Since every element in $\vec{\beta}$ occurs at most m times, at least $(n-m)$ elements in $\{\zeta\beta_1, \dots, \zeta\beta_n\}$ have dual weight $\in \{1, 2, \dots, \lambda - 1\}$. Therefore, the score is $\geqslant (n-m) \cdot (1/4) \log \lambda$; whence, the result.
   In particular, if all elements of $\vec{\beta}$ are distinct, then $m = 1$ and $c = (n - 1)/4n$. Moreover, when $\vec{\beta}$ is chosen uniformly at random from F^n, then with exponentially high probability, it consists of distinct elements from F^*.
2. A *symmetric* function $f \colon F \to \Omega$ satisfies the constraint "$\mathrm{wt}(x) = \mathrm{wt}(y)$ implies $f(x) = f(y)$" for $x, y \in F$. Let $\mathcal{F}$ denote the set of all symmetric functions. A *symmetric local leakage* leaks $f_1, \dots, f_n$ from the shares $s_1, \dots, s_n$, where $f_1, \dots, f_n \in \mathcal{F}$.
   Note that given only the $\mathrm{wt}(x)$, one can compute $f(x)$ for a symmetric function; i.e., $x \to \mathrm{wt}(x) \to f(x)$ is a Markov chain. Therefore, by the data processing inequality (see [13, Chapter 2]), any secret sharing scheme that has ε insecurity against the Hamming weight leakage has ε insecurity against *every* symmetric local leakage.

△

Theorem 2 also gives a systematic way to select reconstruction multipliers $\vec{\beta} \in (F^*)^n$.

Informal Corollary 1. *Let $\vec{\beta} = (\beta_1, \dots, \beta_n) \in (F^*)^n$ If for every β_i there exists another β_j such that $\beta_j \zeta^* \beta_i^{-1}$ has non-extreme (close to neither 0 nor λ) dual Hamming weight, then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ satisfies Equation 5 for all sufficiently large λ.*

We give a concrete instantiation below, where we construct multipliers $\vec{\beta} \in (F^*)^n$ from the irreducible polynomial $\Pi(Z) \in F_2[Z]$ defining $F = F_{2^\lambda} \cong F_2[Z]/\Pi(Z)$. Since the relevant trace-dual weights may depend on $\Pi(Z)$, the choice of $\vec{\beta}$ varies with $\Pi(Z)$. More general recommendations and their proofs are available in Appendix D. In addition, Corollary 1

also allows us to extend our results to the security of Shamir's secret sharing (polynomial masking) with random evaluation points; see Remark 8.

Recommendations for $\vec{\beta}$: an illustrative example

Suppose we are given an insecurity budget of 2^{-48} and $n = 16$, a fairly reasonable expectation in practice. We make the following recommendations based on our technical findings.

1. If $\Pi(Z) = Z^\lambda + Z + 1$, choose $\vec{\beta} = (\beta, 1, \dots, 1) \in (F^*)^n$, where $\beta = Z^{\lfloor \lambda/2 \rfloor}$. For $\lambda \geqslant 256$, this gives the desired insecurity bound.
2. If $\Pi(Z) = Z^\lambda + Z^j + 1$ where $j > 1$ is a small constant, choose $\vec{\beta} = (\beta, 1, \dots, 1) \in (F^*)^n$, where $\beta = Z^i$, where i is the multiple of j closest to $\lambda/2$. Again, for $\lambda \geqslant 256$ and the usual choices of j, this gives the desired insecurity bound.
3. If $\Pi(Z) = Z^\lambda + Z^j + 1$ where j is already comparable to $\lambda/2$, choose $\vec{\beta} = (\beta, 1, \dots, 1) \in (F^*)^n$, where $\beta = Z^j$. This is the simplest choice in the large-j trinomial case.

Over arbitrary fields. Next, we show that generalized additive secret sharing inherits its security from the additive secret sharing, and is therefore *at least as secure as* the additive secret sharing, in the sense that its insecurity is bounded above by a quantity that upper bounds the insecurity of additive secret sharing.

Informal Theorem 3. *Let F_q be a finite field of order q and $\vec{\beta} \in (F_q^*)^n$. Then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is secure against the leakage $\vec{\tau} = (\tau_1, \tau_2, \dots, \tau_n)$ if Add_n is "sufficiently secure" on average over $i \in \{1, 2, \dots, n\}$ against $\vec{\tau_i} = (\tau_i, \tau_i, \dots, \tau_i)$.*

This result implies that one could verify the security of a generalized additive secret sharing against a certain leakage, by testing whether the additive secret sharing (i.e. when all reconstruction multipliers are 1) is *sufficiently secure* against leakage attacks where the same leakage function is applied to every share. Here, the notion of strong security comes from the fact that we need the upper bound of insecurity to be small, not the insecurity itself. See Theorem 3 for the precise statement with exact expressions.

It is worthwhile to note that Theorem 3 applies to *any* finite field. Consequently, we can also derive security guarantees against Hamming weight leakage for schemes over prime fields, including those based on Mersenne primes, by combining our generalized bound with the results of Faust et al. [20].

▶ Remark 3 (Technical subtlety in Theorem 3). Benhamouda et al. [6] introduced the quantity called *Fourier proxy* that measures the local leakage resilience (Equation 1). Proving that this proxy (or its upper bound) is small is a popular technique to demonstrate that the insecurity is small [6, 7, 31, 32, 38, 41, 42, 45].

In Theorem 3, we show that the proxy of the inner product masking is at most an upper bound of the proxy for additive masking, induced by triangle inequality, hence the terminology *sufficiently secure*. We *did not* prove that the insecurity of the inner product masking is at most the insecurity of the additive scheme directly. △

1.3 Technical Overview

Our results are best interpreted by considering the number of parties $n \in \{3, 4, \dots\}$ to be a constant and determining the asymptotics of insecurity as a function of the security

parameter λ. Consider $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$, for arbitrary $\vec{\beta} \in (F^*)^n$. In this section, we illustrate our analysis strategy against the Hamming weight leakage; we present full proofs formally in Section 3.

The analysis relies on spectral-norm estimates of the Hamming slice, which in turn require the asymptotic properties of Krawtchouk polynomials [37, 55]. Existing techniques such as bounding the spectral norm of the Hamming slice via polynomial threshold function estimates, do not yield bounds sufficiently tight for our purposes. See Appendix E.1 for further discussion and Figure 1 for a visualization of the gap between spectral weights at each level. One modern tool for estimating the spectral norm of Hamming slices is the use of level-k inequalities; Appendix E.2 demonstrates why this approach is still insufficient for our purposes.

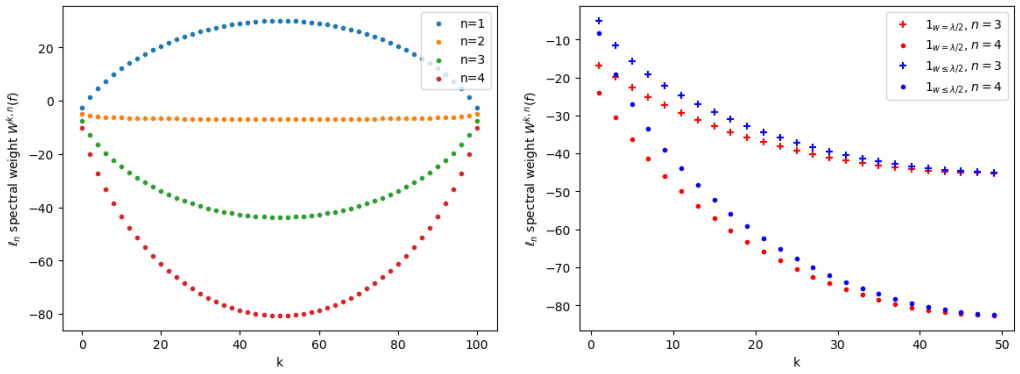

Figure 1 Distribution of ℓ_n-spectral weight at level-k of $f\colon F_{2^\lambda} \to \{0,1\}$, i.e. $W^{k,n}(f) := \sum_{S\colon \mathrm{wt}(S)=k} |\hat{f}(S)|^n$.
[Left] x-axis: $k \in \{0,1,\ldots,\lambda\}$. y-axis: $W^{k,n}(\mathbb{1}_{w=\lambda/2})$ (log-scaled) for $n=1$ (blue), 2 (orange), 3 (green), and 4 (red). Note the change in trend as n increases.
[Right] x-axis: $k \in \{0,1,\ldots,\lambda/2\}$. y-axis: log-scaled $W^{k,n}(\mathbb{1}_{w=\lambda/2})$ (red) and log-scaled $W^{k,n}(\mathbb{1}_{w\leqslant\lambda/2})$ (blue) for $n=3$ (+ markers) and 4 (• markers). Note the gap between $\mathbb{1}_{w=\lambda/2}$ (red) and log-scaled $\mathbb{1}_{w\leqslant\lambda/2}$.

Main Technical Result and Proof Outline

▶ **Theorem 1.** *For $\vec{\beta} \in (F^*)^n \setminus \{(b,\ldots,b)\colon b \in F^*\}$ and $n \in \{3,4,\ldots\}$, we have*

$$\varepsilon\Big(\ \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})\ ;\ \overrightarrow{\mathrm{wt}}\ \Big) = \mathcal{O}\Big(\lambda^{-1/4}\Big).$$

Recall that $\overrightarrow{\mathrm{wt}}(s)$, represents the Hamming weight leakage distribution over the sample space $\{0,1,\ldots,\lambda\}^n$ corresponding to a secret $s \in F$. Similarly, $\overrightarrow{\mathrm{wt}}(U_F)$ represents the joint Hamming weight distribution when the secret is randomly picked from F. We aim to upper-bound the statistical distance between these two probability distributions.

$$2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big)$$
$$= \sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$

Here, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)$ denotes the distribution of shares over F^n for secret $s \in F$, and $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)$ the distribution of shares for a uniformly random secret in F. Note that

each share s_i is uniformly random over F, irrespective of the secret. Therefore, the (marginal) distribution of the Hamming weight of any share is the binomial distribution $B(\lambda, 1/2)$. By Chernoff bound (Lemma 1), it is unlikely that the Hamming weight of any share is significantly far from $\lambda/2$. In particular, for a parameter $\tau \in (0, 1/2]$, the Hamming weight of a share being $\geqslant \lambda^{1/2+\tau}$ far from $\lambda/2$, is at most $2 \cdot \exp(-2\lambda^{2\tau})$. We can control this probability of "atypical weights" by setting $\tau = \frac{\log((n/4)\cdot\log\lambda)}{2\log\lambda}$ and driving the probability below $\lambda^{-n/2}$.

We define the set of all *typical* leakages $\mathsf{Typical}(n,\tau) \subseteq \{0,1,\ldots,\lambda\}^n$ parameterized by τ:

$$\mathsf{Typical}(n,\tau) \;:=\; \Big\{\vec{w} :\; |w_i - \lambda/2| \leqslant \lambda^{1/2+\tau},\ \text{for all } i \in \{1,2,\ldots,n\}\Big\}. \tag{6}$$

The probability that the Hamming weight leakage of any share for secret s or random secret U_F is outside this $\mathsf{Typical}(n,\tau)$ set is (at most) $4n \cdot \exp\big(-2\lambda^{2\tau}\big)$ by the union bound. So, we conclude that

$$\begin{aligned} &2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\ &\quad= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right| \\ &\qquad\qquad \pm\, 4n \cdot \lambda^{-n/2}. \end{aligned}$$

and therefore it suffices to estimate the leakage probability restricted to typical leakages $\vec{w} \in \mathsf{Typical}(n,\tau)$.

To this end, we will use Fourier analysis. Using the Poisson summation formula (Lemma 2) for the generalized additive secret sharing, we can rewrite the right-hand side expression in terms of Fourier coefficients.

$$\begin{aligned} &2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\ &\quad= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \sum_{\zeta\in F^*} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta) \right) \cdot \chi_1\Big(s\cdot\zeta\cdot\Big\langle\vec{\beta},\vec{v}\Big\rangle\Big) \right| \;\pm 4n\cdot\lambda^{-n/2}. \end{aligned}$$

Here, $\mathbb{1}_w \colon F \to \{0,1\}$ is the indicator function of the set all elements in F with Hamming weight $w \in \{0,1,\ldots,\lambda\}$. The shares $\vec{v} \in F^n$ is an arbitrary share of the secret $1 \in F$. Moreover, $\chi_1 \colon F \to \mathbb{C}$ is defined as $\chi_1(x) := (-1)^{\mathsf{Tr}_{F/F_2}(x)}$ (see Section 2.4 for details). To upper-bound the right-hand side expression, we apply the triangle inequality and conclude:

$$2 \;\cdot\; \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \leqslant \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \sum_{\zeta\in F^*} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \;+ 4n\cdot\lambda^{-n/2}.$$

Now, we need to upper-bound the magnitude of $\widehat{\mathbb{1}}_w(\cdot)$, for typical $w \in \{0,1,\ldots,\lambda\}$. We remind the reader that the right-hand side expression is not small for every $\vec{\beta} \in F^n$. For instance, when $\vec{\beta} = \vec{1} = (1,1,\ldots,1) \in F^n$ we know an attack on the corresponding secret sharing scheme. Thus, the resulting secret sharing scheme must be insecure and the right-hand side expression corresponding to that insecure scheme must be large. So, the right-hand side estimate will be small depending on $\vec{\beta}$; our analysis cannot be transparent to this fact.

To approach this estimation problem, and appreciate our key technical components, let us build some elementary intuition of the magnitude of the Fourier coefficients $\widehat{\mathbb{1}}_w(\cdot)$. We remark that $\widehat{\mathbb{1}}_w(x) = 2^{-\lambda} K_w(\mathrm{wt}^\vee(x))$ where $K_w(\cdot)$ is a Krawtchouk polynomial, as defined in [36]. Krawtchouk polynomials find extensive applications in many subfields in mathematics, theoretical computer science, and cryptography; see, for example, [55].

1. First, by symmetry $\widehat{\mathbb{1}}_w(x) = \widehat{\mathbb{1}}_w(y)$, for all $x, y \in F$ satisfying $\mathrm{wt}^\vee(x) = \mathrm{wt}^\vee(y)$.
2. Next, $\widehat{\mathbb{1}}_w(x) = (-1)^w \cdot \widehat{\mathbb{1}}_w(y)$, for all $x, y \in F$ satisfying $\mathrm{wt}^\vee(x) + \mathrm{wt}^\vee(y) = \lambda$, because $\mathbb{1}_w$ is a real-valued function.

As we will see, the contributions of $\widehat{\mathbb{1}}_w(x)$, where $\mathrm{wt}^\vee(x) \in \{1, 2, \ldots, \lambda-1\}$, is relatively small; *this fact is non-trivial to prove and is one of our technical contributions.* The contributions of $\widehat{\mathbb{1}}_w(0)$ and $\widehat{\mathbb{1}}_w(\zeta^*)$, where $\zeta^* \in F$ is the unique element of F with $\mathrm{wt}^\vee(\zeta^*) = \lambda$, are large. Both of them have magnitude equal to the density of the subset of all weight-w elements of F. However, note that $\widehat{\mathbb{1}}_w(0)$ never occurs on the right-hand side expression, because the right-hand side expression only considers $\zeta \in F^*$ and all β_i are also non-zero. The potential "troublemakers" are those terms where $\widehat{\mathbb{1}}_w(\zeta^*)$ appears.

To account for them, we identify the set of candidate $\zeta \in F$ such that $\zeta \cdot \beta_i = \zeta^*$ for some $i \in \{1, 2, \ldots, n\}$.

$$\mathcal{S}_{\vec{\beta}} := \left\{\zeta^* \cdot \beta_1^{-1},\ \zeta^* \cdot \beta_2^{-1},\ \ldots,\ \zeta^* \cdot \beta_n^{-1}\right\}.$$

Note that the cardinality of $\mathcal{S}_{\vec{\beta}}$ is the number of distinct elements in $\vec{\beta}$, which is at most n. We split the right-hand side expression depending on whether $\zeta \in \mathcal{S}_{\vec{\beta}}$ or not, then we estimate them separately:

$$2 \cdot \mathrm{SD}\left(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\right) \leqslant \underbrace{\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|}_{\text{first summand}} + \underbrace{\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|}_{\text{second summand}} + 4n \cdot \lambda^{-n/2}.$$

Second summand estimation. We prove an upper bound on the magnitude $|\widehat{\mathbb{1}}_{w_i}(x)| \leqslant B(x)$ as defined in Lemma 4, for all $x \in F \setminus \{0, \zeta^*\}$. Using this bound, we have:

$$\begin{aligned}\text{second summand} &\leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta) \\ &= \left(2\lambda^{1/2+\tau}\right)^n \cdot \left(\sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta)\right).\end{aligned}$$

The last equality substitutes the cardinality of the $\mathsf{Typical}(n, \tau)$ set. Now, using (generalized) Hölder's inequality (Lemma 3), we have

$$\text{second summand} \leqslant \left(2\lambda^{1/2+\tau}\right)^n \cdot \left(\sum_{\zeta \in F \setminus \{0, \zeta^*\}} B(\zeta)^n\right) \tag{7}$$

We show that this n-th norm, for $n \geqslant 3$, is small. Roughly speaking, Lemma 4 upper bounds the right-hand side expression as follows:

$$\text{second summand} \leqslant \left(2\lambda^{1/2+\tau}\right)^n \cdot \lambda^{-n+1} = (2\lambda^\tau)^n \cdot \lambda^{-n/2+1}. \tag{8}$$

which is $1/\mathsf{poly}(\lambda)$ for $n \geqslant 3$; here, the exponent of the polynomial depends on n. *This result requires a tight estimate of $B(x)$ such that $\mathrm{wt}^\vee(x) = 1$, a technical contribution of our work.*

Substituting $\tau = \frac{\log\left(\frac{n}{4}\log\lambda\right)}{2\log\lambda}$, we get that $2\lambda^{\tau} = (n\log\lambda)^{1/2}$. Henceforth, we will carry this upper bound as $(n\log\lambda)^{n/2}\cdot\lambda^{-n/2+1}$.

▶ Remark 4. Determining the estimates $B(x)$ is equivalent to estimating the evaluations of Krawtchouk polynomials. We require concrete estimates, not asymptotics such as the one in [15]. Elementary estimates suffice for our applications; tighter estimates, for example, those in [36, Section 3], do not yield any qualitative improvement of our results. We present upper bounds on such estimates in Appendix C. △

▶ Remark 5 (A world without estimating the higher order spectral norm). Suppose we upper bound the second summation using prior techniques as used in [6, 7, 20, 40, 42]; they did not analyze the ℓ_n norm. They upper bound the second summand using the ℓ_∞ norm and the ℓ_2 norm of the Fourier coefficients. Using our tight estimate of $B(x) = \lambda^{-1}$, when $\mathrm{wt}^{\vee}(x) = 1$, the old strategy will yield an upper bound of $\mathsf{poly}(\log\lambda)\cdot\lambda^{-(n-2)-(1/2)+n/2}$, which will be $o(1)$ only for $n \geqslant 4$. Our upper bound is tighter; it is $o(1)$ for $n \geqslant 3$. See Appendix E.3 for details. △

First summand estimation. To summarize our derivation so far, for $n \geqslant 3$ parties, we have

$$2\cdot\mathrm{SD}\left(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\right) \leqslant \underbrace{\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\ \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\ \prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|}_{\text{first summand}} + \underbrace{\left((n\log\lambda)^{n/2}+4n/\lambda\right)\cdot\lambda^{-n/2+1}}_{\text{small}}. \tag{9}$$

Note that to upper bound the first summand it suffices to show that the following quantity is small *for every* $\zeta\in\mathcal{S}_{\vec{\beta}}$:

$$\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\ \prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|.$$

Because, if the above quantity is small, then so is the summation restricted to $\vec{w}\in\mathsf{Typical}(n,\tau)$. And, in turn, the expression in the first summand is small too, with an additional multiplicative factor of at most n (since $\mathrm{card}(\mathcal{S}_{\vec{\beta}})\leqslant n$).

To begin, for any $\zeta\in\mathcal{S}_{\vec{\beta}}$, rewrite

$$\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\ \prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \prod_{i=1}^{n}\left(\sum_{w_i\in\{0,1,\ldots,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right) \tag{10}$$

Let $H(\zeta;\vec{\beta}) := \{i\colon \beta_i\zeta\neq\zeta^*\}$. Consider an index $i\notin H(\zeta;\vec{\beta})$. For such an i, we have $\beta_i\zeta=\zeta^*$ and, consequently, $\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \left|\widehat{\mathbb{1}}_{w_i}(\zeta^*)\right| = \left|\widehat{\mathbb{1}}_{w_i}(0)\right| = \binom{\lambda}{w_i}\cdot 2^{-\lambda}$, and therefore, $\sum_{w_i}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \sum_{w_i}\binom{\lambda}{w_i}\cdot 2^{-\lambda} = 1$. As a result, the expression in Equation 10 is

$$(\text{Equation 10}) = \prod_{i\in H(\zeta;\vec{\beta})}\left(\sum_{w_i\in\{0,1,\ldots,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right)$$

If all elements in $\vec{\beta}$ are identical, then, observe that $\mathcal{S}_{\vec{\beta}}$ is a singleton set and $H(\zeta;\vec{\beta})=\emptyset$ – a lost case for us; the expression above is 1. On the other hand, if *it is not the case that all*

elements in $\vec{\beta}$ *are identical*, then $H(\zeta;\vec{\beta}) \neq \emptyset$ for every $\zeta \in \mathcal{S}_{\vec{\beta}}$. For any $i \in H(\zeta;\vec{\beta})$, it will suffice to prove that

$$\sum_{w_i \in \{0,1,\ldots,\lambda\}} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \mathcal{O}\left(\lambda^{-1/4}\right).$$

Define $\zeta' := \beta_i\zeta$. Observe that $\zeta' \in F \setminus \{0,\zeta^*\}$. A standard application of the Parseval's identity (Fact 1) yields the estimate (see Lemma 4 for details):

$$\left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| \leqslant \sqrt{\binom{\lambda}{w_i} \cdot 2^{-\lambda} \cdot \binom{\lambda}{w'}^{-1}},$$

where $w' = \mathrm{wt}^{\vee}(\zeta')$ and $w' \in \{1,2,\ldots,\lambda-1\}$. Therefore, using the fact $\binom{\lambda}{w'} \geqslant \binom{\lambda}{1} = \lambda$, we have

$$\left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| \leqslant \sqrt{\binom{\lambda}{w_i} \cdot 2^{-\lambda} \cdot \lambda^{-1}},$$

Using this upper bound on the Fourier coefficient, we have

$$\begin{aligned}\sum_{w_i \in \{0,1,\ldots,\lambda\}} \left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| &\leqslant 2^{-\lambda/2}\lambda^{-1/2} \sum_{w_i \in \{0,1,\ldots,\lambda\}} \binom{\lambda}{w_i}^{1/2} \\ &< 2^{-\lambda/2}\lambda^{-1/2} \cdot \pi 2^{\lambda/2}\lambda^{1/4} = \pi\lambda^{-1/4} \qquad \text{(by Claim 2)}\end{aligned}$$

which is what we set out to prove.

▶ Remark 6 (Perspective). Suppose $\vec{\beta}$ has $k \geqslant 2$ distinct elements $\beta_1,\beta_2,\ldots,\beta_k$ and they occur $n_1,n_2,\ldots,n_k$ times in $\vec{\beta}$, respectively. Without loss of generality, assume that $1 \leqslant n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k$. Note that $n_1+n_2+\cdots+n_k = n$ and $\mathcal{S}_{\vec{\beta}} = \{\zeta^*\beta_1^{-1},\ldots,\zeta^*\beta_k^{-1}\}$, a set of k elements. Furthermore, the set $H(\zeta^*\beta_i^{-1};\vec{\beta})$ has cardinality $(n-n_i)$, for $i \in \{1,2,\ldots,k\}$. Therefore, our upper bound calculated above will be

$$\sum_{i=1}^{k}\left(\pi \cdot \lambda^{-1/4}\right)^{n-n_i}.$$

And, this upper bound is largest (a.k.a., the weakest) when $n_1 = \cdots = n_{k-1} = 1$ and $n_k = (n-k+1)$. For this case, the upper bound becomes

$$\underbrace{\left(\pi \cdot \lambda^{-1/4}\right)^{(k-1)}}_{\text{dominant term}} + (k-1)\left(\pi \cdot \lambda^{-1/4}\right)^{n-1}$$

Overall, the worst upper bound happens where $\vec{\beta}$ has $k = 2$ distinct elements, one of them occurring once, and the other occurring $(n-1)$ times. Even in this worst case, the upper bound is $\mathcal{O}\left(\lambda^{-1/4}\right)$. △

Putting things together and concluding remarks. Substituting these estimates of the two summands, we get

$$2 \cdot \mathrm{SD}\left(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\right) \leqslant \pi\lambda^{-1/4} + \underbrace{\left((n\log\lambda)^{n/2} + 4n/\lambda\right) \cdot \lambda^{-n/2+1}}_{\text{small}}$$

The "small" quantity in the insecurity upper-bound is (roughly) $\lambda^{-n/2+1}$, which is $o(1)$, for $n \geqslant 3$. This wraps up the proof overview of Theorem 1.

Which schemes are most secure?

Theorem 1 shows that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is secure against Hamming weight leakage as long as the reconstruction multiplier $\vec{\beta}$ is not a constant vector; in other words, the only instance where the generalized additive secret sharing becomes insecure is when it is equivalent to the additive secret sharing. Does this mean all choices of $\vec{\beta}$ are equally secure, or can some choices offer even stronger security? In other words:

Which $\vec{\beta}$ provides $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ the strongest security against Hamming weight leakage?

We identify the *score function* Score that quantifies the security of the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$. This function captures how the choice of $\vec{\beta}$ influences the insecurity, as formalized in the following theorem.

▶ **Theorem 2.** *For $\vec{\beta} \in (F^*)^n$, the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ secret sharing scheme is ε insecure against the Hamming weight leakage, where*

$$\varepsilon = \mathcal{O}(n \log \lambda)^{n/2} \cdot \exp\left(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right) + \mathcal{O}(n \log \lambda)^{n/2} \cdot \lambda^{-n/2+1}.$$

In particular, if $\vec{\beta} \in (F^*)^n$ satisfies the following for $\frac{1}{2} - \frac{1}{n} > c > 0$,

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \geqslant \mathcal{O}(n \log \log \lambda) + cn \log \lambda \tag{11}$$

then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is $\mathcal{O}(\lambda^{-cn})$-insecure against the Hamming weight leakage.

Choosing $\vec{\beta}$ more carefully, by maximizing the minimum score, can lead to a faster reduction in insecurity (as shown in Corollary 1). We now present a different strategy to upper bound the first summand. Below is a brief overview of the proof of this theorem.

First summand estimation using an alternative approach. We upper bound the first summand in Equation 9 as follows:

$$\text{first summand} \leqslant \left(2\lambda^{1/2+\tau}\right)^n \cdot n \cdot \max_{\substack{\vec{w} \in \mathsf{Typical}(n,\tau) \\ \zeta \in \mathcal{S}_{\vec{\beta}}}} \left(\prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \right)$$

The key to upper bounding the first summand is to understand how the monomial $\prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right|$ can become large. Recall that $\widehat{\mathbb{1}}_{w_i}(\zeta^*)$ has a large magnitude. If $\vec{\beta}$ is such that every $\zeta\beta_i$ in the monomial simultaneously becomes ζ^* then the monomial has large magnitude, and we cannot prove the security of the secret-sharing scheme. This is exactly what happens when $\vec{\beta} = \vec{1}$; or, more generally, when all elements in $\vec{\beta}$ are identical.

For $\zeta \in \mathcal{S}_{\vec{\beta}}$, we will assign a score $\mathsf{Score}(\zeta; \vec{\beta})$ such that

$$\prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \leqslant \lambda^{-n/2} \cdot \exp\left(- \mathsf{Score}(\zeta; \vec{\beta}) \right)$$

Equation 3 presents the definition of our score function and Lemma 5 proves that it satisfies the equation above. This definition does not depend on w_i, only on the dual Hamming weights $\mathrm{wt}^{\vee}(\zeta\beta_i)$, where $i \in \{1, 2, \ldots n\}$. As a consequence, we get the following upper bound for the first summand, upon substituting our value of τ:

$$\text{first summand} \leqslant (n \log \lambda)^{n/2} n \cdot \exp\left(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right).$$

If the minimum score for $\zeta \in \mathcal{S}_{\vec{\beta}}$ is $\geqslant c \cdot n \log \lambda$, for some $1/2 \geqslant c > 0$, then the scheme will have insecurity $\leqslant \lambda^{-cn}$. When the elements of $\vec{\beta}$ are all identical, then its minimum score is 0; in which case, the first summand is not small. Substituting this bound into Equation 9, we get our desired result.

Theorem 2 then yields a way to choose reconstruction multipliers $\vec{\beta} \in (F^*)^n$ ensuring the security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$.

▶ **Corollary 1.** *Let $n \geqslant 3$ and $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F^*)^n$ where for every β_i, there exists some $\beta_j \neq \beta_i$ such that*

$$4cn \leqslant \mathrm{wt}^{\vee}(\beta_j \zeta^* \beta_i^{-1}) \leqslant \lambda - 4cn \tag{12}$$

for $c \in (5/36, 1/2 - 1/n)$. Then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is λ^{-cn}-insecure against Hamming weight leakage as long as λ is sufficiently large.

Over arbitrary fields.

We show that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ inherits its security from the security of Add_n, in the sense that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is no less secure than the additive secret sharing Add_n over *any finite field*. We make this connection precise via a *diagonalization* argument that relates the insecurity bound of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ directly to the quantity that is closely related to the insecurity of Add_n.

▶ **Theorem 3** (Diagonalization). *Let F_q be a finite field of order q. Let $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F_q^*)^n$ be multipliers and $\vec{\tau} = (\tau_1, \ldots, \tau_n)$ be the leakage. Define*

$$\mu_i := \sum_{\zeta \in F_q^*} \left(\sum_{\ell_i \in \Omega_i} \left| \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\zeta) \right| \right)^n.$$

Then,

$$\varepsilon(\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})) \leqslant \prod_{i=1}^{n} \mu_i^{1/n} \leqslant \frac{1}{n} \sum_{i=1}^{n} \mu_i \leqslant \max(\mu_1, \ldots, \mu_n)$$

▶ Remark 7. Combining Theorem 3 with the result of Faust et al. [20], we immediately obtain that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ over F_p, where $p = 2^\lambda - 1$ is a Mersenne prime, is $\mathcal{O}(\lambda^{-n/4})$-insecure against Hamming weight leakage whenever $n \geqslant 5$, for all $\vec{\beta} \in (F_p^*)^n$. △

2 Preliminaries

Basic Notations. Let F_q be a finite field of order (cardinality) q and λ be an integer such that $2^{\lambda-1} < q \leqslant 2^\lambda$. Unless the order needs to be specified, we will simply write F to denote the finite field. Let $F^* := F \setminus \{0\}$ denote the multiplicative group of F. We use U_F to denote the uniform distribution over F, and we write $x \leftarrow U_F$ when sampling $x \in F$ uniformly at random.

Given a set S, we denote by $\mathbb{1}_S$ the indicator function for set S, which gives $\mathbb{1}_S(x) = 1$ if $x \in S$ and 0 otherwise. For any function $f\colon D \to R$ where D is the domain and R is the range, we write $f^{-1}(y) := \{x \in D\colon f(x) = y\}$ for the set of all preimages of $y \in R$. For instance, $x \in F$ has $f(x) = w$ if and only if $\mathbb{1}_{f^{-1}(w)}(x) = 1$.

2.1 Secret Sharing (Masking) Schemes

▶ **Definition 1** (Additive Secret Sharing)**.** Let F be a finite field and n a positive integer. Given a secret $s \in F$, additive secret sharing Add_n shares s by sampling $(s_1, \ldots, s_n) \in F^n$ uniformly at random conditioned on $s_1 + \cdots + s_n = s$. More concretely, Add_n consists of the following two algorithms: given $s \in F$,

- $\mathsf{Share}(s)$: Sample $s_1, \ldots, s_{n-1} \leftarrow U_F$, set $s_n = s - (s_1 + \cdots + s_{n-1})$, and return $(s_1, \ldots, s_n)$.
- $\mathsf{Reconstruct}(\{s_1, \ldots, s_n\})$: Return $\tilde{s} = s_1 + \cdots + s_n$.

We denote by $\mathsf{Add}_n(s)$ the resulting distribution of shares $(s_1, \ldots, s_n)$.

▶ **Definition 2** (Generalized Additive Secret Sharing)**.** Let F be a finite field and n a positive integer. Given reconstruction multipliers $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F^*)^n$ and a secret $s \in F$, the generalized additive secret sharing $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ shares s by sampling $(s_1, \ldots, s_n) \in F^n$ uniformly at random conditioned on $\beta_1 s_1 + \cdots + \beta_n s_n = s$. More concretely, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ consists of the following two algorithms:

- $\mathsf{Share}(s)$: Sample $s_1, \ldots, s_{n-1} \leftarrow U_F$, set $s_n = \beta_n^{-1}(s - (\beta_1 s_1 + \cdots + \beta_{n-1} s_{n-1}))$, then return $(s_1, \ldots, s_n)$.
- $\mathsf{Reconstruct}(\{s_1, \ldots, s_n\})$: Return $\tilde{s} = \beta_1 s_1 + \cdots + \beta_n s_n$.

We denote by $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)$ the resulting distribution of shares $(s_1, \ldots, s_n)$.

Note that, by definition, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ sharing $s \in F$ with $\vec{\beta} = (c, \ldots, c) \in (F^*)^n$ where $c \in F^*$ constant is equivalent to Add_n sharing $c^{-1}s$.

The term *generalized* secret sharing was chosen in line with notational conventions in coding theory literature. Observe that, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ can be seen as Add_n generating the shares $(s'_1, \ldots, s'_n)$ such that $s'_1 + \cdots + s'_n = s$, then postprocessing them into $(\beta_1^{-1} s'_1, \ldots, \beta_n^{-1} s'_n)$. Interpreting the shares as codewords of a linear code [43], this postprocessing corresponds to the notion of generalized linear codes; see, for example, [27, Chapter 5].

▶ **Definition 3** (Shamir Secret Sharing)**.** Let F be a finite field and n and k be positive integers such that $k \leqslant n$. Denote by $F[X]_{<k}$ the set of polynomials over F of degree less than k [14, Definition 11.6]. Given evaluation places $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$ with $X_i \neq X_j$ for all $i \neq j$ and a secret $s \in F$, Shamir secret sharing $\mathsf{Shamir}(n, k, \vec{X})$ shares s by:

- $\mathsf{Share}(s)$: Sample a polynomial $P(X) \leftarrow F[X]_{<k}$ uniformly at random conditioned on $P(0) = s$. Evaluate $P(X)$ at each value in $\vec{X}$, i.e. $s_i = P(X_i)$ for $i = 1, \ldots, n$. Return $(s_1, \ldots, s_n)$.
- $\mathsf{Reconstruct}(\{s_{i_1}, \ldots, s_{i_k}\})$: Interpolate the polynomial $\tilde{P}(X) \in F[X]_{<k}$ over points $(X_{i_1}, s_{i_1}), \ldots, (X_{i_k}, s_{i_k})$. Return $\tilde{s} := \tilde{P}(0)$.

We denote by $\mathsf{Shamir}(n, k, \vec{X}; s)$ the resulting distribution of shares $(s_1, \ldots, s_n)$.

▶ **Proposition 1.** *Shamir secret sharing with $k = n$ is an instance of generalized additive secret sharing. Therefore, proving security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ automatically translates to the security of $\mathsf{Shamir}(n, n, \vec{X})$.*

Proof of Proposition 1. It suffices to show that, for all evaluation points $\vec{X} \in (F^*)^n$ and secret $s \in F$, there exists $\vec{\beta} \in (F^*)^n$ such that $\beta_1 s_1 + \cdots + \beta_n s_n = s$ where $(s_1, \ldots, s_n) \leftarrow \mathsf{Shamir}(n, n, \vec{X}; s)$.

Given n pairs $(X_1, s_1), \ldots, (X_n, s_n)$ from $\mathsf{Shamir}(n, n, \vec{X})$, one can recover the polynomial $P(X)$ that was used to compute s_i's via Lagrange interpolation:

$$P(X) := \sum_{i=1}^{n} \underbrace{\left(\prod_{j \in \{1,2,\ldots,n\} \setminus \{i\}} \frac{X - X_j}{X_i - X_j} \right)}_{=: L_i(X)} \cdot s_i = \sum_{i=1}^{n} L_i(X) \cdot s_i$$

and hence the secret $s = P(0) = \sum_{i=1}^{n} L_i(0) \cdot s_i$. Therefore, $\mathsf{Shamir}(n, n, \vec{X})$ that shares s is $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ sharing s, where

$$\beta_i = L_i(0) = \prod_{m \in \{1,2,\ldots,n\} \setminus \{i\}} \frac{X_m}{X_m - X_i}$$

for all $i \in \{1, 2, \ldots, n\}$. ◀

2.2 Leakage-Resilient Secret Sharing

We quantify the variation between two distributions P and Q using the *statistical distance*.

▶ **Definition 4** (Statistical Distance)**.** The statistical distance between two distributions P and Q over a finite space Ω is defined as

$$\mathrm{SD}(P\ ,\ Q) := \frac{1}{2} \sum_{x \in \Omega} \Big| \Pr[P = x] - \Pr[Q = x] \Big|.$$

▶ **Definition 5** (Local Leakage [6, 7])**.** Let F be a finite field and n be a positive integer. Let $\mathcal{S}$ be a secret sharing scheme with sharing algorithm Share. Let $\vec{\tau} = (\tau_1, \ldots, \tau_n)$ be a collection of n functions whose domains are F. For any secret $s \in F$, the leakage distribution $\vec{\tau}(\mathsf{Share}(s))$ is defined by the following experiment:

1. Sample shares $\vec{s} = (s_1, \ldots, s_n)$ from $\mathsf{Share}(s)$.
2. Output $(\tau_1(s_1), \ldots, \tau_n(s_n))$.

We refer to $\vec{\tau}(\mathsf{Share}(s))$ as the joint leakage distribution induced by all shares of $s \in F$, and for brevity we shall also write it as $\vec{\tau}(s)$ instead.

▶ **Definition 6** (ε-insecurity)**.** A secret sharing scheme $\mathcal{S}$ is said to be ε-insecure against a local leakage $\vec{\tau}$ if for all secret $s \in F$,

$$\varepsilon(\mathcal{S}; \vec{\tau}) := 2 \cdot \mathrm{SD}(\vec{\tau}(\mathsf{Share}(s))\ ,\ \vec{\tau}(\mathsf{Share}(U_F))) \leqslant \varepsilon$$

Roughly speaking, if $\mathcal{S}$ has small insecurity against a leakage attack, then the joint distribution of leakage of shares is statistically independent of the secret.

In this paper, we primarily focus on the setting where all leakage functions are the Hamming weight, i.e. $\tau_1 = \cdots = \tau_n = \mathrm{wt}$. And in this case, $\vec{\tau}(\vec{s}) = \overrightarrow{\mathrm{wt}}(\vec{s})$ corresponds to the joint Hamming weight leakage of the shares of s.

▶ **Definition 7** (Typical Weights)**.** We call $w \in \{0, 1, \ldots, \lambda\}$ to be *typical* if $|w - \lambda/2| \leqslant \lambda^{1/2+\tau}$ for some $\tau > 0$. And we say a vector $\vec{w} = (w_1, w_2, \ldots, w_n) \in \{0, 1, \ldots, \lambda\}^n$ is in a *typical set* $\mathsf{Typical}(n, \tau)$ if every w_i is typical:

$$\mathsf{Typical}(n, \tau) := \left\{ \vec{w} \ :\ |w_i - \lambda/2| \leqslant \lambda^{1/2+\tau} \quad \forall i \in \{1, 2, \ldots, n\} \right\}.$$

2.3 Extension Fields and Hamming Weight

The field F_{2^λ} is isomorphic to the vector space F_2^λ upon choosing a basis $\mathcal{B} = (b_1, \dots, b_\lambda)$. An element $\zeta \in F_{2^\lambda}$ is represented as a vector $(\zeta_1, \dots, \zeta_\lambda) \in F_2^\lambda$ satisfying $\zeta = \sum_{j=1}^{\lambda} \zeta_j b_j$. We refer to $(\zeta_1, \dots, \zeta_\lambda) \in F_2^\lambda$ as the *vector representation* of $\zeta \in F_{2^\lambda}$ under the basis $\mathcal{B}$, and the *Hamming weight* $\mathrm{wt}_{\mathcal{B}}(\zeta)$ of $\zeta \in F_{2^\lambda}$ is the number of 1's this vector representation. For brevity, we write $\mathrm{wt}(\zeta) = \mathrm{wt}_{\mathcal{B}}(\zeta)$ unless the basis $\mathcal{B}$ must be specified. We also write $\mathbb{1}_w := \mathbb{1}_{\mathrm{wt}^{-1}(w)}$, i.e.

$$\mathbb{1}_w(x) := \begin{cases} 1, & \text{if } \mathrm{wt}(x) = w \\ 0, & \text{otherwise} \end{cases}$$

▶ **Definition 8** (Field Trace)**.** The trace of an extension field F_{p^d} over the base field F_p, denoted by $\mathsf{Tr}_{F_{p^d}/F_p} \colon F_{p^d} \to F_p$, is defined as

$$\mathsf{Tr}_{F_{p^d}/F_p}(y) := \sum_{i=0}^{d-1} y^{p^i}$$

The *trace-dual coordinate vector* $\zeta^\vee$ of $\zeta \in F_{2^\lambda}$ is its vector representation under the basis $\mathcal{B}^\vee$ dual to $\mathcal{B} = (b_1, \dots, b_\lambda)$, and can be computed as

$$\zeta^\vee := \left(\mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_1), \dots, \mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_\lambda)\right) \in F_2^\lambda$$

because if we write $\mathcal{B}^\vee = (b_1^\vee, \dots, b_\lambda^\vee)$, then

$$\mathsf{Tr}_{F_{2^\lambda}/F_2}(b_i b_j^\vee) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

We hence also have $\mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta x) = \langle \zeta^\vee, x \rangle$ for all $\zeta, x \in F_{2^\lambda}$ (the x in the inner product $\langle \alpha^\vee, x \rangle$ is the vector representation of x). The *trace-dual Hamming weight* of ζ is then the Hamming weight of $\zeta^\vee$, i.e. $\mathrm{wt}^\vee(\zeta) = \mathrm{wt}(\zeta^\vee)$. The map $\zeta \mapsto \zeta^\vee$ is an invertible F_2-linear map, and also efficiently computable [56].

2.4 Fourier Analysis on Finite Fields

We will use Fourier analysis on the additive group $(F_{p^d}, +)$ for a prime $p \geqslant 2$ and degree of extension $d \in \{1, 2, \dots\}$. In this subsection, $F := F_{p^d}$.

Let $\omega_p := \exp(2\pi\imath/p)$. Define the Fourier transformation of $f \colon F \to \mathbb{C}$ over F, denoted $\widehat{f} \colon F \to \mathbb{C}$, as follows:

$$\widehat{f}(\alpha) \;:=\; \frac{1}{q} \sum_{x \in F} f(x) \cdot \omega_p^{-\mathsf{Tr}_{F/F_p}(\alpha x)} \qquad \forall \alpha \in F$$

We call $\chi_\alpha(x) = \omega_p^{\mathsf{Tr}_{F/F_p}(\alpha x)}$ the *character* and $\widehat{f}(\alpha)$ the *Fourier coefficient* of f at α.

▶ **Example 1.** For $p = 2$, we have $\omega := \omega_2 = \exp(\pi\imath) = -1$ and Fourier coefficients are

$$\widehat{f}(\alpha) \;:=\; \frac{1}{q} \sum_{x \in F_{2^d}} f(x) \cdot (-1)^{\mathsf{Tr}_{F/F_2}(\alpha x)}.$$

Since $\mathsf{Tr}_{F/F_2}(\alpha x) = \langle \alpha^\vee, x \rangle$ as mentioned in Section 2.3, $\widehat{\mathbb{1}}_w(\alpha)$ is a function of $\mathrm{wt}^\vee(\alpha)$; in particular, for all $\alpha, \alpha' \in F_{2^d}$, if $\mathrm{wt}^\vee(\alpha) = \mathrm{wt}^\vee(\alpha')$ then $\widehat{\mathbb{1}}_w(\alpha) = \widehat{\mathbb{1}}_w(\alpha')$.

▶ **Fact 1** (Parseval's Identity). *For any function* $f\colon F \to \mathbb{C}$,

$$\frac{1}{\mathrm{card}(F)} \sum_{x \in F} |f(x)|^2 = \sum_{\alpha \in F} \left|\widehat{f}(\alpha)\right|^2.$$

▶ **Fact 2** (Character Sum). *For all* $\alpha \in F$,

$$\sum_{x \in F} \chi_\alpha(x) = \begin{cases} \mathrm{card}(F) & \text{if } \alpha = 0 \\ 0 & \text{otherwise} \end{cases}$$

Note also that the modulus $|\chi_\alpha(x)| = 1$ for any α and x in F.

2.5 Imported Lemmas

▶ **Lemma 1** (Chernoff Bound [44, Theorem 2.1]). *Let* $X_1, X_2, \ldots, X_\lambda$ *be independent Bernoulli random variables with* $\mathbb{E}(X_i) = p$ *for each* i. *Then for any* $t \geqslant 0$,

$$\Pr\left(\left|\sum_{i=1}^{\lambda} X_i - \lambda p\right| \geqslant \lambda t\right) \leqslant 2\exp(-2\lambda t^2).$$

In particular, for $t = \lambda^{-\frac{1}{2}+\tau}$, *the upper bound is* $2\exp(-2\lambda^{2\tau})$.

▶ **Lemma 2** (Poisson Summation Formula [46, Chapter 3.3]). *Let* $C \subseteq F^n$ *denote the set of all shares of the secret* $0 \in F = F_{p^d}$. *Let* $\vec{v} \in F^n$ *denote an arbitrary secret share of the secret* $1 \in F$. *Consider an arbitrary local leakage* $\vec{\tau}\colon F^n \to \Omega^n$. *For any secret* $s \in F$, *let* $\vec{\tau}(s)$ *denote the distribution of the leakage* $\vec{\tau}(\vec{x})$, *where* $\vec{x}$ *is sampled uniformly at random from the set* $s \cdot \vec{v} + C$. *The following identity holds for any leakage value* $\vec{\ell} \in \Omega^n$.

$$\Pr\left[\vec{\tau}(s) = \vec{\ell}\right] = \sum_{\vec{z} \in C^\perp} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(z_i)\right) \cdot \chi_1(s \cdot \langle \vec{z}, \vec{v} \rangle)$$

where $\chi_1(x) = \omega_p^{\mathrm{Tr}_{F/F_p}(x)}$, *whose modulus is* $|\chi_1(x)| = 1$ *for any* $x \in F$.

▶ **Lemma 3** (Generalized Hölder's Inequality [28, Theorem 11]). *Let* $p_1, \ldots, p_n$ *be positive real numbers such that* $p_1 + \cdots + p_n = 1$, *and* $(x_i^{(1)})_{i=1}^k$, $(x_i^{(2)})_{i=1}^k$, $\ldots$, $(x_i^{(n)})_{i=1}^k$ *be sequences of real numbers. Then,*

$$\sum_{i=1}^{k} \left|x_i^{(1)}\right|^{p_1} \cdots \left|x_i^{(n)}\right|^{p_n} \leqslant \left(\sum_{i=1}^{k} \left|x_i^{(1)}\right|\right)^{p_1} \cdots \left(\sum_{i=1}^{k} \left|x_i^{(n)}\right|\right)^{p_n}$$

3 Insecurity Analysis

In this section, we formally state the technical results introduced in Section 1.2 and their proofs outlined in the overview (Section 1.3).

Theorem 1 in Section 3.1 shows that generalized additive secret sharing $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is always provably secure as long as $n \geqslant 3$ and the elements of $\vec{\beta}$ are not all the same. Theorem 2 in Section 3.2 derives the insecurity bound in terms of $\vec{\beta}$, hence allows users to quantify and certify the security of their $\vec{\beta}$, or even to construct secure $\vec{\beta}$ of their own (Corollary 1). We then conclude with Section 3.3 which presents results over any finite field such as Theorem 3, that shows the security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ against a leakage attack can be upper bounded via corresponding quantities for Add_n.

3.1 Worst-case Analysis (Theorem 1)

▶ **Theorem 1.** *For* $\vec{\beta} \in (F^*)^n \setminus \{(b,\dots,b) : b \in F^*\}$ *and* $n \in \{3,4,\dots\}$, *we have*

$$\varepsilon\Big(\ \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})\ ;\ \overrightarrow{\mathrm{wt}}\ \Big) = \mathcal{O}\Big(\lambda^{-1/4}\Big).$$

The proof of Theorem 1 relies on the following lemma that upper bounds our Fourier coefficients; see Appendix A for its proof.

▶ **Lemma 4.** *For* $\lambda \geqslant 2$, $w \in \{1,\dots,\lambda\}$, *and* $\zeta \in F$, *we have* $|\widehat{\mathbb{1}}_w(\zeta)| \leqslant B(\zeta)$ *where*

$$B(\zeta) := \begin{cases} \lambda^{-1/2}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{0,\lambda\} \\ \lambda^{-1}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{1,\lambda-1\} \\ 4\cdot\lambda^{-3/2}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{2,\lambda-2\} \\ \lambda^{-\frac{1}{4}}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-\frac{1}{2}}, & \text{otherwise.} \end{cases}$$

And hence,

$$\sum_{\mathrm{wt}^\vee(\zeta)=1}^{\lambda-1} (B(\zeta))^n \leqslant 3\cdot 5^{\frac{5n}{2}-4}\cdot\lambda^{-n+1}$$

Proof of Theorem 1. By Definition 6, it suffices to prove that the following quantity is upper bounded by ε.

$$\begin{aligned} &2\cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\ &\quad= \sum_{\vec{w}\in\{0,1,\dots,\lambda\}^n} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \right| \end{aligned} \tag{13}$$

Recall from Definition 7 that a weight $w \in \{0,1,\dots,\lambda\}$ is said to be typical if it is only up to $\lambda^{1/2+\tau}$ away from the average $\lambda/2$ for some $\tau > 0$. Let us write $\vec{w} \notin \mathsf{Typical}(n,\tau)$ to denote that $\vec{w} \in \{0,1,\dots,\lambda\}^n \setminus \mathsf{Typical}(n,\tau)$. Chernoff bound (Lemma 1) implies that the probability mass on atypical weights contribute only negligibly to the statistical distance.

$$\begin{aligned} &\sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \right| \\ &\leqslant \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \\ &\qquad\qquad + \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \qquad \text{(by triangle inequality)} \\ &= 2\cdot\max_{s\in F}\left(\sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \right) \\ &= 2\cdot \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};\widetilde{s})}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \qquad \text{(let } \widetilde{s} \text{ be the arg max)} \\ &= 2\cdot \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};\widetilde{s})}[\overrightarrow{\mathrm{wt}}(\vec{s}) \notin \mathsf{Typical}(n,\tau)] \\ &\leqslant 2\cdot \sum_{j=1}^{n} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};\widetilde{s})}[\mathrm{wt}(s_j) \text{ is not typical}] \qquad \text{(by union bound)} \\ &\leqslant 2n\cdot 2\exp(-2\lambda t^2) \qquad \text{(by Chernoff bound (Lemma 1))} \end{aligned}$$

Hence, the expression for the statistical distance (Equation 13) becomes a summation over the set of typical weights $\mathsf{Typical}(n,\tau)$ plus a negligible quantity.

(Equation 13)

$$
\begin{aligned}
&= \sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] \right| \\
&= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] \right| \\
&\qquad \pm \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] \right| \\
&= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] - \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] \right| \qquad (14) \\
&\qquad \pm\ 2\cdot 2n\cdot\exp(-2\lambda^{2\tau})
\end{aligned}
$$

If $\vec{s}\in F^n$ is a share of secret 0, i.e. $\vec{s}\in C := \mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};0)$, then $\beta_1 s_1+\cdots+\beta_n s_n=0$, and for any $\zeta\in F$, we have $\zeta\beta_1 s_1+\cdots+\zeta\beta_n s_n=\zeta\cdot 0=0$. From this, we can deduce $C^\perp=\{\zeta\vec{\beta}\mid\zeta\in F\}$, then by Poisson summation formula (Lemma 2), for any $\vec{v}\in\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};1)$ we have

$$
\begin{aligned}
\Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] &= \sum_{\vec{z}\in C^\perp} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(z_i)\right)\cdot\chi_1(s\cdot\langle\vec{z},\vec{v}\rangle) \\
&= \sum_{\zeta\in F} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_1\left(s\cdot\zeta\cdot\left\langle\vec{\beta},\vec{v}\right\rangle\right) \\
&= \sum_{\zeta\in F} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_1(s\cdot\zeta) \qquad (\because \vec{v}\in\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};1)) \\
&= \sum_{\zeta\in F} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_\zeta(s) \qquad (15)
\end{aligned}
$$

Moreover,

$$
\begin{aligned}
\Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] &= \frac{1}{\mathrm{card}(F)} \sum_{s\in F} \Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right] \\
&= \frac{1}{\mathrm{card}(F)} \sum_{s\in F} \sum_{\zeta\in F} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_\zeta(s) \qquad \text{(by Eq. 15)} \\
&= \frac{1}{\mathrm{card}(F)} \sum_{\zeta\in F} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\sum_{s\in F}\chi_\zeta(s) \\
&= \frac{1}{\mathrm{card}(F)} \sum_{\zeta\in\{0\}} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\mathrm{card}(F) \qquad \text{(by Fact 2)} \\
&= \sum_{\zeta\in\{0\}} \left(\prod_{i=1}^n \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right) \qquad (16)
\end{aligned}
$$

Plugging these into the summand in Equation 14, we get

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\left|\Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};s)}\left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right]-\Pr_{\vec{s}\leftarrow\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta};U_F)}\left[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}\right]\right|$$

$$=\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\left|\sum_{\zeta\in F}\left(\prod_{i=1}^{n}\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_\zeta(s)-\sum_{\zeta\in\{0\}}\left(\prod_{i=1}^{n}\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\right| \qquad \text{(by Equation 15 and 16)}$$

$$=\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\left|\sum_{\zeta\in F^*}\left(\prod_{i=1}^{n}\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot\chi_\zeta(s)\right| \qquad \text{(since } \chi_0(s)=1 \text{ for all } s\in F\text{)}$$

$$\leqslant\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in F^*}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \qquad \text{(by triangle inequality)} \qquad (17)$$

Let $\zeta^*\in F$ be the element such that $\mathrm{wt}^\vee(\zeta^*)=\lambda$ and consider the set

$$\mathcal{S}_{\vec{\beta}} := \left\{\zeta^*\cdot\beta_1^{-1},\ \zeta^*\cdot\beta_2^{-1},\ \ldots,\ \zeta^*\cdot\beta_n^{-1}\right\}.$$

Then for any $\zeta\in\mathcal{S}_{\vec{\beta}}$, at least one of β_i's should give $\beta_i\zeta=\zeta^*$. Consider the following separation of the summation.

(Equation 17)

$$=\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|+\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \qquad (18)$$

Let us upper bound the second summand (the summation over $F^*\setminus\mathcal{S}_{\vec{\beta}}$). As stated in Lemma 4, we denote $B(\zeta)$ to be a function that upper bounds $|\widehat{\mathbb{1}}_w(\zeta)|$. Then,

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|$$

$$\leqslant\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}B(\beta_i\zeta)$$

$$=\left(2\lambda^{1/2+\tau}\right)^n\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}B(\beta_i\zeta) \qquad \text{(since } \mathrm{card}(\mathsf{Typical}(n,\tau))=(2\lambda^{1/2+\tau})^n\text{)}$$

$$\leqslant\left(2\lambda^{1/2+\tau}\right)^n\sum_{\zeta\in F\setminus\{0,\zeta^*\}}B(\zeta)^n \qquad \text{(by Hölder's inequality (Lemma 3))}$$

$$\leqslant 2^{n+2}\cdot 5^{\frac{5n}{2}-4}\cdot\lambda^{n\tau}\cdot\lambda^{-\frac{n}{2}+1} \qquad \text{(by Lemma 4)} \qquad (19)$$

Let $H(\zeta;\vec{\beta}) := \{i\colon \beta_i\zeta\neq\zeta^*\}$. The first summand (the summation over $\mathcal{S}_{\vec{\beta}}$) can be rewritten as follows

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|$$

$$\leqslant\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|$$

(since $\mathsf{Typical}(n,\tau)\subseteq\{0,1,\ldots,\lambda\}^n$ and $|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)|\geqslant 0$)

$$= \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \sum_{\vec{w} \in \{0,1,\ldots,\lambda\}^n} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right|$$

$$= \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i \in \{1,2,\ldots,n\}} \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right|$$

$$= \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \left(\prod_{i \in H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \right) \cdot \left(\prod_{i \notin H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \right) \tag{20}$$

Next, we separate bound the ℓ_1-norms on the right-hand side for those indices $i \in H(\zeta;\vec{\beta})$ and $i \notin H(\zeta;\vec{\beta})$. We use the following claims, whose proofs are provided in Appendix A and Appendix B.1 respectively.

▶ **Claim 1.** *For all $\lambda \in \{1,2,\ldots\}$, $w \in \{1,2,\ldots,\lambda\}$, and $\zeta \in F$,*

$$\left| \widehat{\mathbb{1}}_w(\zeta) \right| \leqslant \frac{1}{2^{\lambda/2}} \binom{\lambda}{w}^{1/2} \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2} \leqslant \frac{1}{\lambda^{1/4}} \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-\frac{1}{2}} \qquad \text{if } \zeta \notin \{0, \zeta^*\}$$

$$\left| \widehat{\mathbb{1}}_w(\zeta) \right| = \frac{1}{2^\lambda} \binom{\lambda}{w} \leqslant \frac{1}{\sqrt{\lambda}} \qquad \text{if } \zeta \in \{0, \zeta^*\}$$

▶ **Claim 2.** *For $m \in \{1,2,\ldots\}$, the following bound holds.*

$$\sum_{i=0}^{m} \binom{m}{i}^{1/2} < \pi \cdot m^{1/4} \cdot 2^{m/2}.$$

Case 1. Consider $i \in H(\zeta;\vec{\beta})$. This is the non-trivial case, we want a non-trivial upper bound.

$$\sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \leqslant \sum_{w_i=0}^{\lambda} \binom{\lambda}{w_i}^{1/2} \cdot 2^{-\lambda/2} \cdot \binom{\lambda}{\mathrm{wt}^\vee(\beta_i \zeta)}^{-1/2} \qquad \text{(by Claim 1)}$$

$$= \binom{\lambda}{\mathrm{wt}^\vee(\beta_i \zeta)}^{-1/2} \sum_{w_i=0}^{\lambda} \binom{\lambda}{w_i}^{1/2} \cdot 2^{-\lambda/2}$$

$$< \binom{\lambda}{\mathrm{wt}^\vee(\beta_i \zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4} \qquad \text{(by Claim 2)}$$

Case 2. Consider $i \notin H(\zeta;\vec{\beta})$. In this case, we have the trivial estimate from Claim 1.

$$\sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| = \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\zeta^*) \right| = \sum_{w_i=0}^{\lambda} \widehat{\mathbb{1}}_{w_i}(0) = \sum_{w_i=0}^{\lambda} \binom{\lambda}{w_i} \cdot 2^{-\lambda} = 1$$

Substituting these values into Equation 20 and continuing the upper bound, we have:

$$\text{(Equation 20)} < \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i \in H(\zeta;\vec{\beta})} \binom{\lambda}{\mathrm{wt}^\vee(\beta_i \zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4} \tag{21}$$

Note that, for any $i \in H(\zeta;\vec{\beta})$, $\mathrm{wt}^{\vee}(\beta_i\zeta) \in \{1,2,\dots,\lambda-1\}$. Therefore, using the fact that $\binom{\lambda}{\mathrm{wt}^{\vee}(\beta_i\zeta)} \geqslant \binom{\lambda}{1} = \lambda$ for any $i \in H(\zeta;\vec{\beta})$, we obtain the following bound for the above quantity:

$$(\text{Equation 21}) \leqslant \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}} \lambda^{-\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{2}} \cdot \pi^{\mathrm{card}(H(\zeta;\vec{\beta}))} \cdot \lambda^{\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{4}} \leqslant (\widetilde{h}+1)\cdot\left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}} \tag{22}$$

because $\mathrm{card}(\mathcal{S}_{\vec{\beta}}) \leqslant \widetilde{h}+1$, where $\widetilde{h} = \min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\Big(\mathrm{card}(H(\zeta;\vec{\beta}))\Big)$. [2]

Therefore, for a sufficiently large λ, the above sum is small as long as we have $\mathrm{card}(H(\zeta;\vec{\beta})) \geqslant 1$; that is, unless $\beta_1 = \beta_2 = \cdots = \beta_n$ (i.e., unless the secret sharing is the additive secret sharing), the above sum would be at most $\lambda^{-1/4}$. More precisely:

$$\begin{aligned}
&2\cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big)\\
&\quad\leqslant \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\ \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n}\Big|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\Big| + \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\ \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n}\Big|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\Big|\\
&\qquad\qquad + 2\cdot 2n\cdot\exp(-2\lambda^{2\tau}) \qquad\qquad \text{(by Equation 14 and 18)}\\
&\quad\leqslant (\widetilde{h}+1)\cdot\left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}} \ +\ 2^{n+2}\cdot 5^{\frac{5n}{2}-4}\cdot\lambda^{n\tau}\cdot\lambda^{-\frac{n}{2}+1} \ +\ 2\cdot 2n\cdot\exp(-2\lambda^{2\tau})\\
&\qquad\qquad \text{(by Equation 19 and 22; also recall that } \widetilde{h} := \min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathrm{card}(H(\zeta;\vec{\beta}))\text{)}\\
&\quad\leqslant 2\pi\cdot\frac{c_n}{\lambda^{1/4}} \ +\ 2^{n+2}\cdot 5^{\frac{5n}{2}-4}\cdot\lambda^{n\tau}\cdot\lambda^{-\frac{n}{2}+1} \ +\ 2\cdot 2n\cdot\exp(-2\lambda^{2\tau})\\
&\qquad\qquad \text{(because } \vec{\beta} \text{ cannot be of the form } (b,b,\dots,b)\in(F^*)^n\text{)}
\end{aligned}$$

which is $\mathcal{O}\big(\lambda^{-1/4}\big)$, for sufficiently large λ. ◀

3.2 Security Characterization (Theorem 2)

▶ **Theorem 2.** *For $\vec{\beta}\in(F^*)^n$, the $\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta})$ secret sharing scheme is ε insecure against the Hamming weight leakage, where*

$$\varepsilon = \mathcal{O}(n\log\lambda)^{n/2}\cdot\exp\Big(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\Big) + \mathcal{O}(n\log\lambda)^{n/2}\cdot\lambda^{-n/2+1}.$$

In particular, if $\vec{\beta}\in(F^*)^n$ satisfies the following for $\frac{1}{2}-\frac{1}{n} > c > 0$,

$$\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta}) \geqslant \mathcal{O}(n\log\log\lambda) + cn\log\lambda \tag{11}$$

then $\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta})$ is $\mathcal{O}(\lambda^{-cn})$-insecure against the Hamming weight leakage.

For the proof of Theorem 2, we use the following lemma that relates the product of Fourier coefficients to our Score function. Its proof is deferred to Appendix A.

[2] If $\zeta\in\mathcal{S}_{\vec{\beta}}$, then there should exist $j\in\{1,2,\dots,n\}$ such that $\zeta = \beta_j^{-1}\zeta^*$, and so $i\in H(\zeta,\vec{\beta})$ iff $\beta_i\neq\beta_j$. Hence, for any $\zeta\in\mathcal{S}_{\vec{\beta}}$, $\mathrm{card}(H(\zeta;\vec{\beta}))\geqslant\mathrm{card}(\mathcal{S}_{\vec{\beta}})-1$, making $\widetilde{h} := \min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathrm{card}(H(\zeta;\vec{\beta}))\geqslant\mathrm{card}(\mathcal{S}_{\vec{\beta}})-1$ as well.

▶ **Lemma 5.** *For any* $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in (F^*)^n$ *and* $\vec{w} = (w_1, w_2, \ldots, w_n) \in \{1, 2, \ldots, \lambda\}^n$,

$$\prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \leqslant \lambda^{-\frac{n}{2}} \cdot \exp\Big(- \mathsf{Score}(\zeta; \vec{\beta}) \Big)$$

Proof of Theorem 2. The proof goes in the same way as for Theorem 1, with the estimation of the second summand unchanged. The only difference lies in the first summand, which naturally gives rise to the score function quantifying the security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$.

The first summand (the summation over $\mathcal{S}_{\vec{\beta}}$) can be rewritten as follows using Lemma 5

$$\begin{aligned}
\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| &\leqslant 2^n \cdot \lambda^{(\frac{1}{2}+\tau)\cdot n} \cdot n \cdot \max_{\substack{\vec{w} \in \mathsf{Typical}(n,\tau) \\ \zeta \in \mathcal{S}_{\vec{\beta}}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\
&\leqslant 2^n \cdot \lambda^{(\frac{1}{2}+\tau)\cdot n} \cdot n \cdot \lambda^{-\frac{n}{2}} \cdot \exp\Big(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \Big) \\
&= (2\lambda^{\tau})^n \cdot n \cdot \exp\Big(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \Big) \qquad (23)
\end{aligned}$$

because the maximum of a sequence is at least as large as its average. Hence, upon choosing

$$\tau = \frac{\log\left(\frac{n}{4} \log \lambda\right)}{2 \log \lambda}$$

so that we have $2\lambda^{\tau} = (n \log \lambda)^{1/2}$, we get

$$\begin{aligned}
&\text{(Equation 18)} \\
&\leqslant (2\lambda^{\tau})^n \cdot n \cdot \exp\Big(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \Big) + 4 \cdot 5^{\frac{5n}{2}-4} \cdot (2\lambda^{\tau})^n \cdot \lambda^{-\frac{n}{2}+1} \\
&\qquad \text{(by Equation 19 and 23)} \\
&\leqslant (n \log \lambda)^{n/2} \cdot n \cdot \exp\Big(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \Big) + 4 \cdot 5^{\frac{5n}{2}-4} \cdot (n \log \lambda)^{n/2} \cdot \lambda^{-\frac{n}{2}+1} \qquad (24)
\end{aligned}$$

In summary, we have the following chain of expressions:

$$\begin{aligned}
&2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\
&= \sum_{\vec{w} \in \{0,1,\ldots,\lambda\}^n} \left| \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right| \\
&\qquad \text{(from Equation 13)} \\
&= \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right| \\
&\qquad \pm 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \qquad \text{(from Equation 14)} \\
&\leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^*} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \qquad \text{(from Equation 17)} \\
&= \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| + \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\
&\qquad + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \qquad \text{(from Equation 18)}
\end{aligned}$$

$$\leqslant (n\log\lambda)^{\frac{n}{2}}\cdot n\cdot\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\right)+4\cdot 5^{\frac{5n}{2}-4}\cdot(n\log\lambda)^{\frac{n}{2}}\cdot\lambda^{-\frac{n}{2}+1}+2\cdot 2n\cdot\lambda^{-\frac{n}{2}}$$

(from Equation 24 and $\tau=\frac{\log\left(\frac{n}{4}\log\lambda\right)}{2\log\lambda}$)

$$\leqslant (n\log\lambda)^{\frac{n}{2}}\cdot n\cdot\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\right)+\left(5^{\frac{5n}{2}-3}\cdot(n\log\lambda)^{\frac{n}{2}}+\frac{4n}{\lambda}\right)\lambda^{-\frac{n}{2}+1}$$

$$\leqslant \mathcal{O}(n\log\lambda)^{\frac{n}{2}}\cdot\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\right)+\mathcal{O}(n\log\lambda)^{\frac{n}{2}}\cdot\lambda^{-\frac{n}{2}+1}$$

(for sufficiently large λ)

Now, suppose that $\vec{\beta}$ gives

$$\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\geqslant\left(\frac{n}{2}+1\right)\log(n\log\lambda)+cn\log\lambda \tag{25}$$

for some constant $c>0$. Then, from the above expression,

$$\begin{aligned}
&2\cdot\mathrm{SD}\left(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\right)\\
&\quad\leqslant (n\log\lambda)^{\frac{n}{2}}\cdot n\cdot\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\right)+\left(5^{\frac{5n}{2}-3}\cdot(n\log\lambda)^{\frac{n}{2}}+\frac{4n}{\lambda}\right)\cdot\lambda^{-\frac{n}{2}+1}\\
&\quad\leqslant (n\log\lambda)^{\frac{n}{2}}\cdot n\cdot(n\log\lambda)^{-\frac{n}{2}-1}\cdot\lambda^{-cn}+\left(5^{\frac{5n}{2}-3}\cdot(n\log\lambda)^{\frac{n}{2}}+\frac{4n}{\lambda}\right)\cdot\lambda^{-\frac{n}{2}+1}\\
&\quad\leqslant \lambda^{-cn}+\mathcal{O}\left(\lambda^{-c'n}\right)=\mathcal{O}\left(\lambda^{-cn}\right)\qquad\qquad\left(\tfrac{\log\lambda}{\lambda}\leqslant\lambda^{-c'}\text{ holds for all }c'\in(0,1/2)\right)
\end{aligned}$$

and this concludes the proof of Theorem 2. ◀

Note that Theorem 2 provides an insecurity bound in terms of reconstruction multipliers $\vec{\beta}\in(F^*)^n$. This consequently gives a method for choosing $\vec{\beta}$ such that $\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta})$ is guaranteed to be secure, by choosing one that makes the bound small.

▶ **Corollary 1.** *Let $n\geqslant 3$ and $\vec{\beta}=(\beta_1,\ldots,\beta_n)\in(F^*)^n$ where for every β_i, there exists some $\beta_j\neq\beta_i$ such that*

$$4cn\leqslant\mathrm{wt}^{\vee}(\beta_j\zeta^*\beta_i^{-1})\leqslant\lambda-4cn \tag{12}$$

for $c\in(5/36,1/2-1/n)$. Then $\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta})$ is λ^{-cn}-insecure against Hamming weight leakage as long as λ is sufficiently large.

Proof of Corollary 1. Consider any $\zeta\in\mathcal{S}_{\vec{\beta}}$. Then, by definition of $\mathcal{S}_{\vec{\beta}}$, we can write $\zeta=\zeta^*\beta_i^{-1}$ for some distinct multiplier β_i in $\vec{\beta}$. By condition, there is another distinct multiplier value $\beta_j\neq\beta_i$ appearing in $\vec{\beta}$ that gives $4cn\leqslant\mathrm{wt}^{\vee}(\beta_j\zeta^*\beta_i^{-1})\leqslant\lambda-4cn$. Therefore,

$$\mathsf{Score}(\zeta;\vec{\beta})=\sum_{\ell=1}^{n}\sigma(\mathrm{wt}^{\vee}(\beta_\ell\cdot\zeta))\geqslant\sigma(\mathrm{wt}^{\vee}(\beta_j\cdot\zeta))=\sigma\left(\mathrm{wt}^{\vee}(\beta_j\zeta^*\beta_i^{-1})\right)\geqslant\left(\frac{8}{5}cn-\frac{1}{4}\right)\log\lambda.$$

The last inequality follows from the definition (Equation 2), and provided that λ is sufficiently large, say $\lambda\geqslant(4cn)^5$. Since $\zeta\in\mathcal{S}_{\vec{\beta}}$ was arbitrary, we get $\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\geqslant\left(\frac{8}{5}cn-\frac{1}{4}\right)\log\lambda$. It satisfies Equation 25 in the proof of Theorem 2 (as long as $cn>5/12$ which by choosing $c>5/36$ it always holds for all $n\geqslant 3$). Therefore, $\mathsf{Gen}(\mathsf{Add}_n,\vec{\beta})$ is at most λ^{-cn}-insecure by Theorem 2. ◀

▶ Remark 8 (Security of Shamir Secret Sharing). Corollary 1 also implies the security of $\mathsf{Shamir}(n, n, \vec{X})$ when the evaluation places $\vec{X} = (X_1, \ldots, X_n)$ are chosen uniformly at random.

Observe that, as discussed in Remark 2, if β_i and β_j are chosen independently at random from F, the constraints in Equation 12 are satisfied with probability exponentially close to 1 by Chernoff bound.

Recall from the proof of Proposition 1 that $\mathsf{Shamir}(n, n, \vec{X})$ can be reduced to $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ such that $\beta_i = \prod_{m \in \{1,2,\ldots,n\} \setminus \{i\}} \frac{X_m}{X_m - X_i}$. Hwang et al. [29] showed that if $X_1, \ldots, X_n$ are chosen independently and uniformly at random, then $\beta_1, \ldots, \beta_n$ are pairwise uniform; that is, any β_i and β_j are (exponentially close to being) independent and uniform over F. Therefore, Equation 12 is satisfied with very high probability, from which we can conclude that $\mathsf{Shamir}(n, n, \vec{X})$ secure against Hamming weight leakage for almost all $\vec{X}$.

In addition, for security certification, note that the mapping $\vec{X} \mapsto \vec{\beta}$ is efficiently computable; hence, given $\vec{X}$, one can simply compute $\vec{\beta}$ from $\vec{X}$, evaluate the score of $\vec{\beta}$, and from there one can verify the security of $\vec{X}$. △

3.3 Towards Generalization (Theorem 3)

The previous two results focused on enhancing the security of additive secret sharing over the binary extension field $F = F_{2^\lambda}$ by introducing additional twists called multipliers $\vec{\beta} = (\beta_1, \ldots, \beta_n)$. It is an appealing ansatz to hope that such a relationship carries over to arbitrary fields. In this section, we prove that if Add_n is secure *in the strong sense* over F_q, then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is indeed secure over F_q as well where q is any prime power.

▶ **Theorem 3** (Diagonalization). *Let F_q be a finite field of order q. Let $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F_q^*)^n$ be multipliers and $\vec{\tau} = (\tau_1, \ldots, \tau_n)$ be the leakage. Define*

$$\mu_i := \sum_{\zeta \in F_q^*} \left(\sum_{\ell_i \in \Omega_i} \left| \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\zeta) \right| \right)^n.$$

Then,

$$\varepsilon(\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})) \leqslant \prod_{i=1}^{n} \mu_i^{1/n} \leqslant \frac{1}{n} \sum_{i=1}^{n} \mu_i \leqslant \max(\mu_1, \ldots, \mu_n)$$

Proof of Theorem 3. Let $C := \{\vec{s} \in F_q^n : \beta_1 s_1 + \cdots + \beta_n s_n = 0\}$ be the set of all shares of the secret $0 \in F_q$ in $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ (i.e. the support of the distribution $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s = 0)$). Since C is the kernel of the non-zero linear functional $\vec{s} \mapsto \beta_1 s_1 + \cdots + \beta_n s_n$, we have $C^\perp = \{\alpha \cdot (\beta_1, \ldots, \beta_n) : \alpha \in F_q\}$. Let $\vec{v}$ be an arbitrary share of the secret $1 \in F_q$. Then, for $\vec{\gamma} = \alpha \cdot (\beta_1, \ldots, \beta_n) \in C^\perp$, we have $\langle \vec{\gamma}, \vec{v} \rangle = \alpha$. Hence, from Poisson summation formula (Lemma 2), we can derive the following:

$$\begin{aligned}
&2 \cdot \mathrm{SD}\big(\vec{\tau}(s)\ ,\ \vec{\tau}(U_{F_q})\big) \\
&\quad \leqslant \sum_{\vec{\ell} \in \Omega_1 \times \cdots \times \Omega_n} \sum_{\vec{\gamma} \in C^\perp \setminus \{\vec{0}\}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\gamma_i) \right| && \text{(by triangle inequality)} \\
&\quad = \sum_{\vec{\ell} \in \Omega_1 \times \cdots \times \Omega_n} \sum_{\alpha \in F_q^*} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\alpha \beta_i) \right| && \text{(because } \langle \vec{\gamma}, \vec{v} \rangle = \alpha \text{ for } \vec{\gamma} \in C^\perp\text{)} \\
&\quad = \sum_{\alpha \in F_q^*} \prod_{i=1}^{n} \sum_{\ell_i \in \Omega_i} \left| \widehat{\mathbb{1}}_{\tau_i^{-1}(\ell)}(\alpha \beta_i) \right| && \text{(switching the order of summations)}
\end{aligned}$$

$$\leqslant \prod_{i=1}^{n}\left(\sum_{\alpha\in F_q^*}\left(\sum_{\ell_i\in\Omega_i}\left|\widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\alpha\beta_i)\right|\right)^n\right)^{1/n} \qquad \text{(by Hölder (Lemma 3))}$$

$$= \prod_{i=1}^{n}\left(\sum_{\zeta\in F_q^*}\left(\sum_{\ell_i\in\Omega_i}\left|\widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\zeta)\right|\right)^n\right)^{1/n} \qquad \text{(since } \beta_i \in F_q^*\text{)}$$

$$\leqslant \frac{1}{n}\sum_{i=1}^{n}\sum_{\zeta\in F_q^*}\left(\sum_{\ell_i\in\Omega_i}\left|\widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(\zeta)\right|\right)^n \qquad \text{(by AM-GM)}$$

◀

If we have a concrete description of the Fourier coefficients of the leakage function, this can be used to obtain tight bounds on the ℓ^n norm, which in turn yields strong security guarantees. Even in settings where a full ℓ^n norm estimation is unavailable, a bound on the second-largest Fourier coefficient is often sufficient to establish security bounds for $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$. In particular, by leveraging bounds on the second-largest coefficient, we can derive several results in the following generalized setting.

Let $\mathsf{Lin}_{n,k'}$ denote a threshold linear secret sharing scheme over F_q with n parties and reconstruction threshold k', where any subset of k' or more parties can uniquely reconstruct the secret, and any subset with fewer than k' parties gains no information. We define $\mathsf{Gen}(\mathsf{Lin}_{n,k'}, \vec{\beta})$ for $\vec{\beta} \in (F_q^*)^n$ analogously to Definition 2: the scheme first generates the shares $(s'_1, \ldots, s'_n)$ of the secret s, and then post-processes them into $(\beta_1^{-1}s'_1, \ldots, \beta_n^{-1}s'_n)$. One construction of $\mathsf{Lin}_{n,k'}$ is via Massey's secret sharing [43] instantiated with an $[n+1, k']$-MDS linear code. In this case, the shares of secret 0 form a $(k'-1)$-dimensional vector space $C_0 \subseteq F_q^n$, and the shares of any secret s form an affine shift of C_0. See [42] for a concise treatment of this concept.

▶ **Imported Theorem 1** (Benhamouda et al. [6,7] restated)**.** *Let $\mathcal{S}_{n,k'}$ be a linear n-party secret sharing scheme over a field $\mathbb{F}$ whose shares of 0 form a vector space of dimension $(k'-1)$ of $\mathbb{F}^n$. Consider $\tau_i : \mathbb{F} \to R_i$ for $i \in \{1, 2, \ldots, n\}$. Partition the indices into $[n] = I_1 \cup I_2 \cup I_3$, where I_1, I_2 each of size $n - k' + 1$. Let, C_0 denote the zero-share space of $\mathcal{S}_{n,k'}$, and $D = \{\{\zeta_i\}_{i\in I_3} : \vec{\zeta} \in C_0^{\perp}\}$. Then for any arbitrary $\vec{\beta} \in (\mathbb{F}^*)^n$, the following bound holds.*

$$\varepsilon\Big(\mathsf{Gen}(\mathcal{S}_{n,k'}; \vec{\beta}), \vec{\tau}\Big)$$
$$\leqslant \left(\prod_{j\in I_1\cup I_2}\sum_{\ell_j\in R_j}\|\mathbb{1}_{\tau_j^{-1}(\ell_j)}\|_2\right)\cdot\left(\sum_{\{\ell_j\in R_j\}_{j\in I_3}}\max_{\vec{\zeta}\in D\setminus\{\vec{0}\}}\prod_{j\in I_3}\left|\widehat{\mathbb{1}}_{\tau_j^{-1}(\ell_j)}(\beta_j\zeta_j)\right|\right)$$

From Imported Theorem 1 and using the result in [20], we could obtain the following corollary which is an extension of the result in [20] to generalized linear secret sharing scheme against Hamming weight leakage attack.

▶ **Corollary 2.** *Let $\mathsf{Lin}_{n,k'}$ be a linear secret sharing over a field $\mathbb{F} = F_p$ where p is a Mersenne prime, and $\vec{\tau} = \overrightarrow{\mathrm{wt}}$ where* wt *is the Hamming weight leakage function. Then,*

$$\varepsilon\Big(\mathsf{Gen}(\mathsf{Lin}_{n,k'}; \vec{\beta}), \overrightarrow{\mathrm{wt}}\Big) \leqslant \mathcal{O}\Big(\lambda^{\frac{5n-6k'+4}{4}}\Big)$$

in particular, for $k' - 1 \geqslant 5n/6 + c$, $\mathsf{Gen}(\mathsf{Lin}_{n,k'}; \vec{\beta})$ is $\mathcal{O}(\lambda^{-c})$-insecure against Hamming weight leakage attack.

4 Open Problems

The following are the immediate open problems in light of our work.

1. $n = 2$ *parties*.
   Our recipe of using the Fourier proxy hits a natural bottleneck when $n = 2$. Even using the most optimistic estimates of Krawtchouk polynomial evaluations, Appendix E.3 demonstrates that our approach cannot prove the security for $n = 2$ case. New technical machinery is required for this case.
2. *Attacks*.
   We proved that if our minimum score of $\vec{\beta}$ is large then it is sufficient to prove the security of the scheme. Is high minimum score also necessary? More concretely, given a vector of multipliers $\vec{\beta}$, does the insecurity of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ surpass a specific insecurity budget ε?
3. *Prime modulus*.
   The case of Hamming weight leakage for Mersenne prime modulus was explored by Faust et al. [20] when $n \geqslant 5$. The cases of general primes and, even for Mersenne primes, $n \in \{2, 3, 4\}$ remains open.

References

1 Donald Q. Adams, Hemanta K. Maji, Hai H. Nguyen, Minh L. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Lower bounds for leakage-resilient secret-sharing schemes against probing attacks. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 976–981, 2021. doi:10.1109/ISIT45174.2021.9518230.

2 Sergey V. Agievich. An upper bound on binomial coefficients in the de moivre-laplace form. *Journal of the Belarusian State University. Mathematics and Informatics (In Russian)*, page 66–74, 2022. English translation available online as arXiv:2205.07120. doi:10.33581/2520-6508-2022-1-66-74.

3 Josep Balasch, Sebastian Faust, and Benedikt Gierlichs. Inner product masking revisited. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 486–510, Sofia, Bulgaria, April 26–30, 2015. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-46800-5_19.

4 Josep Balasch, Sebastian Faust, Benedikt Gierlichs, Clara Paglialonga, and François-Xavier Standaert. Consolidating inner product masking. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 724–754, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland. doi:10.1007/978-3-319-70694-8_25.

5 Mihir Bellare. The spectral norm of finite functions. Technical Report MIT-LCS-TR-495, MIT, Feb 1991.

6 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.

7 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.

8 Peter B Borwein. On the complexity of calculating factorials. *Journal of Algorithms*, 6(3):376–380, 1985.

9 Jean Bourgain. On the distribution of the fourier spectrum of boolean functions. *Israel Journal of Mathematics*, 131(1):269–276, 2002.

10 Luís T. A. N. Brandão and René Peralta. NIST IR 8214C: NIST first call for multi-party threshold schemes. https://csrc.nist.gov/pubs/ir/8214/c/ipd, Jan 25, 2023.

11 Richard P Brent and Paul Zimmermann. *Modern computer arithmetic*, volume 18. Cambridge University Press, 2010.

12 Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412, Santa Barbara, CA, USA, August 15–19, 1999. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-48405-1_26.

13 Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. John Wiley & Sons, 1999.

14 Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen. *Secure multiparty computation and secret sharing*. Cambridge University Press, 2015.

15 Diego Dominici. Asymptotic analysis of the krawtchouk polynomials by the WKB method. *The Ramanujan Journal*, 15:303–338, 2008. doi:10.1007/s11139-007-9078 -9.

16 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.

17 Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete - or how to evaluate the security of any leaking device. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 401–429, Sofia, Bulgaria, April 26–30, 2015. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-46800-5_16.

18 François Durvaux, François-Xavier Standaert, and Santos Merino Del Pozo. Towards easy leakage certification. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *Cryptographic Hardware and Embedded Systems – CHES 2016*, volume 9813 of *Lecture Notes in Computer Science*, pages 40–60, Santa Barbara, CA, USA, August 17–19, 2016. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-662-53140-2_3.

19 François Durvaux, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. How to certify the leakage of a chip? In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 459–476, Copenhagen, Denmark, May 11–15, 2014. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-55220-5_26.

20 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.

21 Sebastian Faust, Loïc Masure, Elena Micheli, Hai Hoang Nguyen, Maximilian Orlt, and François-Xavier Standaert. IP masking with generic security guarantees under minimum assumptions, and applications. In *31st International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2025*, December 8–12 2025.

22 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.

23 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.

24 Louis Goubin and Jacques Patarin. DES and differential power analysis (the "duplication" method). In Çetin Kaya Koç and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES'99*, volume 1717 of *Lecture Notes in Computer Science*, pages 158–172, Worcester, Massachusetts, USA, August 12–13, 1999. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-48059-5_15.

25 Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Longman Publishing Co., Inc., USA, 2nd edition, 1994.

26 Loıc Grenié and Giuseppe Molteni. Inequalities for the beta function. *Math. Inequal. Appl*, 18(4):1427–1442, 2015. doi:10.7153/mia-18-111.

27 Jonathan I Hall. Notes on coding theory, 2003. URL: https://users.math.msu.edu/users/halljo/classes/CODENOTES/CODING-NOTES.HTML.

28 G. H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities*. Cambridge Mathematical Library. Cambridge University Press, 1952.

29 Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, and Xiuyu Ye. Leakage-resilience of shamir's secret sharing: Identifying secure evaluation places. In *6th Conference on Information Theoretic Cryptography (ITC 2025)*, Aug 2025. doi:10.4230/LIPIcs.ITC.2025.3.

30 Norman L Johnson, Adrienne W Kemp, and Samuel Kotz. *Univariate discrete distributions*. John Wiley & Sons, 2005.

31 Dustin Kasser. An improvement upon the bounds for the local leakage resilience of shamir's secret sharing scheme. In Elette Boyle and Mohammad Mahmoody, editors, *TCC 2024: 22nd Theory of Cryptography Conference, Part IV*, volume 15367 of *Lecture Notes in Computer Science*, pages 395–422, Milan, Italy, December 2–6, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-78023-3_13.

32 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.

33 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.

34 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.

35 Mihail N. Kolountzakis, Richard J. Lipton, Evangelos Markakis, Aranyak Mehta, and Nisheeth K. Vishnoi. On the fourier spectrum of symmetric boolean functions. *Combinatorica*, 29:363–387, Jul 2009. doi:10.1007/s00493-009-2310-z.

36 Ilia Krasikov. Nonnegative quadratic forms and bounds on orthogonal polynomials. *Journal of Approximation Theory*, 111(1):31–49, Jul 2001. doi:10.1006/jath.2001.3570.

37 Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. North-Holland Publishing Company, 1977.

38 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 Crypto-*

logy – 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.

39 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.

40 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 *IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, June 26 - July 1, 2022*, pages 2678–2683. IEEE, 2022. doi:10.1109/ISIT50566.2022.9834695.

41 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.

42 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.

43 James L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

44 Colin McDiarmid. *Concentration*, pages 195–248. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998. doi:10.1007/978-3-662-12788-9_6.

45 Hai H. Nguyen. Towards breaking the half-barrier of local leakage-resilient shamir's secret sharing. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part V*, volume 14924 of *Lecture Notes in Computer Science*, pages 257–285, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-68388-6_10.

46 Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2021. Available online as arXiv:2105.10386v1.

47 Ryan O'Donnell, John Wright, and Yuan Zhou. The fourier entropy–influence conjecture for certain classes of boolean functions. In *International Colloquium on Automata, Languages, and Programming*, pages 330–341. Springer, 2011. doi:10.1007/978-3-642-22006-7_28.

48 Jean-Christophe Pain. On an upper bound for central binomial coefficients and catalan numbers. *arXiv preprint arXiv:2407.21064*, 2024.

49 Emmanuel Prouff and Thomas Roche. Higher-order glitches free implementation of the AES using secure multi-party computation protocols. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 63–78, Nara, Japan, September 28 – October 1, 2011. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-642-23951-9_5.

50 Zoltán Sasvári. Inequalities for binomial coefficients. *Journal of Mathematical Analysis and Applications*, 236(1):223–226, Aug 1999. doi:10.1006/jmaa.1999.6420.

51 Amir Shpilka and Avishay Tal. On the minimal fourier degree of symmetric boolean functions. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 200–209. IEEE, 2011. doi:10.1109/CCC.2011.16.

52 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.

53 Terence Tao. *Topics in random matrix theory*, volume 132. American Mathematical Soc., 2012.

54 Flemming Topsøe. Some bounds for the logarithmic function. In Yeol Je Cho, Jong Kyu Kim, and Sever S. Dragomir, editors, *Inequality theory and applications*, volume 4, pages 137–151. Nova Science Publishers, 2007.

55 Jacobus Hendricus van Lint. *Introduction to coding theory*, volume 86. Springer Science & Business Media, 1998.

56 Joachim von zur Gathen and Victor Shoup. Computing frobenius maps and factoring polynomials. *Computational Complexity*, 2:187–224, Sep 1992.

57 Shengxin Zhu. Summation of gaussian shifts as jacobi's third theta function. *arXiv preprint arXiv:1806.08474*, 2018.

A Proof of Technical Lemmas (Lemma 4 and 5)

▶ **Claim 3.** *For all* $\lambda \in \{1, 2, \dots\}$, $w \in \{1, 2, \dots, \lambda\}$, *and* $\zeta \in F$,

$$\widehat{\mathbb{1}}_w(\zeta) = \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}^\vee(\zeta)} (-1)^k \binom{\mathrm{wt}^\vee(\zeta)}{k} \binom{\lambda - \mathrm{wt}^\vee(\zeta)}{w-k}$$

Proof of Claim 3. By definition of Fourier transformation (see Section 2.4),

$$\begin{aligned}
\widehat{\mathbb{1}}_w(\zeta) &:= \frac{1}{2^\lambda} \sum_{x \in F} \mathbb{1}_w(x) \cdot (-1)^{\langle \zeta^\vee, x \rangle} \\
&= \frac{1}{2^\lambda} \sum_{\substack{x \in F \\ \mathrm{wt}(x) = w}} (-1)^{\langle \zeta^\vee, x \rangle} \\
&= \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}(\zeta^\vee)} (-1)^k \cdot \mathrm{card}(\{x \colon \mathrm{wt}(x) = w,\ \mathrm{card}(\mathrm{Supp}(\zeta^\vee) \cap \mathrm{Supp}(x)) = k\})
\end{aligned}$$

Let us count the number of $x \in \mathrm{wt}^{-1}(w) \subseteq F$ that satisfies $|\mathrm{Supp}(\zeta^\vee) \cap \mathrm{Supp}(x)| = k$, given $k \in [0, \mathrm{wt}^\vee(\zeta)]$. $\zeta^\vee$ has $\mathrm{wt}^\vee(\zeta)$-many 1's in its binary representation (recall $\mathrm{wt}(\zeta^\vee) = \mathrm{wt}^\vee(\zeta)$). In order for $x \in F$ to give $|\mathrm{Supp}(\zeta^\vee) \cap \mathrm{Supp}(x)| = k$, it should have k-many overlapping 1's with $\zeta^\vee$. Its remaining $(w-k)$-many 1's can lie anywhere outside the digits where $\zeta^\vee$ has a 1 in it (because otherwise it will induce more overlapping 1's, making $\langle \zeta^\vee, x \rangle$ greater than k). Hence,

$$\mathrm{card}(\{x \colon \mathrm{wt}(x) = w,\ \mathrm{card}(\mathrm{Supp}(\zeta^\vee) \cap \mathrm{Supp}(x)) = k\}) = \binom{\mathrm{wt}^\vee(\zeta)}{k} \binom{\lambda - \mathrm{wt}^\vee(\zeta)}{w-k}$$

and therefore,

$$\widehat{\mathbb{1}}_w(\zeta) = \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}^\vee(\zeta)} (-1)^k \binom{\mathrm{wt}^\vee(\zeta)}{k} \binom{\lambda - \mathrm{wt}^\vee(\zeta)}{w-k}$$

as desired. ◀

▶ Remark 9. Observe from Claim 3 above that the value of $\widehat{\mathbb{1}}_w(\zeta)$ depends only on w and $\mathrm{wt}^\vee(\zeta) = \mathrm{wt}(\zeta^\vee)$, i.e. $\widehat{\mathbb{1}}_w(\zeta)$ is a *symmetric function* in the sense that it is invariant to the permutation of digits of $\zeta^\vee$. This is not an unexpected outcome because $\widehat{\mathbb{1}}_w(x)$ is a symmetric Boolean function itself, and Fourier transform of symmetric Boolean function over Boolean hypercube should also be symmetric (see [35, 47, 51], for more details). △

▶ **Claim 1.** *For all* $\lambda \in \{1, 2, \dots\}$, $w \in \{1, 2, \dots, \lambda\}$, *and* $\zeta \in F$,

$$\begin{aligned}
\left|\widehat{\mathbb{1}}_w(\zeta)\right| &\leqslant \frac{1}{2^{\lambda/2}} \binom{\lambda}{w}^{1/2} \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2} \leqslant \frac{1}{\lambda^{1/4}} \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-\frac{1}{2}} && \text{if } \zeta \notin \{0, \zeta^*\} \\
\left|\widehat{\mathbb{1}}_w(\zeta)\right| &= \frac{1}{2^\lambda} \binom{\lambda}{w} \leqslant \frac{1}{\sqrt{\lambda}} && \text{if } \zeta \in \{0, \zeta^*\}
\end{aligned}$$

Proof of Claim 1. Binomial coefficients are upper bounded by the central binomial coefficient, which can be then upper bounded as follows: for all $w \in \{1, 2, \dots, \lambda\}$,

$$\binom{\lambda}{w} \leqslant \binom{\lambda}{\lfloor \lambda/2 \rfloor} \leqslant \frac{2^\lambda}{\sqrt{\pi\lambda/2}} \leqslant \frac{2^\lambda}{\sqrt{\lambda}} \tag{26}$$

This immediately implies the required upper bound for $\zeta = 0$:

$$\widehat{\mathbb{1}}_w(\zeta) = \frac{1}{2^\lambda}\binom{\lambda}{w} \leqslant \frac{1}{\sqrt{\lambda}}$$

Similarly for $\zeta = \zeta^*$, we obtain the required upper bound using the following identity.

$$\left|\widehat{\mathbb{1}}_w(\zeta^*)\right| = \frac{1}{\mathrm{card}(F)}\left|\sum_{x\in F} \mathbb{1}_w(x)\cdot(-1)^{\mathrm{wt}(x)}\right| = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x) = \widehat{\mathbb{1}}_w(0)$$

Now consider an arbitrary $\zeta \in F^*$. Note that Parseval's identity (Fact 1) states

$$\sum_{\alpha\in F}\widehat{\mathbb{1}}_w(\alpha)^2 = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x)^2 \tag{27}$$

Simplifying the left-hand side of Equation 27, we get

$$\frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x)^2 = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x) = \frac{1}{2^\lambda}\binom{\lambda}{w}$$

For the right-hand side of Equation 27, note that, for any $\zeta \in F^*$,

$$\begin{aligned}\sum_{\alpha\in F}\widehat{\mathbb{1}}_w(\alpha)^2 = \sum_{\alpha\in F}\left|\widehat{\mathbb{1}}_w(\alpha)\right|^2 &\geqslant \sum_{\substack{\alpha\in F \text{ s.t.}\\ \mathrm{wt}^\vee(\alpha)=\mathrm{wt}^\vee(\zeta)}}\left|\widehat{\mathbb{1}}_w(\alpha)\right|^2 \\ &= \sum_{\substack{\alpha\in F \text{ s.t.}\\ \mathrm{wt}^\vee(\alpha)=\mathrm{wt}^\vee(\zeta)}}\left|\widehat{\mathbb{1}}_w(\zeta)\right|^2 = \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}\left|\widehat{\mathbb{1}}_w(\zeta)\right|^2\end{aligned}$$

where the last two equalities come from the observation made in Remark 9. Putting these into Equation 27 then gives us the following:

$$\begin{aligned}\sum_{\alpha\in F}\widehat{\mathbb{1}}_w(\alpha)^2 = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x)^2 &\implies \frac{1}{2^\lambda}\binom{\lambda}{w} \geqslant \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}\left|\widehat{\mathbb{1}}_w(\zeta)\right|^2 \\ &\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \frac{1}{2^{\lambda/2}}\binom{\lambda}{w}^{1/2}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2} \\ &\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \frac{1}{\lambda^{1/4}}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2} \quad (\because \text{Equation 26})\end{aligned}$$

as desired. ◀

▶ **Lemma 4.** *For $\lambda \geqslant 2$, $w \in \{1,\ldots,\lambda\}$, and $\zeta \in F$, we have $|\widehat{\mathbb{1}}_w(\zeta)| \leqslant B(\zeta)$ where*

$$B(\zeta) := \begin{cases}\lambda^{-1/2}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{0,\lambda\}\\ \lambda^{-1}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{1,\lambda-1\}\\ 4\cdot\lambda^{-3/2}, & \text{if } \mathrm{wt}^\vee(\zeta) \in \{2,\lambda-2\}\\ \lambda^{-\frac{1}{4}}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-\frac{1}{2}}, & \text{otherwise.}\end{cases}$$

And hence,

$$\sum_{\mathrm{wt}^\vee(\zeta)=1}^{\lambda-1}(B(\zeta))^n \leqslant 3\cdot 5^{\frac{5n}{2}-4}\cdot\lambda^{-n+1}$$

Proof of Lemma 4. For brevity let us denote $\mathrm{wt}^*(\zeta) := \min\{\mathrm{wt}^\vee(\zeta), \lambda - \mathrm{wt}^\vee(\zeta)\}$. The cases where $\mathrm{wt}^*(\zeta) = 0$ and $\mathrm{wt}^*(\zeta) \geqslant 2$ follow from Claim 1.

Let us first prove for the case $\mathrm{wt}^*(\zeta) = 1$. Recall from Claim 3 that if $\mathrm{wt}^\vee(\zeta) = 1$,

$$2^\lambda \cdot \widehat{\mathbb{1}}_w(\zeta) = \sum_{k=0}^{1} (-1)^k \binom{1}{k}\binom{\lambda-1}{w-k} = \binom{\lambda-1}{w} - \binom{\lambda-1}{w-1} = \binom{\lambda}{w}\left(\frac{\lambda-2w}{\lambda}\right) \tag{28}$$

$$\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \sqrt{\frac{2}{\pi\lambda}} \cdot \exp\left(-\frac{2\cdot(\lambda/2-w)^2}{\lambda+1}\right) \cdot \frac{|\lambda-2w|}{\lambda} \qquad \text{(by Corollary 3)}$$

$$\leqslant \sqrt{\frac{4}{\pi \mathrm{e}}} \cdot \frac{1}{\lambda} \leqslant \frac{1}{\lambda} \qquad \text{(by Corollary 4)}$$

Then, we have

$$\sum_{\mathrm{wt}^*(\zeta)=1} (B(\zeta))^n = 2 \cdot \binom{\lambda}{1} \cdot \left(\frac{1}{\lambda}\right)^n \leqslant 2 \cdot \lambda^{-n+1}$$

Similarly, for $\mathrm{wt}^*(\zeta) = 2$ case,

$$2^\lambda \cdot \widehat{\mathbb{1}}_w(\zeta) = \binom{\lambda}{w}\frac{(\lambda-2w)^2-\lambda}{\lambda(\lambda-1)} \tag{29}$$

$$\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \sqrt{\frac{2}{\pi\lambda}} \cdot \exp\left(-\frac{2\cdot(\lambda/2-w)^2}{\lambda+1}\right) \cdot \frac{\left|(\lambda-2w)^2-\lambda\right|}{\lambda(\lambda-1)} \qquad \text{(by Corollary 3)}$$

$$\leqslant \sqrt{\frac{2}{\pi}} \cdot \left(\frac{6}{\mathrm{e}} + 2\right) \cdot \frac{1}{\lambda^{3/2}} \leqslant 4 \cdot \lambda^{-3/2} \qquad \text{(by Corollary 4)}$$

and we get

$$\sum_{\mathrm{wt}^*(\zeta)=2} (B(\zeta))^n = 2 \cdot \binom{\lambda}{2} \cdot \left(4 \cdot \lambda^{-3/2}\right)^n \leqslant 4^n \cdot \lambda^{-\frac{3n}{2}+2}$$

For the remaining parts of the sum of $(B(\zeta))^n$, consider the following.

$$\begin{aligned}
\sum_{\mathrm{wt}^\vee(\zeta)=3}^{\lambda-3} (B(\zeta))^n &= 2 \cdot \sum_{\mathrm{wt}^*(\zeta)\geqslant 3} (B(\zeta))^n \\
&= 2 \cdot \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{3}^{-\frac{n}{2}+1} + 2 \cdot \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{4}^{-\frac{n}{2}+1} + 2 \cdot \sum_{k=5}^{\lambda/2} \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{k}^{-\frac{n}{2}+1} \\
&\leqslant 2 \cdot \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{3}^{-\frac{n}{2}+1} + 2 \cdot \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{4}^{-\frac{n}{2}+1} + 2 \cdot \frac{\lambda}{2} \cdot \lambda^{-\frac{n}{4}} \cdot \binom{\lambda}{5}^{-\frac{n}{2}+1} \\
&\leqslant 3^{\frac{3n}{2}-2} \cdot \lambda^{-n/4} \cdot \lambda^{-\frac{3n}{2}+3} + 4^{2n-3} \cdot \lambda^{-n/4} \cdot \lambda^{-2n+4} \\
&\qquad + 5^{\frac{5n}{2}-5} \cdot \lambda^{-n/4+1} \cdot \lambda^{-\frac{5n}{2}+5} \\
&= 3^{\frac{3n}{2}-2} \cdot \lambda^{-\frac{7n}{4}+3} \;+\; 4^{2n-2} \cdot \lambda^{-\frac{9n}{4}+4} \;+\; 5^{\frac{5n}{2}-5} \cdot \lambda^{-\frac{11n}{4}+6} \\
&\leqslant 5^{\frac{5n}{2}-4} \cdot \lambda^{-\frac{7n}{4}+3}
\end{aligned}$$

Therefore, comparing it with the previous expression, we obtain:

$$\begin{aligned}
\sum_{\mathrm{wt}^\vee(\zeta)=1}^{\lambda-1} (B(\zeta))^n &\leqslant \underbrace{2 \cdot \lambda^{-n+1}}_{\text{Signal}} + \underbrace{4^n \cdot \lambda^{-\frac{3n}{2}+2}}_{\text{Medium}} + \underbrace{5^{\frac{5n}{2}-4} \cdot \lambda^{-\frac{7n}{4}+3}}_{\text{Noise}} \\
&\leqslant 3 \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{-n+1} \quad \left(\text{as } n-1 < \tfrac{3n}{2}-2 \text{ and } n-1 < \tfrac{7n}{4}-3 \text{ for } n \geqslant 3\right)
\end{aligned}$$

as desired. ◀

From Lemma 4, note that

$$\begin{aligned}\left(2\lambda^{1/2+\tau}\right)^n \sum_{\zeta\in F\setminus\{0,\zeta^*\}} B(\zeta)^n &= 2^n\cdot\lambda^{n/2+n\tau}\cdot\sum_{\mathrm{wt}^\vee(\zeta)=1}^{\lambda-1}(B(\zeta))^n\\ &\leqslant 3\cdot 5^{\frac{5n}{2}-4}\cdot(2\lambda^\tau)^n\cdot\lambda^{-\frac{n}{2}+1}\\ &\leqslant 2^n\cdot 5^{\frac{5n}{2}-3}\cdot\lambda^{\tau n}\cdot\lambda^{-\frac{n}{2}+1}\end{aligned}$$

which is small for sufficiently large λ when $n\geqslant 3$.

▶ **Lemma 5.** *For any $\vec{\beta}=(\beta_1,\beta_2,\dots,\beta_n)\in(F^*)^n$ and $\vec{w}=(w_1,w_2,\dots,w_n)\in\{1,2,\dots,\lambda\}^n$,*

$$\prod_{i=1}^n\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\leqslant\lambda^{-\frac{n}{2}}\cdot\exp\left(-\mathsf{Score}(\zeta;\vec{\beta})\right)$$

Proof of Lemma 5. If $\mathrm{wt}^\vee(\beta_i\zeta)\notin\{0,\lambda\}$, by Claim 1 (or Lemma 4),

$$\begin{aligned}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| &\leqslant \frac{1}{\lambda^{1/4}}\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}^{-1/2}=\frac{1}{\lambda^{1/2}}\cdot\frac{1}{\lambda^{-1/4}}\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}^{-1/2}\\ &\leqslant\lambda^{-1/2}\cdot\exp\left(-\frac{1}{2}\log\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}+\frac{\log\lambda}{4}\right)\end{aligned}$$

Otherwise, we have $|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)|\leqslant\lambda^{-1/2}$. Set $h^*:=\mathrm{card}(\{i\colon\mathrm{wt}^\vee(\beta_i\zeta)\in\{0,\lambda\}\})$. Then,

$$\begin{aligned}\prod_{i=1}^n\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| &= \left(\prod_{i\colon\mathrm{wt}^\vee(\beta_i\zeta)\in\{0,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right)\cdot\left(\prod_{i\colon\mathrm{wt}^\vee(\beta_i\zeta)\notin\{0,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right)\\ &\leqslant\lambda^{-\frac{h^*}{2}}\cdot\left(\prod_{i\colon\mathrm{wt}^\vee(\beta_i\zeta)\notin\{0,\lambda\}}\lambda^{-\frac{1}{2}}\cdot\exp\left(-\frac{1}{2}\log\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}+\frac{\log\lambda}{4}\right)\right)\\ &=\lambda^{-\frac{h^*}{2}}\cdot\lambda^{-\frac{(n-h^*)}{2}}\cdot\exp\left(-\sum_{i\colon\mathrm{wt}^\vee(\beta_i\zeta)\notin\{0,\lambda\}}\left(\frac{1}{2}\log\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}-\frac{\log\lambda}{4}\right)\right)\\ &=\lambda^{-\frac{n}{2}}\cdot\exp\left(-\sum_{i=1}^n\sigma(\mathrm{wt}^\vee(\beta_i\zeta))\right)\qquad\text{(see Equation 2)}\\ &=\lambda^{-\frac{n}{2}}\cdot\exp\left(-\mathsf{Score}(\zeta;\vec{\beta})\right)\qquad\text{(see Equation 3)}\end{aligned}$$

as desired. ◀

B Binomial Coefficients Estimations

We aim to prove a de Moivre-Laplace form (a.k.a., Gaussian-looking) upper bound on the binomial coefficients similar to Agievich [2] and Pain [48], which will simplify our analysis later.

▶ **Corollary 3** (Binomial Coefficient Estimation). *For any $a\in\{1,2,\dots\}$ and $b\in\{0,1,\dots,a\}$, the following bound holds.*

$$\binom{a}{b}\leqslant\frac{2^a}{\sqrt{\pi\cdot(a/2)}}\cdot\exp\left(-2\cdot\frac{(b-a/2)^2}{a+1}\right)$$

This result will follow straightforwardly from Lemma 6 and Lemma 7 that prove the result for even and odd a, respectively.[3] Chernoff bound immediately yields the bound

$$\binom{a}{b} \leqslant 2^a \cdot \exp\left(-2 \cdot \frac{(b-a/2)^2}{a}\right)$$

Our upper bound is tighter by a multiplicative factor of $\mathcal{O}\left(a^{-1/2}\right)$.

▶ **Lemma 6.** *For $n \in \{1, 2, \dots\}$ and $x \in \{0, 1, \dots, n\}$ the following bounds hold*

$$\binom{2n}{n-x} \leqslant \binom{2n}{n} \cdot \exp\left(-\frac{x^2}{n+1/2}\right) \leqslant \frac{2^{2n}}{\sqrt{\pi n}} \cdot \exp\left(-\frac{x^2}{n+1/2}\right)$$

By the Central Limit Theorem, we expect, for fixed x/n,

$$\binom{2n}{n-x} \to \binom{2n}{n} \cdot \exp\left(-\frac{x^2}{n}\right) \qquad \text{as } n \to \infty$$

Berry-Esseen [53, Chapter 2.2] and Camp-Paulson [30, Chapter 3.6], for example, additively bound the gap between these two distributions. This lemma will prove a de Moivre-Laplace form upper bound instead.

Proof of Lemma 6. We will use the following fact for the proof of our lemma:

▶ **Claim 4.** *For $x \in (0, 1]$, we have $x \leqslant \exp\left(-2 \cdot \frac{1-x}{1+x}\right)$.*

Proof of Claim 4. Substituting $t = 1 - x$, the inequality is equivalent to

$$\ln(1-t) \leqslant -\frac{t}{1-t/2} = \sum_{i \geqslant 1} -\frac{t^i}{2^{i-1}},$$

which is true by inspection. ◀

Topsøe presents tighter bounds in [54]. Our upper bound is equivalent to lower bounding $\ln(1+x)$, for $x \in [0, \infty)$. The bound above corresponds to the lower bound ϕ_1 in [54, Table 1]. In general, such bounds are a consequence of the identity [54, Equation 28].

Now, for the proof of our lemma, consider the following manipulation:

$$\begin{aligned}
\binom{2n}{n-x} &= \binom{2n}{n} \cdot \frac{(n-x+1)\cdots n}{(n+1)\cdots(n+x)} = \binom{2n}{n} \cdot \prod_{i=1}^{x} \frac{n-x+i}{n+x-i+1} && \text{(rearranging)} \\
&\leqslant \binom{2n}{n} \cdot \prod_{i=1}^{x} \exp\left(-2 \cdot \frac{2x-2i+1}{2n+1}\right) && \text{(using Claim 4)} \\
&= \binom{2n}{n} \cdot \exp\left(-2 \cdot \frac{2x^2 - x(x+1) + x}{2n+1}\right) \\
&= \binom{2n}{n} \cdot \exp\left(-\frac{x^2}{n+1/2}\right).
\end{aligned}$$

The final part of the result follows from Fact 3 below.

[3] This result also translates into a lower bound for Euler's Beta function, c.f. [26], improving the lower bound when the two input parameters to Euler's Beta function are close.

▶ **Fact 3.** *For* $n \in \{1, 2, \dots\}$, $\binom{2n}{n} \leqslant \frac{2^{2n}}{\sqrt{\pi n}}$.

Tighter estimates are possible (for example, [50, Corollary 1]); however, for our application, this elementary estimate suffices. This completes the proof of Lemma 6. ◀

▶ **Lemma 7.** *For* $n \in \{1, 2, \dots\}$ *and* $x \in \{0, 1, \dots, n\}$ *the following bounds hold*

$$\binom{2n+1}{n-x} \leqslant \binom{2n+1}{n} \cdot \exp\left(-\frac{x(x+1)}{n+1}\right) \leqslant \frac{2^{2n+1}}{\sqrt{\pi(n+1/2)}} \cdot \exp\left(-\frac{(x+1/2)^2}{n+1}\right)$$

Proof of Lemma 7. By similar reasoning as in the proof of Lemma 6,

$$\begin{aligned}
\binom{2n+1}{n-x} &= \binom{2n+1}{n} \frac{(n-x+1)\cdots n}{(n+2)\cdots(n+x)} = \binom{2n+1}{n} \prod_{i=1}^{x} \frac{n-x+i}{n+x+2-i} \\
&\leqslant \binom{2n+1}{n} \prod_{i=1}^{x} \exp\left(-2 \cdot \frac{2(x+1-i)}{2n+2}\right) && \text{(by Claim 4)} \\
&= \binom{2n+1}{n} \exp\left(-\sum_{i=1}^{x} \frac{2(x+1-i)}{n+1}\right) \\
&= \binom{2n+1}{n} \exp\left(-\frac{x(x+1)}{n+1}\right) && \text{(proves the first part of the lemma)} \\
&= \frac{1}{2} \cdot \binom{2n+2}{n+1} \cdot \exp\left(-\frac{x(x+1)}{n+1}\right) \\
&\leqslant \frac{2^{2n+1}}{\sqrt{\pi(n+1)}} \cdot \exp\left(-\frac{x(x+1)}{n+1}\right) && \text{(by Fact 3)} \\
&= \frac{2^{2n+1}}{\sqrt{\pi(n+1)}} \cdot \exp\left(-\frac{(x+1/2)^2}{n+1}\right) \cdot \exp\left(\frac{1}{4(n+1)}\right) && \text{(completing the square)} \\
&= \frac{2^{2n+1}}{\sqrt{\pi(n+1/2)}} \cdot \exp\left(-\frac{(x+1/2)^2}{n+1}\right) \cdot \sqrt{\frac{n+1/2}{n+1} \cdot \exp\left(\frac{1}{2(n+1)}\right)} \\
&= \frac{2^{2n+1}}{\sqrt{\pi(n+1/2)}} \cdot \exp\left(-\frac{(x+1/2)^2}{n+1}\right) \cdot \sqrt{\left(1 - \frac{1}{2(n+1)}\right) \cdot \exp\left(\frac{1}{2(n+1)}\right)} \\
&\leqslant \frac{2^{2n+1}}{\sqrt{\pi(n+1/2)}} \cdot \exp\left(-\frac{(x+1/2)^2}{n+1}\right). && \text{(because } 1-\theta \leqslant \exp(-\theta)\text{)}
\end{aligned}$$

This completes the proof of the second inequality. ◀

B.1 Estimating Sum of Powers of Binomial Coefficients

▶ **Claim 5.** *For arbitrary* $\theta \in \mathbb{R}$ *and* $m \in \mathbb{R}_{>0}$, *the following bound holds.*

$$\sum_{\Delta \in \theta + \mathbb{Z}} \exp\left(-\frac{\Delta^2}{m}\right) \leqslant \sqrt{\pi m} + 1.$$

This upper bound admits an elementary proof for all m, which we present below. For large m, significantly tighter bounds could be derived by connecting this sum to the third Jacobi theta function. For example, [57, Theorem 2.2] proved the following estimate.

$$\left| \frac{1}{\sqrt{\pi m}} \sum_{\Delta \in \theta + \mathbb{Z}} \exp\left(-\frac{\Delta^2}{m}\right) - 1 \right| \leqslant \operatorname{csch}(\pi^2 m).$$

Proof of Claim 5. We will use the property that $\exp(-x^2/m)$ is decreasing for $x \geqslant 0$ and the fact that $\int_{-\infty}^{\infty} \exp(-t^2/m)\mathrm{d}t = \sqrt{\pi m}$. Because $\exp(-x^2/m)$ is even and the LHS is periodic in θ (with period 1), it suffices to consider $\theta \in [0, 1/2]$. For brevity, denote $f(\Delta) = \exp\left(-\Delta^2/m\right)$ and $\overline{\theta} = (1-\theta)$. Then,

$$\begin{aligned}
&\sum_{\Delta \in \theta + \mathbb{Z}} \exp\left(-\frac{\Delta^2}{m}\right) \\
&= \left(\theta f(\theta) + \sum_{\Delta \in \{1+\theta, 2+\theta, \dots\}} f(\Delta)\right) + \left(\overline{\theta} f(-\overline{\theta}) + \sum_{\Delta \in \{-\overline{\theta}-1, -\overline{\theta}-2, \dots\}} f(\Delta)\right) \\
&\qquad + \overline{\theta} f(\theta) + \theta f(-\overline{\theta}) \\
&\leqslant \int_0^{\infty} f(t)\mathrm{d}t + \int_{-\infty}^{0} f(t)\mathrm{d}t + \overline{\theta} \cdot f(0) + \theta \cdot f(0) \\
&\leqslant \sqrt{\pi m} + 1.
\end{aligned}$$

This completes the proof of the claim. ◀

▶ Remark 10. We can prove the tighter bound

$$\sum_{\Delta \in \theta + \mathbb{Z}} \exp\left(-\frac{\Delta^2}{m}\right) \leqslant \sqrt{\pi m} + \exp\left(-\frac{\widehat{\theta}^2}{m}\right),$$

where $\widehat{\theta} \in [0, 1/2]$ is the distance of θ from $\mathbb{Z}$, i.e., $\min_{i \in \mathbb{Z}} |\theta - i|$. △

▶ **Claim 2.** *For $m \in \{1, 2, \dots\}$, the following bound holds.*

$$\sum_{i=0}^{m} \binom{m}{i}^{1/2} < \pi \cdot m^{1/4} \cdot 2^{m/2}.$$

Proof of Claim 2. Consider the following manipulation.

$$\begin{aligned}
\sum_{i=0}^{m} \binom{m}{i}^{1/2} &\leqslant \frac{2^{m/2}}{(\pi m/2)^{1/4}} \sum_{i=0}^{m} \exp\left(-\frac{(i-m/2)^2}{m+1}\right) && \text{(using Corollary 3)} \\
&\leqslant \frac{2^{m/2}}{(\pi m/2)^{1/4}} \cdot \left(1 + \sqrt{\pi(m+1)}\right) && \text{(using Claim 5)} \\
&\leqslant 2^{m/2} \cdot \left(\max_{t \geqslant 1} \frac{1 + \sqrt{\pi(t+1)}}{(\pi t/2)^{1/4}} \cdot \frac{1}{t^{1/4}}\right) \cdot m^{1/4}
\end{aligned}$$

The maximum is achieved at $t = 1$ and the value is $(2/\pi)^{1/4} + 2 \cdot (\pi/2)^{1/4} < 3.14 < \pi$. ◀

▶ Remark 11. In general, for $p \in (0, 1]$, we can prove that

$$\sum_{i=0}^{m} \binom{m}{i}^{p} \leqslant \frac{2^{pm}}{(\pi m/2)^{p/2}} \cdot \left(1 + \sqrt{\frac{\pi(m+1)}{2p}}\right) \leqslant \sqrt{2} \cdot (1 + \pi^{-1/2}) \cdot \frac{1}{\sqrt{p}} \cdot 2^{pm} \cdot m^{(1-p)/2}$$

△

C Concrete Upper Bound on Krawtchouk Polynomials

▶ **Claim 6.** *For $a \in \mathbb{R}_{>0}$ and $x, k \in \mathbb{R}_{\geqslant 0}$, the following bound holds*

$$\exp\left(-\frac{x^2}{a}\right) \cdot x^k \leqslant \begin{cases} 1, & \text{if } k = 0. \\ \left(\frac{ka}{2\mathrm{e}}\right)^{k/2}, & \text{otherwise.} \end{cases}$$

Proof. We first maximize $-\frac{x^2}{a} + k \cdot \ln x$. It is maximized at $x^2 = ka/2$. Therefore, $\exp(-x^2/a) \cdot x^k \leqslant \exp(-k/2) \cdot (ka/2)^{k/2}$. ◀

The following estimates follow immediately from Claim 6.

▶ **Corollary 4.** *For $x \in \mathbb{R}_{\geqslant 0}$ and $m \in \mathbb{Z}$, the following bounds hold.*

1. *For $m \geqslant 1$:*
$$\exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{2x}{m} \leqslant \frac{2^{1/2}}{\mathrm{e}^{1/2}} \cdot \frac{1}{m^{1/2}}.$$
2. *For $m \geqslant 2$:*
$$\exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{\left|(2x)^2 - m\right|}{m(m-1)} \leqslant \left(\frac{6}{\mathrm{e}} + 2\right) \cdot \frac{1}{m}.$$

Proof. In this proof we will repeatedly use the bound

$$\exp\left(-\frac{2x^2}{m+1}\right) \cdot (2x)^k \leqslant \left(k \cdot \frac{m+1}{\mathrm{e}}\right)^{k/2} \tag{30}$$

which follows from Claim 6 by setting $a = (m+1)/2$.

1. For $m \geqslant 1$,
$$\begin{aligned} \exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{2x}{m} &\leqslant \left(\frac{m+1}{\mathrm{e}}\right)^{1/2} \cdot \frac{1}{m} && \text{(using Equation 30 with } k = 1) \\ &= \left(\frac{m+1}{\mathrm{e}m}\right)^{1/2} \cdot \frac{1}{m^{1/2}} \\ &\leqslant \left(\frac{2}{\mathrm{e}}\right)^{1/2} \cdot \frac{1}{m^{1/2}}. && \text{(bound holds for } m \geqslant 1) \end{aligned}$$
2. For $m \geqslant 2$,
$$\begin{aligned} &\exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{\left|(2x)^2 - m\right|}{m(m-1)} \\ &\leqslant \exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{(2x)^2 + m}{m(m-1)} \\ &= \exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{(2x)^2}{m(m-1)} + \exp\left(-\frac{2x^2}{m+1}\right) \cdot \frac{1}{(m-1)} \\ &\leqslant \left(2 \cdot \frac{m+1}{\mathrm{e}}\right) \cdot \frac{1}{m(m-1)} + \frac{1}{m-1} && \text{(using Equation 30 with } k \in \{2, 0\}) \\ &= \left[\frac{2(m+1)}{\mathrm{e}(m-1)} + \frac{m}{m-1}\right] \cdot \frac{1}{m} \\ &\leqslant \left(\frac{6}{\mathrm{e}} + 2\right) \cdot \frac{1}{m} && \text{(bound holds for } m \geqslant 2.) \end{aligned}$$

◀

D Choice of Reconstruction Multipliers

D.1 Improving Constants in the Security Bound

Recall from the proof of Theorem 2 that

$$\begin{aligned}
&2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\
&\quad \leqslant (n\log\lambda)^{\frac{n}{2}} \cdot n \cdot \exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta;\vec{\beta})\right) + \left(5^{\frac{5n}{2}-3}\cdot(n\log\lambda)^{\frac{n}{2}} + \frac{4n}{\lambda}\right)\lambda^{-\frac{n}{2}+1} \\
&\quad \leqslant \mathcal{O}(n\log\lambda)^{\frac{n}{2}} \cdot \exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta;\vec{\beta})\right) + \mathcal{O}(n\log\lambda)^{\frac{n}{2}} \cdot \lambda^{-\frac{n}{2}+1}
\end{aligned}$$

The strategy is to choose β that makes the score function $\min_{\zeta\in\mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta;\vec{\beta})$ sufficiently large (Equation 25) that it dominates the multiplicative factor $(n\log\lambda)^{\frac{n}{2}}\cdot n$ in front of it and vanishes altogether.

$$\min_{\zeta\in\mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta;\vec{\beta}) \geqslant \left(\frac{n}{2}+1\right)\log(n\log\lambda) + cn\log\lambda \qquad \text{(Equation 25 restated)}$$

However, even in the 'best case' where the first summand completely vanishes to zero, the second summand remains. While $\mathcal{O}(n\log\lambda)^{n/2}$ is negligible compared to $\lambda^{-n/2+1}$ in asymptotic sense, it could be not in concrete cases. For instance, suppose $n = 16$ and the security budget is 2^{-48}. Then, we should chose λ that satisfies:

$$\left(5^{\frac{5n}{2}-3}\cdot(n\log\lambda)^{\frac{n}{2}} + \frac{4n}{\lambda}\right)\lambda^{-\frac{n}{2}+1} \leqslant 2^{-50}$$

i.e. $\lambda \geqslant 2^{30}$ approximately, which is highly impractical.

This second summand bound was an artifact of Equation 19 in the proof of Theorem 1 (and our choice of τ such that $2\lambda^\tau = (n\log\lambda)^{1/2}$); it was:

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| + 4n\exp(-2\lambda^{2\tau}) \leqslant \left(5^{\frac{5n}{2}-3}(n\log\lambda)^{\frac{n}{2}} + \frac{4n}{\lambda}\right)\lambda^{-\frac{n}{2}+1}$$

and the bound was obtained by applying the union bound and Lemma 4. Alternatively, we can bound it as follows:

$$\begin{aligned}
&\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \\
&= \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left(\sum_{w_i=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right) \\
&\leqslant \prod_{i=1}^{n}\left(\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \left(\sum_{w_i=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right)^n\right)^{1/n} \qquad \text{(by Hölder's inequality (Lemma 3))} \\
&\leqslant \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_{w}(\beta\zeta)\right|\right)^n \qquad \text{(upper bound every sum with the largest one)} \\
&\leqslant \sum_{\zeta\in F^*\setminus\{0,\zeta^*\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_{w}(\zeta)\right|\right)^n
\end{aligned}$$

$$\leqslant \sum_{\mathrm{wt}^\vee(\zeta)\in\{1,\lambda-1\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n + \sum_{\mathrm{wt}^\vee(\zeta)\in\{2,\lambda-2\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n + \sum_{\mathrm{wt}^\vee(\zeta)\in\{3,\ldots,\lambda-3\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n \tag{31}$$

By Equation 28 in the proof of Lemma 4, for ζ such that $\mathrm{wt}^\vee(\zeta) \in \{1, \lambda-1\}$,

$$\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \sum_w \frac{1}{2^\lambda}\binom{\lambda}{w}\frac{|\lambda-2w|}{\lambda} = \frac{1}{2^{\lambda-1}}\binom{\lambda-1}{\lfloor(\lambda-1)/2\rfloor} \leqslant \sqrt{\frac{1}{\lambda}}$$

$$\implies \sum_{\mathrm{wt}^\vee(\zeta)\in\{1,\lambda-1\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n \leqslant 2\binom{\lambda}{1}\lambda^{-n/2} = 2\lambda^{-n/2+1} \tag{32}$$

Similarly, for $\mathrm{wt}^\vee(\zeta) \in \{2, \lambda-2\}$, we can use Equation 29 to conclude

$$\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \sum_w \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \frac{6}{\lambda} \qquad \text{(as long as } \lambda > 2\text{)}$$

$$\implies \sum_{\mathrm{wt}^\vee(\zeta)\in\{2,\lambda-2\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n \leqslant \binom{\lambda}{2}\frac{6^n}{\lambda^n} = 6^n\lambda^{-n+2} \tag{33}$$

and lastly, for $\mathrm{wt}^\vee(\zeta) \in \{3, \ldots, \lambda-3\}$, we just use Lemma 4.

$$\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \leqslant \sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \lambda^{-1/4}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2} = 2\lambda^{1/4+\tau}\binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-1/2}$$

$$\begin{aligned}
\implies \sum_{\mathrm{wt}^\vee(\zeta)\in\{3,\ldots,\lambda-3\}} \left(\sum_{w=\lambda/2\pm\lambda^{1/2+\tau}} \left|\widehat{\mathbb{1}}_w(\zeta)\right| \right)^n &\leqslant 2^n\lambda^{n/4+n\tau} \sum_{\mathrm{wt}^\vee(\zeta)=3}^{\lambda-3} \binom{\lambda}{\mathrm{wt}^\vee(\zeta)}^{-n/2} \\
&\leqslant 2^n\lambda^{n/4+n\tau} \sum_{k=3}^{\lambda-3} \binom{\lambda}{k}^{-n/2+1} \\
&\leqslant 2^n\lambda^{n/4+n\tau}(\lambda-5)\binom{\lambda}{3}^{-n/2+1} \\
&\leqslant \lambda^{n/4}(n\log\lambda)^{n/2}\frac{6^{n/2-1}}{(\lambda-2)^{3n/2-4}}
\end{aligned} \tag{34}$$

Substituting these (Equation 32, 33, and 34) into our new bound (Equation 31), we get:

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}} \prod_{i=1}^n \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|$$

$$\leqslant 2\lambda^{-n/2+1} + 6^n\lambda^{-n+2} + \lambda^{n/4}(n\log\lambda)^{n/2}\frac{6^{n/2-1}}{(\lambda-2)^{3n/2-4}}$$

The first term $\lambda^{-n/2+1}$ determines the strictly asymptotic behavior as $\lambda \to \infty$.

Using this new upper bound for the second summand, one can calculate that $\lambda \geqslant 256$ is sufficient to keep the second summand strictly below 2^{-48} with $n = 16$ parties, which is a significant improvement over the previous bound. It is also sufficient to make the first summand (the term with the Score function) strictly below 2^{-48} for $n = 16$, provided that the condition in Corollary 1 is satisfied.

D.2 Hamming Weights under Different Irreducible Polynomials

In this subsection, we write $\mathsf{Tr} = \mathsf{Tr}_{F_{2^\lambda}/F_2}$ for brevity.

▶ **Claim 7.** *Let $\Pi(Z) = Z^\lambda + Z + 1 \in F_2[Z]$ be irreducible and $F = F_{2^\lambda} = F_2[Z]/(\Pi(Z))$. Let $Z \in F$ be the element with $Z^\lambda = Z + 1$, and*

$$(\zeta^*)^\vee = \big(\mathsf{Tr}(\zeta^*), \mathsf{Tr}(Z\zeta^*), \cdots, \mathsf{Tr}(Z^{\lambda-1}\zeta^*)\big) := (1, 1, \ldots, 1).$$

Then, for $0 \leqslant i \leqslant \lambda - 1$, we have $\mathrm{wt}^\vee(Z^i\zeta^*) = \lambda - i$ and $\mathrm{wt}^\vee(Z^{-i}\zeta^*) = \lambda - \lceil i/2 \rceil$.

Proof. Let $s_m := \mathrm{Tr}(Z^m\zeta^*)$ for $m \in \mathbb{Z}$. Then $s_0 = s_1 = \cdots = s_{\lambda-1} = 1$. Since $Z^\lambda = Z + 1$, using the F_2-linearity of trace function, we get

$$s_{m+\lambda} = s_{m+1} + s_m \text{ and } s_{-m} = s_{\lambda-m} + s_{1-m}$$

Consider $Z^i\zeta^*$. We count the 1's in $s_i, s_{i+1}, \ldots, s_{i+\lambda-1}$. The first part $s_i, s_{i+1}, \ldots, s_{\lambda-1}$ contains exactly $\lambda - i$ ones, because these indices lie in $\{0, \ldots, \lambda - 1\}$. For the remaining indices, let us write them as $s_{\lambda+m}$ with $0 \leqslant m \leqslant i - 1$. Since $i \leqslant \lambda - 1$, both m and $m + 1$ lie between 0 and $\lambda - 1$. Hence

$$s_{\lambda+m} = s_{m+1} + s_m = 1 + 1 = 0$$

and hence $\mathrm{wt}^\vee(Z^i\zeta^*) = \lambda - i$.

Now consider $Z^{-i}\zeta^*$. Let us we count the 1's in $s_{-i}, s_{-i+1}, \ldots, s_{-1}, s_0, s_1, \ldots, s_{\lambda-i-1}$. The nonnegative part $s_0, s_1, \ldots, s_{\lambda-i-1}$ contributes $\lambda - i$ ones. It remains to count the ones among $s_{-1}, s_{-2}, \ldots, s_{-i}$. Put $m \geqslant 1$. From $s_{-m} = s_{\lambda-m} + s_{1-m}$ and the fact that $s_{\lambda-m} = 1$ for $1 \leqslant m \leqslant i$, we obtain $s_{-m} = 1 + s_{1-m}$. Since $s_0 = 1$, this gives $s_{-1} = 0$ and then inductively

$$s_{-1}, s_{-2}, s_{-3}, \ldots = 0, 1, 0, \ldots$$

Among $s_{-1}, \ldots, s_{-i}$, the number of ones is $\lfloor i/2 \rfloor$. Hence,

$$\mathrm{wt}^\vee(Z^{-i}\zeta^*) = (\lambda - i) + \left\lfloor \frac{i}{2} \right\rfloor = \lambda - \left\lceil \frac{i}{2} \right\rceil$$

and this proves the claim. ◀

▶ **Claim 8.** *Let $\Pi(Z) = Z^\lambda + Z^j + 1 \in F_2[Z]$ be irreducible and $F = F_{2^\lambda} = F_2[Z]/(\Pi(Z))$. Let $Z \in F$ be the element with $Z^\lambda = Z^j + 1$, and*

$$(\zeta^*)^\vee := \big(\mathsf{Tr}(\zeta^*), \mathsf{Tr}(Z\zeta^*), \cdots, \mathsf{Tr}(Z^{\lambda-1}\zeta^*)\big) := (1, 1, \ldots, 1).$$

Let $i = kj$ with $0 \leqslant i \leqslant \lambda - j$. Then $\mathrm{wt}^\vee(Z^i\zeta^*) = \lambda - i$ and

$$\mathrm{wt}^\vee(Z^{-i}\zeta^*) = \begin{cases} \lambda - kj/2, & \text{if } k \text{ is even} \\ \lambda - j - (k-1)j/2, & \text{if } k \text{ is odd} \end{cases}$$

Proof. Similar to the previous claim, let for every m, $s_m := \mathsf{Tr}(Z^m\zeta^*)$. Then, as previous we have, $s_0 = s_1 = \cdots = s_{\lambda-1} = 1$, $s_{m+\lambda} = s_{m+j} + s_m$ and $s_{-m} = s_{\lambda-m} + s_{j-m}$.

Let us first consider $Z^i\zeta^*$. We need to count the ones in $s_i, s_{i+1}, \ldots, s_{i+\lambda-1}$. The first part $s_i, s_{i+1}, \ldots, s_{\lambda-1}$ contains exactly $\lambda - i$ ones, because these indices lie in $\{0, \ldots, \lambda - 1\}$. For the remaining indices, write them as $s_{\lambda+m}$ with $0 \leqslant m \leqslant i - 1$. Since $i \leqslant \lambda - j$, both m and $m + j$ lie between 0 and $\lambda - 1$. Hence,

$$s_{\lambda+m} = s_{m+j} + s_m = 1 + 1 = 0$$

and hence $\mathrm{wt}^\vee(Z^i\zeta^*) = \lambda - i$.

Now we consider $Z^{-i}\zeta^*$. We need to count the ones in $s_{-i}, s_{-i+1}, \ldots, s_{-1}, s_0, s_1, \ldots, s_{\lambda-i-1}$. The nonnegative part $s_0, s_1, \ldots, s_{\lambda-i-1}$ contributes $\lambda - i$ ones. It remains to count the ones among $s_{-1}, s_{-2}, \ldots, s_{-i}$. Put $m \geqslant 1$. From $s_{-m} = s_{\lambda-m} + s_{j-m}$ and the fact that $s_{\lambda-m} = 1$ for $1 \leqslant m \leqslant i$, we obtain $s_{-m} = 1 + s_{j-m}$. For $1 \leqslant m \leqslant j$, we have $j - m \in \{0, \ldots, j-1\}$, and hence $s_{j-m} = 1$. Therefore

$$s_{-1} = s_{-2} = \cdots = s_{-j} = 0.$$

For $m > j$, the same relation gives $s_{-m} = 1 + s_{-(m-j)}$. Thus, within the segment $s_{-1}, s_{-2}, \ldots, s_{-i}$, the values occur in alternating blocks of length j: first j zeros, then j ones, then j zeros, and so on. Since $i = kj$, the number of ones in this segment is $kj/2$ if k is even, and $(k-1)j/2$ if k is odd. Therefore,

$$\begin{aligned}\mathrm{wt}^\vee(Z^{-i}\zeta^*) &= \begin{cases}(\lambda - kj) + kj/2, & \text{if } k \text{ is even}\\ (\lambda - kj) + (k-1)j/2, & \text{if } k \text{ is odd}\end{cases}\\ &= \begin{cases}\lambda - kj/2, & \text{if } k \text{ is even}\\ \lambda - j - (k-1)j/2, & \text{if } k \text{ is odd}\end{cases}\end{aligned}$$

and this proves the claim. ◀

▶ **Claim 9.** *Let* $\Pi(Z) = Z^\lambda + Z^j + 1 \in F_2[Z]$ *be irreducible and* $F = F_{2^\lambda} = F_2[Z]/(\Pi(Z))$. *Let* $Z \in F$ *be the element with* $Z^\lambda = Z^j + 1$, *and*

$$(\zeta^*)^\vee := \left(\mathsf{Tr}(\zeta^*), \mathsf{Tr}(Z\zeta^*), \cdots, \mathsf{Tr}(Z^{\lambda-1}\zeta^*)\right) := (1, 1, \ldots, 1).$$

Then $\mathrm{wt}^\vee(Z^j\zeta^*) = \lambda - j$ *and* $\mathrm{wt}^\vee(Z^{-j}\zeta^*) = \lambda - j$.

Proof. This is the special case $i = j$, equivalently $k = 1$, of the previous claim. Indeed, $\mathrm{wt}^\vee(Z^j\zeta^*) = \lambda - j$. For the inverse direction, since $k = 1$ is odd, the previous claim gives

$$\mathrm{wt}^\vee(Z^{-j}\zeta^*) = \lambda - j - \frac{(1-1)j}{2} = \lambda - j.$$

This proves the claim. ◀

E Limitations of Existing Approaches

In this section, for simplicity, we set every function to have $\{0,1\}^\lambda$ as its domain. Fourier analysis on the Boolean hypercube $\{0,1\}^\lambda$ [46] is equivalent to Fourier analysis on $(F_{2^\lambda}, +)$ (see Section 2.4) under a self-dual basis $\mathcal{B} = \mathcal{B}^\vee$. In particular, for all $f\colon \{0,1\}^\lambda \to \mathbb{C}$, its Fourier transform $\widehat{f}\colon \{0,1\}^\lambda \to \mathbb{C}$ such that

$$\widehat{f}(\alpha) = \frac{1}{2^\lambda} \sum_{x \in \{0,1\}^\lambda} f(x)(-1)^{\langle \alpha, x\rangle}$$

Additionally, $\mathrm{wt}^\vee(x) = \mathrm{wt}(x)$ for all $x \in \{0,1\}^n$.

E.1 Approximating the Spectral Norm of the Hamming Slice via Hamming Ball

Let $\mathbb{1}_{\leqslant w}(x)$ be the indicator function for the Hamming ball of radius w: $\mathbb{1}_{\leqslant w}(x) = 1$ if $\mathrm{wt}(x) \leqslant w$ and 0 otherwise. Then, the indicator function for Hamming slice can be written as $\mathbb{1}_w = \mathbb{1}_{\leqslant w} - \mathbb{1}_{\leqslant (w-1)}$, and by linearity of the Fourier transform we have $\widehat{\mathbb{1}}_w = \widehat{\mathbb{1}}_{\leqslant w} - \widehat{\mathbb{1}}_{\leqslant (w-1)}$, and hence by the triangle inequality, $|\widehat{\mathbb{1}}_w| \leqslant |\widehat{\mathbb{1}}_{\leqslant w}| + |\widehat{\mathbb{1}}_{\leqslant (w-1)}|$. In addition, the complement of $\mathbb{1}_{\leqslant w}$ is $\mathbb{1}_{>w}$, which is a *linear threshold function* (LTF).

Threshold functions are widely studied objects and with many of their Fourier-analytic properties already well-established. It is therefore natural to approximate the spectrum of the Hamming slice through such approaches. While this representation is precise, the resulting spectral estimates are too coarse for tight security analysis. Existing bounds for LTFs are asymptotic and do not provide meaningful guarantees in the Hamming slice regime (i.e., $\log \lambda$-bit leakage function).

To see this, for $n \geqslant 3$, we consider the effect of approximating the central slice $\mathbb{1}_{\lambda/2}$ by the majority function $\mathbb{1}_{\geqslant \lambda/2}$. Denote the levelwise (level-k) ℓ_n-spectral weight as $W_{k,n}(f) := \sum_{|S|=k} |\widehat{f}(S)|^n$. Using classical results on LTFs [5, 9, 46], one obtains

$$W_{k,n}\left(\mathbb{1}_{\geqslant \lambda/2}\right) = \mathcal{O}\left(k^{-3n/4} \cdot \binom{\lambda}{k}^{-n/2+1}\right)$$

Observe that this decays rapidly as k increases, and the first few levels dominate the spectral weight, as shown in Figure 1. For sufficiently large λ, the total spectral weight ($0 < |S| < \lambda$) or the (almost) ℓ_n-spectral norm becomes $\mathcal{O}\left(\lambda^{-n/2+1}\right)$. Applying this result to approximate the second summand in our security analysis for $\mathbb{1}_{\lambda/2}$ yields an insecurity bound of $\mathcal{O}(\lambda)$, which is meaningless in our context.

In contrast, for the central Hamming slice $\mathbb{1}_{\lambda/2}$, using direct Krawtchouk analysis for the first few levels and Parseval's theorem for the rest, we prove that levelwise ℓ_n-spectral weights satisfy

$$W_{k,n}\left(\mathbb{1}_{\lambda/2}\right) = \begin{cases} \mathcal{O}\left(\lambda^{-n/2} \cdot \binom{\lambda}{k}^{-n/2+1}\right) & \text{for } k = 1, 2, 3, 4 \\ \mathcal{O}\left(\lambda^{-n/4} \cdot \binom{\lambda}{k}^{-n/2+1}\right) & \text{for } k \geqslant 5 \end{cases}$$

Note again that lower levels are the dominating levels as shown in Figure 1. One can see then that for sufficiently large λ, the (almost) ℓ_n-spectral norm of $\mathbb{1}_{\lambda/2}$ is $\mathcal{O}\left(\lambda^{-n+1}\right)$. Substituting this, we obtain the bound $\mathcal{O}\left(\lambda^{-n/2+1}\right)$ for the second summand in our security analysis, which allows us to obtain polynomial security for all $n \geq 3$.

Therefore, the key distinction is that the naïve threshold-based estimate overestimates the low-level spectral weight of the Hamming slice, losing a critical $\lambda^{n/2}$ factor in the exponent of the spectral norm. Recovering this factor requires a direct spectral analysis using Krawtchouk polynomials, which accurately captures the insecurity.

E.2 Approximating the Spectral Norm of the Hamming Slice via Level-k Inequalities

▶ **Imported Theorem 2** (Level-1 Inequality [46, Chapter 5.4]). *For $f\colon \{0,1\}^n \to \{0,1\}$ with $\mathbb{E}[f] =: \alpha \leqslant 1/2$,*

$$W^1[f] := \sum_{j=1}^{n} \widehat{f}(e_j)^2 \leqslant 2\alpha^2 \log\left(\frac{1}{\alpha}\right)$$

where $e_j := (0, \ldots, 0, \underset{j\text{-}th}{1}, 0, \ldots, 0) \in \{0,1\}^n$.

In our context, e_j would mean an element F_{2^λ} with Hamming weight 1. Then, the level-1 inequality (Imported Theorem 2) would imply

$$\sum_{\zeta \in F:\ \mathrm{wt}(\zeta)=1} \widehat{\mathbb{I}}_w(\zeta)^2 \leqslant 2\rho_w^2 \log\left(\frac{1}{\rho_w}\right) \tag{35}$$

where $\rho_w := \frac{1}{2^\lambda}\binom{\lambda}{w}$ denotes the density of Hamming slice of weight w in F_{2^λ}. Since $x^2\log(1/x)$ is an increasing function over the interval $(0, 1/\sqrt{e})$,

$$2\rho_w^2 \log\left(\frac{1}{\rho_w}\right) \leqslant 2\rho_{\lfloor \lambda/2 \rfloor}^2 \log\left(\frac{1}{\rho_{\lfloor \lambda/2 \rfloor}}\right) \lesssim \frac{\log(\lambda)}{\lambda} \tag{36}$$

where the last inequality is a consequence of Fact 3. As Remark 9 noted, $\widehat{\mathbb{I}}_w(\zeta)$ depends solely on w and $\mathrm{wt}(\zeta)$. Hence, Equation 35 and 36 give us:

$$\left|\widehat{\mathbb{I}}_w(\zeta)\right| \lesssim \frac{\sqrt{\log(\lambda)}}{\lambda} \qquad \text{for all } \zeta \in F_{2^\lambda} \text{ where } \mathrm{wt}(\zeta) = 1 \text{ or } \lambda - 1 \tag{37}$$

which is what we obtained in Lemma 4 but with a logarithmic overhead.

▶ **Imported Theorem 3** (Level-k Inequality [46, Chapter 9.5]). *For* $f\colon \{0,1\}^n \to \{0,1\}$ *with* $\mathbb{E}[f] =: \alpha$ *and* $k \leqslant 2\ln(1/\alpha)$ *a positive integer,*

$$W^{\leqslant k}[f] := \sum_{\substack{\zeta \in \{0,1\}^n \\ \mathrm{wt}(\zeta) \leqslant k}} \widehat{f}(\zeta)^2 \leqslant \alpha^2 \cdot \left(\frac{2e}{k}\ln\left(\frac{1}{\alpha}\right)\right)^k$$

Clearly $W^2[f] \leqslant W^{\leqslant 2}[f]$, and so again with Remark 9 and Equation 36 in mind, we obtain

$$\left|\widehat{\mathbb{I}}_w(\zeta)\right| \lesssim \frac{\ln(\lambda)}{\lambda^{3/2}} \qquad \text{for all } \zeta \in F_{2^\lambda} \text{ where } \mathrm{wt}(\zeta) = 2 \text{ or } \lambda - 2 \tag{38}$$

which again is Lemma 4 with an additional logarithmic factor. These logarithmic overheads will accumulate and carry over to the expression for insecurity. Hence, while the resulting insecurity bound may not change the bound for the number of parties, the required bit-length λ for the same level of security will increase.

E.3 Optimistic Analysis

We argue that, while retaining the technical framework of our analysis, using the most optimistic estimates of Krawtchouk evaluations, one can optimistically only hope to prove security of schemes for $n \geqslant 3$ parties. Given this observation, our presentation introduces only the minimum technical machinery to prove our security result for $n \geqslant 3$ parties. For $n = 2$, new analysis techniques need to be developed.

We begin with the observation that the insecurity is upper-bounded by

$$\sum_{\vec{w} \in \{0,1,\ldots,\lambda\}^n} \sum_{\zeta \in F^*} \prod_{i=1}^{n} \left|\widehat{\mathbb{I}}_{w_i}(\beta_i \zeta)\right|$$

We separate the quantity as:

$$\underbrace{\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|}_{\text{first summand}}+\underbrace{\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|}_{\text{second summand}}$$

Upper bounding just the second summand non-trivially will be a challenge. Let $B(z;w)$ denote an upper bound on $\left|\widehat{\mathbb{1}}_w(\zeta)\right|$, where $z=\mathrm{wt}(\zeta)$. Using this upper bound, we get the following upper bound on the second summand above.

$$\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}B(\ \mathrm{wt}(\beta_i\zeta)\ ;w_i)\leqslant\sum_{1\leqslant z\leqslant\lambda-1}\binom{\lambda}{z}\cdot\left(\sum_{w\in\{0,1,\ldots,\lambda\}}B(z;w)\right)^n \tag{39}$$

So, we need an estimate for $\sum_w B(z;w)$. $B(z;w)$ is an upper bound on the evaluation of the Krawtchouk polynomial. $B(z;w)$ will have the property that it will decrease as z gets closer to $\lambda/2$. The most optimistic estimates from [36, Theorem 10] put it as (roughly)[4]

$$B(z;w)^2=\lambda^{-1}\cdot\binom{\lambda}{w}2^{-\lambda}\cdot\binom{\lambda}{z}^{-1}$$

We highlight that the multiplicative λ^{-1} factor is the non-trivial part; without that factor, the upper bound is straightforward. In light of this optimistic estimate, we have

$$\begin{aligned}\sum_w B(z;w)&=\lambda^{-1/2}2^{-\lambda/2}\binom{\lambda}{z}^{-1/2}\sum_w\binom{\lambda}{w}^{1/2}\\&=\lambda^{-1/2}2^{-\lambda/2}\binom{\lambda}{z}^{-1/2}2^{\lambda/2}\lambda^{1/4}=\lambda^{-1/4}\binom{\lambda}{z}^{-1/2}\end{aligned}$$

The last equality uses the asymptotic estimate from [25, Answer to Problem 9.18 on page 593].[5] We substitute this estimate back in Equation 39 to get our overall upper bound on the second summand

$$\sum_{1\leqslant z\leqslant\lambda-1}\binom{\lambda}{z}^{1-n/2}\lambda^{-n/4}.$$

For $n=2$, the upper bound on the second summand is $\sqrt{\lambda}$, which is meaningless. Only for $n\geqslant 3$, the upper bound on the second summand can be meaningful. In fact, it suffices to (1) use an accurate estimate for $B(1;w)$ and (2) elsewhere use the trivial Parseval-based estimate

$$B(z;w)^2=\binom{\lambda}{w}2^{-\lambda}\binom{\lambda}{z}^{-1}.$$

[4] The result of [36, Theorem 10] is more nuanced. For back-of-the-envelope calculations, ignoring a small correction term, it implies $\binom{\lambda}{z}B(z;w)^2$ has order $(z(\lambda-z))^{-1/2}\cdot\binom{\lambda}{w}2^{-\lambda}$. When $z=\Theta(\lambda)$, which is a constant fraction of all possible $z\in\{0,1,\ldots,\lambda\}$, this quantity is $\lambda^{-1}\cdot\binom{\lambda}{w}2^{-\lambda}$.

[5] An upper bound of $2^{\lambda/2}(\lambda+1)^{1/2}$ is straightforward using Cauchy-Schwarz. The tighter $\mathcal{O}\left(\lambda^{1/4}\right)$ asymptotic term requires additional effort.