Leakage-resilient Secret-sharing against Hamming Weight Leakage

Aniruddha Biswas Jihun Hwang Hemanta K. Maji Xiuyu Ye

July 1, 2025

Abstract

The additive secret sharing over a characteristic 2 field is vulnerable to the Hamming weight leakage attack – the sum of the Hamming weights of all the shares and the secret has even parity. This work constructs variants of this secret sharing that protect their secret from the Hamming weight leakage.

We consider generalized additive and Shamir secret sharing (over any characteristic 2 field), where all n parties are required for secret reconstruction. These schemes are parameterized by a vector $\vec{\beta} \in (F^*)^n$ such that the dot product of the shares with it reconstructs the secret. Our contributions are the following:

1. Given $\vec{\beta}$, compute the corresponding secret sharing's security against Hamming weight leakage.
2. Construct secure secret sharing schemes against Hamming weight leakage.
3. Prove that the additive secret sharing is essentially the only scheme vulnerable to Hamming weight leakage.
4. Prove that Shamir's secret sharing with random evaluation places is secure with high probability.
5. Determine the security of Shamir's scheme with specific evaluation places.

The security against Hamming weight leakage translates into security against arbitrary symmetric function leakage from the shares.

Our analysis proceeds via Fourier analysis and makes two key contributions. (1) We use a *rearrangement inequality* in the analysis, a first in this line of work. (2) We identify a *score function* that determines the security of the secret sharing corresponding to $\vec{\beta}$.

1 Introduction

Traditionally, a (threshold) secret sharing protects its secret against an adversary who cannot recover a quorum of shares. However, side channel attacks can partially compromise every share to reveal secret information. *Local leakage-resilience* is a security metric introduced by Benhamouda et al. [BDIR18, BDIR21] that insists on the independence of this leakage from the secret. This work considers the local leakage resilience of secret sharing schemes where all shares are needed to reconstruct the secret.

We consider *generalized additive secret sharing* and *Shamir secret sharing* with reconstruction threshold n, the number of parties. The secret sharing is over a finite field F of size 2^λ, where λ represents the security parameter. Such schemes are parameterized by a sequence of reconstruction multipliers $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in (F^*)^n$ and the corresponding secret sharing is denoted by $\mathsf{GenAdd}(\vec{\beta})$. The shares $(s_1, s_2, \ldots, s_n) \in F^n$ of a secret $s \in F$ are random elements satisfying the constraint $\beta_1 \cdot s_1 + \beta_2 \cdot s_2 + \cdots \beta_n \cdot s_n = s$.

Elements of F are *represented as F_2-polynomials* of degree $< \lambda$ using the isomorphism $F \equiv F_2[Z]/\Pi(Z)$, where $\Pi(Z)$ is a monic irreducible polynomial of degree λ. In this representation, for $x \in F$, $\mathrm{wt}(x)$ denotes the number of non-zero coefficients of the polynomial – the *Hamming weight* of x. This work will characterize the security of $\mathsf{GenAdd}(\vec{\beta})$ against the Hamming weight leakage from every share. Recently, Faust et al. [FMM+24] presented a fascinating expository work connecting practical side-channel attacks and local leakage resilience against the Hamming weight attack; we refer interested readers to this work for broader motivation.

To develop an understanding of security/insecurity landscape of such secret sharing schemes, it is instructive to illustrate a vulnerability of such schemes explicitly. Consider $\mathsf{GenAdd}(\vec{\beta})$, where $\vec{\beta} = (1, 1, \ldots, 1)$; here 1 represents the multiplicative identity of F. It is the classical *additive secret sharing* scheme; its shares of a secret s will satisfy the identity $s_1 + s_2 + \cdots + s_n = s$. Note that the Hamming weight function $\mathrm{wt}\colon F \to \{0, 1, \ldots, \lambda\}$ satisfies the "linearity" identity: $\mathrm{wt}(x+y) = \mathrm{wt}(x) + \mathrm{wt}(y) \mod 2$.[1] Consequently, we have: $\mathrm{wt}(s_1) + \mathrm{wt}(s_2) + \cdots + \mathrm{wt}(s_n) = \mathrm{wt}(s) \mod 2$. So, the Hamming weight of the shares reveals $\mathrm{wt}(s) \mod 2$; thus $\mathsf{GenAdd}(\ (1, 1, \ldots, 1)\ )$ is insecure against the Hamming weight leakage from each share. In general, when $\beta_1 = \beta_2 = \cdots = \beta_n$, the Hamming weight of the shares reveals $\mathrm{wt}(s \cdot \beta_1^{-1}) \mod 2$.

With this background and in light of the ongoing NIST efforts in standardizing secret sharing schemes [BP23], a natural question arises:

Is $\mathsf{GenAdd}(\vec{\beta})$ is secure against the Hamming weight leakage?

Summary of our results. For $n \geqslant 3$ parties, we present an efficiently computable score for $\vec{\beta}$ – the larger the score, the smaller is $\mathsf{GenAdd}(\vec{\beta})$'s insecurity. We identify $\vec{\beta}$ such that $\mathsf{GenAdd}(\vec{\beta})$ is secure against the Hamming weight leakage, for $n \geqslant 3$. This characterization depends on the representation used; in our case, it is the choice of the irreducible polynomial $\Pi(Z)$. Next, we prove that the generalized additive secret sharing is vulnerable if (and only if) all elements in $\vec{\beta}$ are identical; i.e., the schemes above are the only vulnerable ones. Finally, we characterize the evaluation places $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in (F^*)^n$ for Shamir secret sharing that protects it against Hamming weight leakage. In particular, choosing evaluation places randomly yields a secure secret sharing with high probability.

Our analysis proceeds via Fourier analysis, and our key technical and conceptual contributions include: (1) the use of *rearrangement inequality* in the analysis and (2) identification of the efficiently computable *score function* capturing the insecurity of $\mathsf{GenAdd}(\vec{\beta})$. These security results extend to arbitrary symmetric function leakage per share because any symmetric function is computable from the Hamming weight.

Comparison with bit probing attacks. Local leakage resilience of secret sharing over characteristic 2 fields have been investigated in [MNPY24]. It considers an adversary who probes the shares' representation to learn whether specific bits are set or not. Note that $\mathrm{wt}(x)$ can be approximated by the average of the number of set bits when randomly probing $\mathcal{O}(\log \lambda)$ bits of x's representation (using Chernoff bound). However, security against $\mathcal{O}(\log \lambda)$ physical bits per share does not suffice to imply security against the Hamming weight itself. For instance, whether $\mathrm{wt}(x)$ is even or odd cannot be simulated accurately by random bit probing. Roughly speaking, "high sensitivity" functions of $\mathrm{wt}(x)$ cannot be simulated by random physical proving, in general. Thus, local leakage resilience characterization against the Hamming weight leakage needs a separate analysis.

[1] We clarify that the $+$ in the expression "$x + y$" is the addition operator of F. On the other hand, the $+$ in the expression "$\mathrm{wt}(x) + \mathrm{wt}(y)$" is the integer addition operator.

Furthermore, efficiently computable score function for $\vec{\beta}$ against physical bit probes is unknown; a preliminary inefficient scoring function appears in [Ngu25].

1.1 Our Technical Results

Basic notation. Let F be the finite field of order 2^λ. Elements of F are *represented* as $F_2[Z]$ elements using the isomorphism $F \equiv F_2[Z]/\Pi(Z)$, for some monic irreducible polynomial $\Pi(Z)$ of degree λ. For $x \in F$, its *Hamming weight*, denoted by $\mathrm{wt}(x)$, is the number of non-zero coefficients in this (F_2-polynomial) representation of x.

Secret sharing scheme and security. For $n \in \{1, 2, \dots\}$ parties and $\vec{\beta} = (\beta_1, \beta_2, \dots, \beta_n) \in (F^*)^n$, let $\mathsf{GenAdd}(\vec{\beta})$ represent the *generalized additive secret sharing scheme* that samples uniformly random shares $\vec{s} = (s_1, s_2, \dots, s_n) \in F^n$ satisfying $\beta_1 \cdot s_1 + \beta_2 \cdot s_2 + \cdots + \beta_n \cdot s_n = s$, where $s \in F$ is the secret. For a secret $s \in F$, the Hamming weight leakage is the joint distribution of $(\mathrm{wt}(s_1), \mathrm{wt}(s_2), \dots, \mathrm{wt}(s_n))$ over the sample space $\{0, 1, \dots, \lambda\}^n$. For succinctness, we represent this leakage joint distribution by $\overrightarrow{\mathrm{wt}}(s)$. Likewise, $\overrightarrow{\mathrm{wt}}(U_F)$ represents the leakage joint distribution for a uniformly random secret $s \in F$.

Leakage resilience. We say that $\mathsf{GenAdd}(\vec{\beta})$ secret sharing has ε *insecurity* against the Hamming weight leakage attack if, for every secret $s \in F$, we have:

$$2 \cdot \mathrm{SD}\big(\ \overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\ \big) \leqslant \varepsilon. \tag{1}$$

Roughly speaking, if a secret sharing has small insecurity against the Hamming weight leakage, then the leakage joint distribution is statistically independent of the secret s.

Notation for our results. Define $\sigma\colon \{0, 1, \dots, \lambda\} \to \mathbb{R}$ as follows

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

Remark 1 (Behavior of σ)**.** *Recall that $\binom{\lambda}{w} \geqslant (\lambda/w)^w$. Therefore, we have $\sigma(w) \geqslant (w^*/2) \cdot \log(\lambda/w^*) - (1/4) \cdot \log\lambda$, 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 the central limit theorem, we know that $\binom{\lambda}{\frac{\lambda}{2} \pm x}$ behaves like $\frac{2^\lambda}{\sqrt{\pi\lambda/2}} \exp\Big(-\frac{2x^2}{\lambda}\Big)$. So, $\sigma(\lambda/2 \pm x)$ behaves like $\frac{\log 2}{2}\lambda - \frac{1}{2}\log\lambda - \frac{2x^2}{\lambda}$. 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.

$$\mathsf{Score}(\zeta; \vec{\beta}) \ := \ \sum_{i=1}^{n} \sigma\big(\ \mathrm{wt}(\beta_i \cdot \zeta)\ \big). \tag{2}$$

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

$$\mathcal{S}_{\vec{\beta}} \ := \ \big\{\ \zeta^* \cdot \beta_1^{-1},\ \zeta^* \cdot \beta_2^{-1},\ \dots,\ \zeta^* \cdot \beta_n^{-1}\ \big\} \subseteq F^*. \tag{3}$$

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

Our results. We aim to characterize $\vec{\beta} \in (F^*)^n$ such that $\mathsf{GenAdd}(\vec{\beta})$ is secure. This characterization will build on the following technical result that we prove.

Informal technical result. For $n \in \{3, 4, \dots\}$, we prove that $\mathsf{GenAdd}(\vec{\beta})$ is λ^{-cn} insecure, where $c \in (0, 1/2]$ such that

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}\left(\zeta; \vec{\beta}\right) \geqslant cn \cdot \log \lambda. \tag{4}$$

For clarity of presentation, we ignore additive $\log\log\lambda$ terms in the right-hand side of the expression above. Note that, given $\vec{\beta}$, one can efficiently compute and test whether the minimum score is $\geqslant cn \log \lambda$. For example, if all elements of $\vec{\beta}$ are identical, we know that the $\mathsf{GenAdd}(\vec{\beta})$ is highly insecure. In this case, the minimum score is 0 and our technical result cannot upper bound the insecurity by a small quantity.

Following corollaries are immediate:

1. If every element in $\vec{\beta}$ occurs at most m times, then $\mathsf{GenAdd}(\vec{\beta})$ satisfies Equation 4 with $c = (n-m)/4n$. This is because $\beta_i\zeta$, for $\zeta \in \mathcal{S}_{\vec{\beta}}$, is either ζ^* or has weight $\in \{1, 2, \dots, \lambda\}$. 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 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 picked uniformly randomly from F^n, it has all distinct F^* elements with exponentially high probability.

2. Suppose $\vec{\beta}$ is such that $4cn \leqslant \mathrm{wt}(\beta_2\zeta^*\beta_1^{-1}) \leqslant \lambda - 4cn$ and $4cn \leqslant \mathrm{wt}(\beta_1\zeta^*\beta_2^{-1}) \leqslant \lambda - 4cn$. So, $\sigma(\mathrm{wt}(\beta_1\zeta^*\beta_2^{-1}))$ and $\sigma(\mathrm{wt}(\beta_2\zeta^*\beta_1^{-1}))$ are both $\geqslant cn \log\lambda$ for all $\lambda \geqslant (4cn)^2$. As a result, $\mathsf{Score}(\zeta; \vec{\beta}) \geqslant cn \cdot \log\lambda$ for any $\zeta \in \mathcal{S}_{\vec{\beta}}$. Then, Equation 4 is satisfied for all $\lambda \geqslant (4cn)^2$.

   For independent and random $\beta_1, \beta_2 \in F$, by the Chernoff bound, with exponentially-close-to-1 probability, these two weight constraints above are satisfied. Based on this observation, the leakage-resilient result extends to the security of Shamir's secret-sharing scheme with random evaluation points as follows. Recall that Shamir's secret-sharing with reconstruction threshold n picks a random polynomial $P(X) \in F[X]$ with $\deg P < n$ such that $P(0) = s$, the secret. The shares of the parties are $s_i = P(\alpha_i)$, for $i \in \{1, 2, \dots, n\}$ and $\alpha_i \in F^*$ are the evaluation places. We will consider the scenario where $\alpha_1, \dots, \alpha_n$ are picked independently and uniformly at random from F. This secret sharing is equivalent to $\mathsf{GenAdd}(\vec{\beta})$, where $\vec{\beta}$ is the sequence of corresponding Lagrange multipliers. [HMNY25] proved that β_1 and β_2 are (exponentially close to being) independent and uniform over F. Consequently, the resulting secret sharing scheme is secure against Hamming weight leakage.

   Furthermore, given evaluation places $\vec{\alpha}$, we can efficiently compute the sequence of Lagrange multipliers $\vec{\beta}$ and its score to determine the security of this specific Shamir's scheme.

3. A *symmetric* $f\colon F \to \Omega$ function 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 ([CT99, Chapter 2]), any secret sharing scheme that has ε insecurity against the Hamming weight leakage has ε insecurity against *every* symmetric local leakage.

4. Finally, we prove that if *not all elements of* $\vec{\beta}$ *are identical*, then $\mathsf{GenAdd}(\vec{\beta})$ is (at most) $\lambda^{-1/4}$ insecure. That is, the only vulnerable generalized additive secret sharing schemes are those illustrated in the example in the introduction, albeit their insecurity may not decay sufficiently quickly. Choosing $\vec{\beta}$ with a large minimum score is the recipe to ensure small insecurity, as indicated by our results above.

1.2 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 the $\mathsf{GenAdd}(\vec{\beta})$ secret sharing, for arbitrary $\vec{\beta} \in (F^*)^n$. We illustrate our analysis strategy against the Hamming weight leakage. Our key technical contributions are (1) the use of *rearrangement inequality* when analyzing security of secret-sharing schemes and (2) identifying the *score function* that determines the security of the $\mathsf{GenAdd}(\vec{\beta})$ secret sharing. We will prove the following technical result.

Theorem 1. *For* $\vec{\beta} \in (F^*)^n$*, the* $\mathsf{GenAdd}(\vec{\beta})$ *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*

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \geqslant \mathcal{O}(n \log\log \lambda) + cn \log \lambda \tag{5}$$

for $\frac{1}{2} - \frac{1}{n} > c > 0$*, then* $\mathsf{GenAdd}(\vec{\beta})$ *is* $\mathcal{O}(\lambda^{-cn})$ *insecure against the Hamming weight leakage.*

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

$$2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s) \ , \ \overrightarrow{\mathrm{wt}}(U_F)\big) = \sum_{\vec{w} \in \{0,1,\dots,\lambda\}^n} \left| \Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(s;\vec{\beta})} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(U_F;\vec{\beta})} [\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right| \tag{6}$$

Here, $\mathsf{GenAdd}(\vec{\beta}, s)$ represents the distribution of shares over F^n for the secret $s \in F$. Likewise, $\mathsf{GenAdd}(\vec{\beta}, U_F)$ denotes the distribution of shares for a uniformly random secret in F. Note that each share 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 the 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 $2 \cdot \exp(-2\lambda^{2\tau})$. For example, we can control this probability of "atypical weights" by setting $\tau = \frac{\log\left(\frac{n}{4} \cdot \log \lambda\right)}{2 \log \lambda}$ and driving the probability below $\lambda^{-n/2}$.

So, we define the set of all typical leakage $\mathsf{Typical}(n, \tau) \subseteq \{0, 1, \dots, \lambda\}^n$ parameterized by τ:

$$\mathsf{Typical}(n, \tau) \ := \ \Big\{ \vec{w} \ : \ |w_i - \lambda/2| \leqslant \lambda^{1/2+\tau}, \ \text{for all } i \in \{1, 2, \dots, n\} \Big\}. \tag{7}$$

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) $4n\exp\bigl(-2\lambda^{2\tau}\bigr)$ by the union bound. So, we conclude that

$$2\cdot \mathrm{SD}\bigl(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\bigr) = \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}] \right| \pm 4n\cdot\lambda^{-n/2}. \tag{8}$$

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 using the Fourier coefficients.

$$2\cdot \mathrm{SD}\bigl(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\bigr) = \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \sum_{\zeta\in F^*} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right)\cdot \chi_1\Bigl(s\cdot\zeta\cdot\Bigl\langle\vec{1},\vec{v}\Bigr\rangle\Bigr)\right| \pm 4n\cdot\lambda^{-n/2}. \tag{9}$$

Here, $\mathbb{1}_w\colon F\to\{0,1\}$ is the characteristic 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 $1\in F$ and $\vec{1}=(1,1,\ldots,1)\in F^n$. Moreover, $\chi_1\colon F\to\mathbb{C}$ is defined as

$$\chi_1(x) \ :=\ \exp\left(\frac{2\pi\imath}{p}\cdot \mathsf{Tr}_{F/F_2}(x)\right). \tag{10}$$

To upper-bound the right-hand side expression, we apply the triangle inequality and conclude:

$$2\cdot \mathrm{SD}\bigl(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\bigr) \leqslant \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \sum_{\zeta\in F^*} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \ + 4n\cdot\lambda^{-n/2}. \tag{11}$$

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 $\vec{\beta}=\vec{1}$ 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 $\widehat{\mathbb{1}}_w(x)=2^{-\lambda}K_w(\mathrm{wt}(x))$ where $K_w(\cdot)$ is Krawtchouk polynomial, as defined in [Kra01]. Krawtchouk polynomials find extensive applications in many subfields in theoretical computer science and cryptography; see, for example, [VL98].

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

As we will see, the contributions of $\widehat{\mathbb{1}}_w(x)$, where $\mathrm{wt}(x)\in\{1,2,\ldots,\lambda-1\}$, 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 with $\mathrm{wt}(\zeta^*)=\lambda$, is large; it is the density of the subset of those elements of F whose Hamming weight is w. 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 $i \in \{1, 2, \ldots, n\}$.

$$\mathcal{S}_{\vec{\beta}} := \left\{\zeta^* \cdot \beta_1^{-1},\ \zeta^* \cdot \beta_2^{-1},\ \ldots,\ \zeta^* \cdot \beta_n^{-1}\right\}. \tag{12}$$

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.

$$\begin{aligned} 2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \leqslant & \underbrace{\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|}_{\text{first summand}} \\ & + \underbrace{\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|}_{\text{second summand}} \\ & + 4n \cdot \lambda^{-n/2}. \end{aligned} \tag{13}$$

Now, we will estimate these two summands separately.

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

$$\text{second summand} \leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta) \tag{14}$$

$$= \left(2\lambda^{1/2+\tau}\right)^n \cdot \left(\sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta)\right). \tag{15}$$

The last equality substitutes the cardinality of the $\mathsf{Typical}(n, \tau)$ set.

Note that the $\zeta \mapsto \beta_i \zeta$ is a permutation over F^*. So, we have n permutations $\zeta \mapsto \beta_i \zeta$, for $i \in \{1, 2, \ldots, n\}$, and the monomial $\prod_{i=1}^{n} B(\beta_i \zeta)$ is a product n permuted elements. Finally, $\left(\sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta)\right)$ is the sum of all permuted monomials, such that $B(\zeta^*)$ never appears. Lemma 3 presents our rearrangement lemma that upper bounds this sum as follows:

$$\text{second summand} \leqslant \left(2\lambda^{1/2+\tau}\right)^n \cdot \left(\sum_{\zeta \in F \setminus \{0, \zeta^*\}} B(\zeta)^n\right) \tag{16}$$

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:

$$\text{second summand} \leqslant \left(2\lambda^{1/2+\tau}\right)^n \cdot \lambda^{-n+1} = (2\lambda^{\tau})^n \cdot \lambda^{-n/2+1}. \tag{17}$$

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 $\mathrm{wt}(x) = 1$, 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 2 (A world without the rearrangement lemma)**.** *Suppose we upper bound the second summation using prior techniques as used in [BDIR18, BDIR21, MPSW21, MNPW22, FMM+24]; they did not use the rearrangement lemma. 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 $\mathrm{wt}(x) = 1$, 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 rearrangement lemma-based upper bound is tighter; it is $o(1)$ for $n \geqslant 3$.*

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

$$2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \leqslant \underbrace{\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|}_{\text{first summand}} + \underbrace{\Big((n \log \lambda)^{n/2} + 4n/\lambda\Big) \cdot \lambda^{-n/2+1}}_{\text{small}}. \tag{18}$$

Our expression above indicates that the first summand solely determines the security of the generalized additive secret sharing. We will characterize $\vec{\beta}$ for which the first summand is small; in particular, $\vec{\beta} = \vec{1} \in F^n$ should not be secure.

To begin, we upper bound the first summand as follows:

$$\text{first summand} \leqslant \Big(2\lambda^{1/2+\tau}\Big)^n \cdot n \cdot \max_{\substack{\vec{w} \in \mathsf{Typical}(n,\tau) \\ \zeta \in \mathcal{S}_{\vec{\beta}}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \tag{19}$$

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

$$\prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \leqslant \lambda^{-n/2} \cdot \exp\Big(-\mathsf{Score}(\zeta; \vec{\beta})\Big) \tag{20}$$

Equation 2 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 Hamming weights of $\zeta\beta_i \in F^*$, where $i \in \{1, 2, \ldots n\}$. As a consequence, we get the following upper bound for the first summand:

$$\begin{aligned}
\text{first summand} &\leqslant \Big(2\lambda^{1/2+\tau}\Big)^n \cdot n \cdot \max_{\zeta \in \mathcal{S}_{\vec{\beta}}} \lambda^{-n/2} \cdot \exp\Big(-\mathsf{Score}(\zeta; \vec{\beta})\Big) \\
&= (2\lambda^{\tau})^n \cdot n \cdot \exp\left(-\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta})\right) \\
&= (n \log \lambda)^{n/2} n \cdot \exp\left(-\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta})\right).
\end{aligned} \tag{21}$$

In the last equality above, we substitute our value of τ. 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.

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

$$2{\cdot}\mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \leqslant (n\log\lambda)^{n/2} n{\cdot}\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta;\vec{\beta})\right) + \underbrace{\Big((n\log\lambda)^{n/2} + 4n/\lambda\Big)\cdot\lambda^{-n/2+1}}_{\text{small}}. \tag{22}$$

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

Remark 3. *1. Determining the estimates $B(x)$ is equivalent to estimating the evaluations of Krawtchouk polynomials. We require concrete estimates, not asymptotics [Dom08]. Elementary estimates suffice for our applications; tighter estimates, for example, those in [Kra01, Section 3], do not yield any qualitative improvement of our results.*

2. Lemma 4 also needs concrete estimates of Krawtchouk polynomial evaluations. We present upper bounds on such estimates in Appendix E.

Which schemes are vulnerable? Recall from the example in the introduction that if $\vec{\beta} = (\beta_1,\ldots,\beta_n)$ such that $\beta_1 = \cdots = \beta_n \in F^*$, then the Hamming weight leakage correlates with the secret. Are these the only insecure choices?

Which $\mathsf{GenAdd}(\vec{\beta})$ scheme is vulnerable to Hamming weight leakage?

We present a different strategy to upper bound the insecurity in Section 3.3 and demonstrate that if all elements in $\vec{\beta}$ are not identical, then $\mathsf{GenAdd}(\vec{\beta})$ has insecurity at most $\lambda^{-1/4}$. We prove the following result.

Theorem 2. *For $\vec{\beta}\in(F^*)^n$ and $\zeta\in\mathcal{S}_{\vec{\beta}}$, let $H(\zeta;\vec{\beta}) := \{i\colon \beta_i\zeta \neq \zeta^*\}$ and $\widetilde{h} = \min\limits_{\zeta\in\mathcal{S}_{\vec{\beta}}}\Big(\mathrm{card}(H(\zeta;\vec{\beta}))\Big)$. Then,*

$$\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\ \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\ \prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \leqslant (\widetilde{h}+1)\cdot\left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}}$$

Choosing $\vec{\beta}$ more carefully, with a large minimum score, would ensure quicker reduction in insecurity. We present a quick overview of this theorem's proof.

Note that 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 theorem 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

$$\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\ \prod_{i=1}^{n}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \prod_{i=1}^{n}\left(\sum_{w_i\in\{0,1,\ldots,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right|\right) \tag{23}$$

Consider an index $i \notin H(\zeta; \vec{\beta})$. For such an i, we have $\beta_i \zeta = \zeta^*$ and, consequently, $\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \left|\widehat{\mathbb{1}}_{w_i}(\zeta^*)\right| = \left|\widehat{\mathbb{1}}_{w_i}(0)\right| = \binom{\lambda}{w_i} \cdot 2^{-\lambda}$. 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 23 is

$$= \prod_{i \in H(\zeta;\vec{\beta})} \left(\sum_{w_i \in \{0,1,\ldots,\lambda\}} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| \right) \tag{24}$$

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 *its 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

$$\sum_{w_i \in \{0,1,\ldots,\lambda\}} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| = \mathcal{O}(\lambda)^{-1/4}. \tag{25}$$

Define $\zeta' := \beta_i\zeta$. Observe that $\zeta' \in F \setminus \{0, \zeta^*\}$. A standard application of the Parseval's identity yields the estimate:

$$\left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| \leqslant \sqrt{\binom{\lambda}{w_i} \cdot 2^{-\lambda} \cdot \binom{\lambda}{w'}^{-1}}, \tag{26}$$

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

$$\left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| \leqslant \sqrt{\binom{\lambda}{w_i} \cdot 2^{-\lambda} \cdot \lambda^{-1}}, \tag{27}$$

Using this upper bound on the Fourier coefficient, we have

$$\begin{aligned}
\sum_{w_i \in \{0,1,\ldots,\lambda\}} \left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| &\leqslant 2^{-\lambda/2}\lambda^{-1/2} \sum_{w_i \in \{0,1,\ldots,\lambda\}} \binom{\lambda}{w_i}^{1/2} \\
&< 2^{-\lambda/2}\lambda^{-1/2} \cdot \pi 2^{\lambda/2}\lambda^{1/4} \quad \text{(we prove this concrete upper bound in Claim 5)} \\
&= \pi\lambda^{-1/4},
\end{aligned}$$

which is what we set out to prove.

Remark 4 (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* $\mathcal{S}_{\vec{\beta}} = \left\{\zeta^*\beta_1^{-1}, \ldots, \zeta^*\beta_k^{-1}\right\}$*, 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*

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

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* $\mathcal{O}\left(\lambda^{-1/4}\right)$*.*

2 Preliminaries

Notations Let λ represents the security parameter. We use $F = F_{2^\lambda}$ to denote a finite field of order 2^λ and $F^* := F \setminus \{0\}$ its multiplicative group. When sampling an element $x \in F$ uniformly randomly from F, we write $x \leftarrow U_F$; here, U_F stands for uniform distribution over F.

We denote by $\mathbb{1}_S$ the indicator function for a set S, defined as $\mathbb{1}_S(x) = 1$ if $x \in S$ and $\mathbb{1}_S(x) = 0$ otherwise. For any function $f\colon D \to R$, we let $f^{-1}(y)$ be the set of the preimage of y, that is $f^{-1}(y) := \{x \in D\colon f(x) = y\}$. For instance, if $x \in F$ has $\mathrm{wt}(x) = w$, then $\mathbb{1}_{\mathrm{wt}^{-1}(w)}(x) = 1$ but $\mathbb{1}_{\mathrm{wt}^{-1}(w')}(x) = 0$ for all $w' \neq w$. We shall denote $\mathbb{1}_{\mathrm{wt}^{-1}(w)} =: \mathbb{1}_w$ throughout the paper for the sake of simplicity, in other words

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

Additionally, we write $x = a \pm c$ to denote $x \in [a - c, a + c]$ for all real x and a, and $c > 0$. We use $\mathrm{card}(S)$ to denote the cardinality of the set S (i.e. the number of elements in S).

2.1 Secret Sharing Scheme

Definition 1 (Generalized Additive Secret Sharing)**.** *Let F be a finite field and n be a positive integer. Given the multipliers $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in (F^*)^n$ and secret $s \in F$, $\mathsf{GenAdd}(\vec{\beta}, s)$ shares the secret s via:*

- $\mathsf{Share}(s)$*: Samples $s_1, s_2, \ldots, s_{n-1} \leftarrow U_F$ and sets $s_n = s - \beta_n^{-1}(\beta_1 s_1 + \cdots + \beta_{n-1} s_{n-1})$.*
- $\mathsf{Reconstruct}(\{s_1, \ldots, s_n\})$*: Computes $\beta_1 s_1 + \beta_2 s_2 + \cdots + \beta_n s_n$.*

Definition 2 ($(n, k, \vec{X})$-Shamir Secret Sharing)**.** *Let F be a finite field and n, k be a positive integer such that $k \leqslant n$. Given the evaluation places $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$, and secret $s \in F$, $\mathsf{Shamir}(n, k, \vec{X})$ shares the secret s by*

- $\mathsf{Share}(s)$*: Samples a polynomial $P(X) \in F[X]_{\deg \leqslant k-1}$ such that $P(0) = s$ uniformly randomly, then evaluates it at $\vec{X}$, i.e. $s_i := P(X_i)$ for $i = 1, \ldots, n$.*
- $\mathsf{Reconstruct}(\{s_{i_1}, \ldots, s_{i_k}\})$*: Obtain a unique polynomial $\widetilde{P}(X) \in F[X]_{\deg \leqslant k-1}$ by conducting polynomial interpolation over (X_{i_1}, s_{i_1}), …, (X_{i_k}, s_{i_k}). Compute $s' := \widetilde{P}(0)$.*

Additive secret sharing is then an instance of generalized additive secret sharing where all multipliers are 1 (or the same). Moreover,

Proposition 1. *$\mathsf{Shamir}(n, n, \vec{X})$ is an instance of generalized additive secret sharing.*

Therefore, proving security of GenAdd automatically translates to the security of Shamir for $k = n$.

Proof of Proposition 1. Given n pairs of evaluation points and shares $(X_1, s_1), \ldots, (X_n, s_n)$, one can recover the polynomial $P(X) \in F[X]_{\deg \leqslant n-1}$ that was used to compute the shares s_i's via Lagrange interpolation, and hence the secret as well:

$$P(X) := \sum_{i=1}^{n} \underbrace{\left(\prod_{j \in \{1,2,\ldots,n\} \setminus \{i\}} \frac{X - X_j}{X_i - X_j} \right)}_{=: L_i(X)} \cdot s_i = \sum_{i=1}^{n} L_i(X) \cdot s_i \implies s = P(0) = \sum_{i=1}^{n} L_i(0) \cdot s_i$$

Therefore, $\mathsf{Shamir}(n, n, \vec{X}, s)$ is $\mathsf{GenAdd}(\vec{\beta}, s)$ where $\beta_i = L_i(0) = \prod_{j \in \{1,2,\ldots,n\} \setminus \{i\}} \frac{X_j}{X_j - X_i}$ for all i. □

2.2 Hamming weight Leakage and Leakage-resilient Secret Sharing

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

Definition 3 (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 4 (Hamming weight leakage)**.** *Hamming weight leakage $\overrightarrow{\mathrm{wt}} = (\mathrm{wt}, \mathrm{wt}, \ldots, \mathrm{wt})$ is a collection of n Hamming weight function $\mathrm{wt}\colon F \to \{0, 1, \ldots, \lambda\}$. For any secret $s \in F$, the leakage distribution $\overrightarrow{\mathrm{wt}}(\vec{s})$ over secret shares of s is defined by the following experiment. (a) Sample shares $\vec{s} = (s_1, s_2, \ldots, s_n)$. (b) Output $(\mathrm{wt}(s_1), \mathrm{wt}(s_2), \ldots, \mathrm{wt}(s_n))$. Furthermore, $\overrightarrow{\mathrm{wt}}(\vec{s})$ denotes the joint Hamming weight leakage distribution over all shares.*

Definition 5 (ε-insecurity)**.** *A secret sharing scheme is ε-insecure against Hamming weight leakage if, for Hamming weight leakage $\overrightarrow{\mathrm{wt}}$ and a pair of secret $(s^{(0)}, s^{(1)})$, the statistical distance between the joint Hamming weight leakage distribution $\overrightarrow{\mathrm{wt}}(\mathsf{Share}(s^{(0)}))$ and $\overrightarrow{\mathrm{wt}}(\mathsf{Share}(s^{(1)}))$ is at most ε.*

Definition 6. *We say a weight $w \in \{0, 1, \ldots, \lambda\}$ is typical if $|w - \lambda/2| \leqslant \lambda^{1/2+\tau}$ for some $\tau > 0$, and a vector of weights $\vec{w} = (w_1, w_2, \ldots, w_n) \in \{0, 1, \ldots, \lambda\}^n$ is in a typical set if every w_i is typical:*

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

2.3 Rearrangement Inequality

Consider two finite sequences $\{x_i\}_{i=1}^n$ and $\{y_i\}_{i=1}^n$ of positive real numbers. The sum of product of pair of numbers $x_i y_j$ achieves maximal when they have similar ordering. Specifically, when $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$ and $y_1 \leqslant y_2 \leqslant \ldots \leqslant y_n$, for any permutation σ belongs to the permutation group S_n of $\{1, 2, \ldots, n\}$, $x_n y_1 + \ldots + x_1 y_n \leqslant x_{\sigma(1)} y_1 + \ldots + x_{\sigma(n)} y_n \leqslant x_1 y_1 + \ldots x_n y_n$. The following theorem [Rud52] generalizes the result to multiple sequences of numbers.

Imported Theorem 1 (Rearrangement Inequality [Rud52])**.** *Consider the set of nonnegative numbers $\{a_{ij}\}$ for $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, n\}$. Let $a'_{i1}, a'_{i2}, \ldots, a'_{in}$ denote the array obtained by rearranging $a_{i1}, a_{i2}, \ldots, a_{in}$ in non-increasing order such that $a'_{i1} \geqslant a'_{i2} \geqslant \ldots \geqslant a'_{in}$. Then,*

$$\sum_{j=1}^{n}\prod_{i=1}^{k} a_{ij} \leqslant \sum_{j=1}^{n}\prod_{i=1}^{k} a'_{ij} \quad \textit{and} \quad \prod_{j=1}^{n}\sum_{i=1}^{k} a_{ij} \leqslant \prod_{j=1}^{n}\sum_{i=1}^{k} a'_{ij}.$$

2.4 Fourier Analysis over Finite Field

We shall use Fourier analysis over the additive group $(F, +)$ of a finite field $F = F_{p^d}$ for some prime $p \geqslant 2$ and degree of extension $d \in \{1, 2, \ldots\}$.

Definition 7. *The trace of an extension field $F = F_{p^d}$ over the base field F_p, denoted by $\mathsf{Tr}_{F/F_p}\colon F \to F_p$, is defined as $\mathsf{Tr}_{F/F_p}(y) := \sum_{i=0}^{d-1} y^{p^i}$.*

Let $\omega_p := \exp(2\pi\imath/p)$. Define the Fourier transformation of $f\colon F \to F$ 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. For example, if $F = F_{2^d}$, then $\omega := \omega_2 = \exp(\pi\imath) = -1$ and the Fourier coefficients and characters become

$$\widehat{f}(\alpha) \;:=\; \frac{1}{q}\sum_{x\in F_{2^d}} f(x)\cdot (-1)^{\langle x,\alpha\rangle}$$

where $\langle x, \alpha\rangle \in F_2$ denotes the inner product of x and α viewed as vectors. This is possible because the extension field F_{p^d} is isomorphic to $(F_p)^d$, the vector space of dimension d with base field F_p.

Fact 1 (Parseval's Identity)**.** $\dfrac{1}{\mathrm{card}(F)}\displaystyle\sum_{x\in F}|f(x)|^2 = \sum_{\alpha\in F}\left|\widehat{f}(\alpha)\right|^2$.

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 of character $|\chi_\alpha(x)| = 1$ for any α and x in F.

3 Insecurity Analysis

This section presents the full proof of main result (Theorem 1) that was outlined in the technical overview (Section 1.2).

3.1 Results Needed for Proof of Theorem 1

Lemma 1 (Chernoff Bound [McD98, Theorem 2.1])**.** *Let $X_1, X_2, \ldots, X_\lambda$ be independent Bernoulli random variables with $\mathbf{E}(X_i) = p$ 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 [O'D21, Chapter 3.3])**.** *Let $C \subseteq F^n$ denote the set of all shares of the secret $0 \in F = F_{p^\lambda}$. 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 $\vec{\ell} \in \Omega^n$.*

$$\Pr\left[\vec{\tau}(s) = \vec{\ell}\right] = \sum_{\vec{z}\in C^\perp}\left(\prod_{i=1}^{n}\widehat{\mathbb{1}}_{\tau_i^{-1}(\ell_i)}(z_i)\right)\cdot\chi_1(s\cdot\langle\vec{z},\vec{v}\rangle). \tag{28}$$

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

We will need a slight variation of the rearrangement inequality introduced in [Wu20].

Lemma 3 (Rearrangement Inequality)**.** *Consider non-negative reals $a_0, a_1, \ldots, a_T$ and n permutations $\pi^{(1)}, \ldots, \pi^{(n)}$ over the set $\{0, 1, \ldots, T\}$. Consider an $n \times (T+1)$ matrix A defined by*

$$A_{i,j} = a_{\pi^{(i)}(j)},$$

where $i \in \{1, 2, \ldots, n\}$ and $j \in \{0, 1, \ldots, T\}$. Let $\mathcal{S}$ be defined

$$\mathcal{S} := \left\{ j : \exists i \in \{1, \ldots, n\} \text{ such that } \pi^{(i)}(j) = 0 \right\} \subseteq \{0, 1, \ldots, T\}.$$

Then the following inequality holds:

$$\sum_{0 \leqslant j \leqslant T:\, j \notin \mathcal{S}} \prod_{i=1}^{n} a_{\pi^{(i)}(j)} = \sum_{0 \leqslant j \leqslant T:\, j \notin \mathcal{S}} \prod_{i=1}^{n} A_{i,j} \leqslant \sum_{j=1}^{T} a_j^n. \tag{29}$$

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

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

And hence,

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

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 Lemma 3, Lemma 4, and Lemma 5 can be found in Appendix A.

3.2 Proof of Theorem 1

Theorem 1. *For $\vec{\beta} \in (F^*)^n$, the $\mathsf{GenAdd}(\vec{\beta})$ 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

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \geqslant \mathcal{O}(n \log \log \lambda) + cn \log \lambda \tag{5}$$

for $\frac{1}{2} - \frac{1}{n} > c > 0$, then $\mathsf{GenAdd}(\vec{\beta})$ is $\mathcal{O}(\lambda^{-cn})$ insecure against the Hamming weight leakage.

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

$$2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big)$$
$$= \sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right| \tag{30}$$

Recall from Definition 6 that a weight $w \in \{0,1,\ldots,\lambda\}$ 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 $\vec{w} \in \{0,1,\ldots,\lambda\}^n \setminus \mathsf{Typical}(n,\tau)$. Chernoff bound (Lemma 1) implies that the probability mass on atypical weights contribute only negligibly to the statistical distance.

$$\sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$
$$\leqslant \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] + \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}]$$
(by triangle inequality)
$$\leqslant 2 \cdot \max_{s\in F} \left(\sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right)$$
$$= 2 \cdot \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},\widetilde{s})}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}]$$ (let $\widetilde{s}$ be the arg max)
$$= 2 \cdot \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},\widetilde{s})}[\overrightarrow{\mathrm{wt}}(\vec{s}) \notin \mathsf{Typical}(n,\tau)]$$
$$= 2 \cdot \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},\widetilde{s})}[\mathrm{wt}(s_1),\ldots,\text{or } \mathrm{wt}(s_n) \text{ is not typical}]$$ (definition of $\mathsf{Typical}(n,\tau)$)
$$\leqslant 2 \cdot \sum_{j=1}^{n} \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},\widetilde{s})}[\mathrm{wt}(s_i) \text{ is not typical}]$$ (by union bound)
$$\leqslant 2n \cdot 2\exp(-2\lambda t^2)$$ (by Chernoff bound (Lemma 1))

Hence, the expression for the statistical distance in Equation 30 becomes a summation over a typical set $\mathsf{Typical}(n,\tau)$ plus a negligible quantity.

(Equation 30)
$$= \sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$
$$= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$
$$\pm \sum_{\vec{w}\notin\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$
$$= \sum_{\vec{w}\in\mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] - \Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}] \right|$$

$$\pm\, 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \tag{31}$$

If $\vec{s} \in F^n$ is a share of secret 0, i.e. $\vec{s} \in C := \mathsf{GenAdd}(\vec{\beta}, 0)$, 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 $\vec{v} \in \mathsf{GenAdd}(\vec{\beta}, 1)$ we have

$$\begin{aligned}
\Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(\vec{\beta}, s)}\left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] &= \sum_{\vec{z} \in C^\perp} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(z_i)\right) \cdot \chi_1(s \cdot \langle \vec{z}, \vec{v} \rangle) \\
&= \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_1\left(s \cdot \zeta \cdot \left\langle \vec{\beta}, \vec{v} \right\rangle\right) \\
&= \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_1(s \cdot \zeta) \qquad (\text{because } \vec{v} \in \mathsf{GenAdd}(\vec{\beta}, 1)) \\
&= \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_\zeta(s) \qquad (32)
\end{aligned}$$

Moreover,

$$\begin{aligned}
\Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(\vec{\beta}, U_F)}\left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] &= \frac{1}{\mathrm{card}(F)} \sum_{s \in F} \Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(\vec{\beta}, s)}\left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] \\
&= \frac{1}{\mathrm{card}(F)} \sum_{s \in F} \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_\zeta(s) \qquad (\text{by Equation 32}) \\
&= \frac{1}{\mathrm{card}(F)} \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \sum_{s \in F} \chi_\zeta(s) \\
&= \frac{1}{\mathrm{card}(F)} \sum_{\zeta \in \{0\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \mathrm{card}(F) \qquad (\text{by Fact 2}) \\
&= \sum_{\zeta \in \{0\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \qquad (33)
\end{aligned}$$

Plugging these into the summand in Equation 31, we get

$$\begin{aligned}
&\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(\vec{\beta}, s)}\left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] - \Pr_{\vec{s} \leftarrow \mathsf{GenAdd}(\vec{\beta}, U_F)}\left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] \right| \\
&= \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \left| \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_\zeta(s) - \sum_{\zeta \in \{0\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \right| \qquad (\text{by Equation 32 and 33}) \\
&= \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \left| \sum_{\zeta \in F^*} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right) \cdot \chi_\zeta(s) \right| \qquad (\text{because } \chi_0(s) = 1 \text{ for all } s \in F) \\
&\leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^*} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \qquad (\text{by triangle inequality}) \qquad (34)
\end{aligned}$$

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

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

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.

$$(\text{Equation 34}) = \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| + \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \tag{35}$$

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,

$$\begin{aligned}
&\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\
&\qquad \leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta) \\
&\qquad = \left(2\lambda^{1/2+\tau}\right)^n \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} B(\beta_i \zeta) && (\text{because } \mathrm{card}(\mathsf{Typical}(n,\tau)) = (2\lambda^{1/2+\tau})^n) \\
&\qquad \leqslant \left(2\lambda^{1/2+\tau}\right)^n \sum_{\zeta \in F \setminus \{0, \zeta^*\}} B(\zeta)^n && (\text{by rearrangement lemma (Lemma 3)}) \\
&\qquad \leqslant 2^{n+1} \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{n\tau} \cdot \lambda^{-\frac{n}{2}+1} && (\text{by Lemma 4})
\end{aligned} \tag{36}$$

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

$$\begin{aligned}
&\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\
&\qquad \leqslant 2^n \cdot \lambda^{(\frac{1}{2}+\tau)\cdot n} \cdot n \cdot \max_{\substack{\vec{w} \in \mathsf{Typical}(n,\tau) \\ \zeta \in \mathcal{S}_{\vec{\beta}}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\
&\qquad \leqslant 2^n \cdot \lambda^{(\frac{1}{2}+\tau)\cdot n} \cdot n \cdot \lambda^{-\frac{n}{2}} \cdot \exp\left(-\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right) && (\text{by Lemma 5}) \\
&\qquad = (2\lambda^{\tau})^n \cdot n \cdot \exp\left(-\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right)
\end{aligned} \tag{37}$$

because the maximum of a sequence is at least as large as its average. Hence, Equation 35 becomes as follows, upon choosing $\tau = \frac{\log\left(\frac{n}{4}\log\lambda\right)}{2\log\lambda}$ (so that $2\lambda^{\tau} = (n\log\lambda)^{1/2}$):

$$\begin{aligned}
&(\text{Equation 35}) \\
&\qquad \leqslant (2\lambda^{\tau})^n \cdot n \cdot \exp\left(-\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right) + 2 \cdot 5^{\frac{5n}{2}-4} \cdot (2\lambda^{\tau})^n \cdot \lambda^{-\frac{n}{2}+1} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{by Equation 36 and 37})
\end{aligned}$$

$$\leqslant (n\log\lambda)^{n/2}\cdot n\cdot\exp\left(-\min_{\zeta\in\mathcal{S}_{\vec{\beta}}}\mathsf{Score}(\zeta;\vec{\beta})\right)+2\cdot 5^{\frac{5n}{2}-4}\cdot(n\log\lambda)^{n/2}\cdot\lambda^{-\frac{n}{2}+1} \tag{38}$$

Therefore, 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{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}]-\Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}]\right| && \text{(from Equation 30)}\\
&=\sum_{\vec{w}\in\mathsf{Typical}(n,\tau)}\left|\Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},s)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}]-\Pr_{\vec{s}\leftarrow\mathsf{GenAdd}(\vec{\beta},U_F)}[\overrightarrow{\mathrm{wt}}(\vec{s})=\vec{w}]\right|\pm 2\cdot 2n\cdot\exp(-2\lambda^{2\tau}) && \text{(from Equation 31)}\\
&\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}) && \text{(from Equation 34)}\\
&=\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|+2\cdot 2n\cdot\exp(-2\lambda^{2\tau}) && \text{(from Equation 35)}\\
&\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)+2\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}} && \text{(from Equation 38 and } \tau=\tfrac{\log\left(\frac{n}{4}\log\lambda\right)}{2\log\lambda}\text{)}\\
&\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}\\
&\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} && \text{(for sufficiently large } \lambda\text{)}
\end{aligned}$$

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

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

for some constant c. Then, from the above expression,

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

and this concludes the proof of Theorem 1. □

3.3 Worst-case Analysis

Recall from the statement and proof of Theorem 1 that the first summand (Equation 37) translates to the term containing the score function $\mathsf{Score}(\zeta; \vec{\beta})$ that quantifies the security of multipliers $\vec{\beta}$. However, one can bound the sum of Fourier coefficients (instead of taking the maximum and applying union bound) and prove that the scheme $\mathsf{GenAdd}(\vec{\beta}, s)$ has o(1) insecurity when not all elements in $\vec{\beta}$ are identical.

Theorem 2. *For $\vec{\beta} \in (F^*)^n$ and $\zeta \in \mathcal{S}_{\vec{\beta}}$, let $H(\zeta; \vec{\beta}) := \{i \colon \beta_i \zeta \neq \zeta^*\}$ and $\widetilde{h} = \min\limits_{\zeta \in \mathcal{S}_{\vec{\beta}}} \Big(\mathrm{card}(H(\zeta; \vec{\beta}))\Big)$. Then,*

$$\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \leqslant (\widetilde{h}+1) \cdot \left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}}$$

Proof of Theorem 2. We first upper bound the summand as follows.

$$\begin{aligned}
&\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \\
&\quad \leqslant \sum_{\vec{w} \in \{0,1,\ldots,\lambda\}^n} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \qquad (\text{as } \mathsf{Typical}(n,\tau) \subseteq \{0,1,\ldots,\lambda\}^n \text{ and } |\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)| \geqslant 0) \\
&\quad = \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \sum_{\vec{w} \in \{0,1,\ldots,\lambda\}^n} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \\
&\quad = \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i \in \{1,2,\ldots,n\}} \sum_{w_i=0}^{\lambda} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| \\
&\quad = \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \left(\prod_{i \in H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|\right) \cdot \left(\prod_{i \notin H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right|\right) \qquad (39)
\end{aligned}$$

Next, we separate bound the ℓ_1-norms on the right-hand side for those indices $i \in H(\zeta; \vec{\beta})$ and $i \notin H(\zeta; \vec{\beta})$.

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

$$\begin{aligned}
\sum_{w_i=0}^{\lambda} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i \zeta)\right| &\leqslant \sum_{w_i=0}^{\lambda} \binom{\lambda}{i}^{1/2} \cdot 2^{-\lambda/2} \cdot \binom{\lambda}{\mathrm{wt}(\beta_i\zeta)}^{-1/2} && (\text{by Claim 2}) \\
&= \binom{\lambda}{\mathrm{wt}(\beta_i\zeta)}^{-1/2} \sum_{w_i=0}^{\lambda} \binom{\lambda}{i}^{1/2} \cdot 2^{-\lambda/2} \\
&< \binom{\lambda}{\mathrm{wt}(\beta_i\zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4} && (\text{by Claim 5})
\end{aligned}$$

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

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

Substituting these values into Equation 39 and continuing the upper bound, we have:

$$(\text{Equation 39}) < \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i \in H(\zeta;\vec{\beta})} \binom{\lambda}{\mathrm{wt}(\beta_i \zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4} \tag{40}$$

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

$$\begin{aligned}(\text{Equation 40}) &\leqslant \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \lambda^{-\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{2}} \cdot \pi^{\mathrm{card}(H(\zeta;\vec{\beta}))} \cdot \lambda^{\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{4}} \\ &\leqslant (\widetilde{h}+1) \cdot \left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}} \qquad (\text{since } \mathrm{card}(\mathcal{S}_{\vec{\beta}}) \leqslant \widetilde{h}+1 \text{ [2]})\end{aligned}$$

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

Corollary 1. *For any $\vec{\beta} \in (F^*)^n$ such that $\vec{\beta} \neq (b,b,\ldots,b)$ for some $b \in F^*$, $\mathsf{GenAdd}(\vec{\beta})$ is $\mathcal{O}(\lambda)^{-1/4}$ insecure.*

Proof of Corollary 1. We follow the same direction as in the proof of Theorem 1. First, recall from Equation 31 and Equation 35 in the proof of Theorem 1 that

$$\begin{aligned}&2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \\ &\leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| + \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \quad (41)\end{aligned}$$

We bound the second summand as we did in the proof of Theorem 1 (Equation 36), but bound the first summand using Theorem 2.

$$\begin{aligned}(\text{Equation 41}) &\leqslant (\widetilde{h}+1) \cdot \left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}} + 2^{n+1} \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{n\tau} \cdot \lambda^{-\frac{n}{2}+1} + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \\ &\qquad\qquad (\text{recall that } \widetilde{h} := \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathrm{card}(H(\zeta;\vec{\beta}))) \\ &\leqslant 2\pi \cdot \frac{c}{\lambda^{1/4}} + 2^{n+1} \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{n\tau} \cdot \lambda^{-\frac{n}{2}+1} + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau}) \\ &\qquad\qquad (\text{because } \vec{\beta} \text{ cannot be of the form } (b,b,\ldots,b) \in (F^*)^n)\end{aligned}$$

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

[2] If $\zeta \in \mathcal{S}_{\vec{\beta}}$, then there should exist $j \in \{1,2,\ldots,n\}$ 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.

4 Open Problems

Following are the immediate open problem in light of our work.

1. $n = 2$ *parties.* Our recipe of using the Fourier proxy and upper bound it using the rearrangement inequality hits a natural bottleneck when $n = 2$. Even using the most optimistic estimates of Krawtchouk polynomial evaluations, Appendix C 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 $\mathsf{GenAdd}(\vec{\beta})$ 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. [FMM+24] when $n \geqslant 5$. The cases of general primes and, even for Mersenne primes, $n \in \{2, 3, 4\}$ remains open.

References

[Agi22] 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. ↑29

[BDIR18] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 531–561, Santa Barbara, CA, USA, August 19–23, 2018. Springer, Cham, Switzerland. doi:10.1007/978-3-319-96884-1_18. ↑1, 8

[BDIR21] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34(2):10, April 2021. doi:10.1007/s00145-021-09375-2. ↑1, 8

[BP23] 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. ↑2

[CT99] Thomas M. Cover and Joy A. Thomas. *Elements of information theory.* John Wiley & Sons, 1999. ↑4

[Dom08] 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. ↑9

[FMM+24] Sebastian Faust, Loïc Masure, Elena Micheli, Maximilian Orlt, and François-Xavier Standaert. Connecting leakage-resilient secret sharing to practice: Scaling trends and physical dependencies of prime field masking. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 316–344, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58737-5_12. ↑2, 8, 21

[GKP94] 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. ↑32

[GM15] Loıc Grenié and Giuseppe Molteni. Inequalities for the beta function. *Math. Inequal. Appl*, 18(4):1427–1442, 2015. doi:10.7153/mia-18-111. ↑29

[HMNY25] 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. URL: https://www.cs.purdue.edu/homes/hmaji/papers/HMNY24.pdf. ↑4

[JKK05] Norman L Johnson, Adrienne W Kemp, and Samuel Kotz. *Univariate discrete distributions*. John Wiley & Sons, 2005. ↑29

[KLM+09] 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. ↑25

[Kra01] 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. ↑6, 9, 31

[McD98] Colin McDiarmid. *Concentration*, pages 195–248. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998. doi:10.1007/978-3-662-12788-9_6. ↑13

[MNPW22] 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. ↑8

[MNPY24] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye. Constructing leakage-resilient Shamir's secret sharing: Over composite order fields. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024, Part IV*, volume 14654 of *Lecture Notes in Computer Science*, pages 286–315, Zurich, Switzerland, May 26–30, 2024. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58737-5_11. ↑2

[MPSW21] Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. Constructing locally leakage-resilient linear secret-sharing schemes. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 779–808, Virtual Event, August 16–20, 2021. Springer, Cham, Switzerland. doi:10.1007/978-3-030-84252-9_26. ↑8

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

[O'D21] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2021. Available online as arXiv:2105.10386v1. ↑13

[OWZ11] 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. ↑25

[Pai24] Jean-Christophe Pain. On an upper bound for central binomial coefficients and catalan numbers. *arXiv preprint arXiv:2407.21064*, 2024. ↑29

[Rud52] Harry D Ruderman. Two new inequalities. *The American Mathematical Monthly*, 59(1):29–32, Jan 1952. doi:10.2307/2307185. ↑12

[Sas99] Zoltán Sasvári. Inequalities for binomial coefficients. *Journal of Mathematical Analysis and Applications*, 236(1):223–226, Aug 1999. doi:10.1006/jmaa.1999.6420. ↑30

[ST11] 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. ↑25

[Tao12] Terence Tao. *Topics in random matrix theory*, volume 132. American Mathematical Soc., 2012. ↑29

[Top07] 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. ↑29

[VL98] Jacobus Hendricus Van Lint. *Introduction to coding theory*, volume 86. Springer Science & Business Media, 1998. ↑6

[Wu20] Chai Wah Wu. On rearrangement inequalities for multiple sequences. *arXiv preprint arXiv:2002.10514*, 2020. ↑14, 24

[Zhu18] Shengxin Zhu. Summation of gaussian shifts as jacobi's third theta function. *arXiv preprint arXiv:1806.08474*, 2018. ↑32

A Proof of Lemmas used in Theorem 1

A.1 Proof of Our Rearrangement Inequality (Lemma 3)

Lemma 3 (Rearrangement Inequality)**.** *Consider non-negative reals $a_0, a_1, \ldots, a_T$ and n permutations $\pi^{(1)}, \ldots, \pi^{(n)}$ over the set $\{0, 1, \ldots, T\}$. Consider an $n \times (T+1)$ matrix A defined by*

$$A_{i,j} = a_{\pi^{(i)}(j)},$$

where $i \in \{1, 2, \ldots, n\}$ and $j \in \{0, 1, \ldots, T\}$. Let $\mathcal{S}$ be defined

$$\mathcal{S} \;:=\; \Big\{\, j : \exists i \in \{1, \ldots, n\} \text{ such that } \pi^{(i)}(j) = 0 \,\Big\} \subseteq \{0, 1, \ldots, T\}.$$

Then the following inequality holds:

$$\sum_{0 \leqslant j \leqslant T\colon\, j \notin \mathcal{S}} \prod_{i=1}^{n} a_{\pi^{(i)}(j)} = \sum_{0 \leqslant j \leqslant T\colon\, j \notin \mathcal{S}} \prod_{i=1}^{n} A_{i,j} \leqslant \sum_{j=1}^{T} a_j^n. \tag{29}$$

Proof of Lemma 3. Consider a new $n \times (T+1)$ matrix B defined by

$$B_{i,j} \;:=\; \begin{cases} 0, & \text{if } \pi^{(i)}(j) = 0 \\ A_{i,j}, & \text{otherwise.} \end{cases}$$

We remark that for every row i, there is exactly one j where the first condition of the assignment is satisfied because $\pi^{(i)}$ is a permutation. So, the i-th row of B has a permutation of $a_1, \ldots, a_T$ and an extra 0 (corresponding to where the first case in the definition was used in the assignment). Note that

$$\sum_{0 \leqslant j \leqslant T\colon\, j \notin \mathcal{S}} \prod_{i=1}^{n} A_{i,j} = \sum_{j=0}^{T} \prod_{i=1}^{n} B_{i,j}. \tag{42}$$

Therefore, it suffices to upper-bound the expression involving $B_{i,j}$s instead.

Next, we will use the rearrangement lemma presented in [Wu20, Lemma 1]. Let B' be the $n \times (T+1)$ matrix where each row of B is sorted in increasing order. By this rearrangement lemma, we get

$$\sum_{j=0}^{T} \prod_{i=1}^{n} B_{i,j} \leqslant \sum_{j=0}^{T} \prod_{i=1}^{n} B'_{i,j}. \tag{43}$$

Note that

$$\sum_{j=0}^{T} \prod_{i=1}^{n} B'_{i,j} = \sum_{j=1}^{T} \prod_{i=1}^{n} B'_{i,j} = \sum_{j=1}^{T} a_j^n, \tag{44}$$

because every row has a 0, and, therefore, the first column of B' is all 0s. Finally, the entries $B'_{i,1}, \ldots, B'_{i,T}$ are sorting of the sequence $a_1, \ldots, a_T$.

Putting these together, using Equation 42, Equation 43, and Equation 44 sequentially, we get our bound as follows:

$$\sum_{0 \leqslant j \leqslant T\colon\, j \notin \mathcal{S}} \prod_{i=1}^{n} A_{i,j} = \sum_{j=0}^{T} \prod_{i=1}^{n} B_{i,j} \leqslant \sum_{j=0}^{T} \prod_{i=1}^{n} B'_{i,j} = \sum_{j=1}^{T} a_j^n.$$

This completes our proof. □

A.2 Proof of Upper Bounds of Fourier Coefficients (Lemma 4 and Lemma 5)

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

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

Proof of Claim 1. By definition of Fourier transformation,

$$\widehat{\mathbb{1}}_w(\zeta) := \frac{1}{2^\lambda} \sum_{x \in F} \mathbb{1}_w(x) \cdot (-1)^{\langle \zeta, x \rangle} = \frac{1}{2^\lambda} \sum_{\substack{x \in F \\ \mathrm{wt}(x) = w}} (-1)^{\langle \zeta, x \rangle} = \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}(\zeta)} (-1)^k \cdot \#\{x \colon \langle \zeta, x \rangle = k\}$$

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

$$\#\{x \colon \langle \zeta, x \rangle = k\} = \binom{\mathrm{wt}(\zeta)}{k} \binom{\lambda - \mathrm{wt}(\zeta)}{w-k}$$

and therefore,

$$\widehat{\mathbb{1}}_w(\zeta) = \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}(\zeta)} (-1)^k \cdot \#\{x \colon \langle \zeta, x \rangle = k\} = \frac{1}{2^\lambda} \sum_{k=0}^{\mathrm{wt}(\zeta)} (-1)^k \binom{\mathrm{wt}(\zeta)}{k} \binom{\lambda - \mathrm{wt}(\zeta)}{w-k}$$

as desired. □

Remark 5. *Observe from Claim 1 above that the value of $\widehat{\mathbb{1}}_w(\zeta)$ depends only on w and $\mathrm{wt}(\zeta)$. In other words, $\widehat{\mathbb{1}}_w(\zeta)$ is a symmetric function in the sense that it is invariant to the permutation of digits of ζ. 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 [KLM+09, ST11, OWZ11], for more details).*

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

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

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

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

$$\binom{\lambda}{w} \leqslant \binom{\lambda}{\lfloor \lambda/2 \rfloor} \leqslant \frac{2^\lambda}{\sqrt{\pi \lambda / 2}} \leqslant \frac{2^\lambda}{\sqrt{\lambda}} \tag{45}$$

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 idetity.

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

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

$$\sum_{\alpha\in F}\widehat{\mathbb{1}}_w(\alpha)^2 = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x)^2 \tag{46}$$

Simplifying the left-hand side of Equation 46, 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 46, note that, for any $\zeta \in F^*$,

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

where the last equality comes from the observation made in Remark 5. Putting these into Equation 46 then gives us the following:

$$\begin{aligned}
\sum_{\alpha\in F}\widehat{\mathbb{1}}_w(\alpha)^2 = \frac{1}{\mathrm{card}(F)}\sum_{x\in F}\mathbb{1}_w(x)^2 \implies \frac{1}{2^\lambda}\binom{\lambda}{w} &\geqslant \binom{\lambda}{\mathrm{wt}(\zeta)}\left|\widehat{\mathbb{1}}_w(\zeta)\right|^2 \\
\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| &\leqslant \frac{1}{2^{\lambda/2}}\binom{\lambda}{w}^{1/2}\binom{\lambda}{\mathrm{wt}(\zeta)}^{-1/2} \\
\implies \left|\widehat{\mathbb{1}}_w(\zeta)\right| &\leqslant \frac{1}{\lambda^{1/4}}\binom{\lambda}{\mathrm{wt}(\zeta)}^{-1/2} \qquad (\because \text{Equation 45})
\end{aligned}$$

as desired. □

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

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

And hence,

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

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

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

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

$$\leqslant \sqrt{\frac{4}{\pi \mathrm{e}}} \cdot \frac{1}{\lambda} \leqslant \frac{1}{\lambda} \qquad \text{(by Corollary 3)}$$

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,

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

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

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

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.

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

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

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

as desired. □

From Lemma 4, note that

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

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 $\vec{w}=(w_1,w_2,\dots,w_n)\in\{1,2,\dots,\lambda\}^n$,*

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

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

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

Otherwise (if $\mathrm{wt}(\beta_i\zeta)\in\{0,\lambda\}$), we have $\Big|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\Big|\leqslant\lambda^{-1/2}$, and therefore

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

which proves the lemma. □

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 [Agi22] and Pain [Pai24], which will simplify our analysis later.

Corollary 2 (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 $\binom{2n}{n-x} \to \binom{2n}{n} \cdot \exp\left(-x^2/n\right)$, for fixed x/n as $n \to \infty$. Berry-Esseen [Tao12, Chapter 2.2] and Camp-Paulson [JKK05, 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 3. *For $x \in (0, 1]$, we have $x \leqslant \exp\left(-2 \cdot \frac{1-x}{1+x}\right)$.*

Proof. 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. □

[Top07] presents tighter bounds. 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 [Top07, Table 1]. In general, such bounds are a consequence of the identity [Top07, Equation 28].

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

$$\begin{aligned}
\binom{2n}{n-x} &= \binom{2n}{n} \cdot \frac{(n-x+1)\cdots n}{(n+1)\cdots(n+x)} \\
&= \binom{2n}{n} \cdot \prod_{i=1}^{x} \frac{n-x+i}{n+x-i+1} && \text{(rearranging)} \\
&\leqslant \binom{2n}{n} \cdot \prod_{i=1}^{x} \exp\left(-2 \cdot \frac{2x-2i+1}{2n+1}\right) && \text{(using Claim 3)} \\
&= \binom{2n}{n} \cdot \exp\left(-2 \cdot \frac{2x^2 - x(x+1) + x}{2n+1}\right) = \binom{2n}{n} \cdot \exp\left(-\frac{x^2}{n+1/2}\right).
\end{aligned}$$

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. [GM15], 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, [Sas99, Corollary 1]); however, for our application, this elementary estimate suffices. □

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,

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

This completes the proof of the second inequality. □

C Optimistic Analysis

In this appendix, 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

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

In preparation for using the rearrangement lemma, 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.

$$\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in F^*\setminus\mathcal{S}_{\vec{\beta}}}\prod_{i=1}^{n}B(\,\mathrm{wt}(\beta_i\zeta)\,;w_i)$$

$B(z;w)$ will have the property that it will decrease as z gets closer to $\lambda/2$. When satisfying this property, we can use the rearrangement lemma to upper-bound the expression above and we rearrange this expression.

$$\begin{aligned}
&\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{\zeta\in F\setminus\{0,\zeta^*\}}\prod_{i=1}^{n}B(\,\mathrm{wt}(\zeta)\,;w_i)\\
&=\sum_{\vec{w}\in\{0,1,\ldots,\lambda\}^n}\sum_{1\leqslant z\leqslant\lambda-1}\binom{\lambda}{z}\prod_{i=1}^{n}B(z;w_i)\\
&=\sum_{1\leqslant z\leqslant\lambda-1}\binom{\lambda}{z}\cdot\left(\sum_{w\in\{0,1,\ldots,\lambda\}}B(z;w)\right)^n
\end{aligned}\tag{47}$$

So, we need an estimate for $\sum_w B(z;w)$. $B(n;w)$ is an upper bound on the evaluation of the Krawtchouk polynomial. The most optimistic estimates from [Kra01, 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

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

[4]The result of [Kra01, 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 $\lambda^{-1}\cdot\binom{\lambda}{w}2^{-\lambda}$.

$$= \lambda^{-1/4} \binom{\lambda}{z}^{-1/2}.$$

The last equality uses the asymptotic estimate from [GKP94, Answer to Problem 9.18 on page 593].[5] We substitute this estimate back in Equation 47 to get our overall upper bound on the second summand.

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

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

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

D Some Estimates: Sum of Powers of Binomial Coefficients

Claim 4. *For arbitrary $\theta \in \mathbb{R}$ and $m \in \mathbb{R}_{>0}$, the following bound holds.*

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

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, [Zhu18, Theorem 2.2] proved the following estimate.

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

Proof of Claim 4. 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,

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

This completes the proof of the claim. □

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

Remark 6. *We can prove the tighter bound*

$$\sum_{\Delta\in\theta+\mathbb{Z}} \exp\bigl(-\Delta^2/m\bigr) \leqslant \sqrt{\pi m} + \exp\Bigl(-\widehat{\theta}^2/m\Bigr),$$

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 5. *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 5. Consider the following manipulation.

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

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

Remark 7. *In general, for* $p \in (0, 1]$*, we can prove that*

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

E 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*

$$\exp(-x^2/a) \cdot x^k \leqslant \begin{cases} 1, & \text{if } k = 0. \\ (ka/2\mathrm{e})^{k/2}, & \text{otherwise.} \end{cases} \tag{48}$$

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

Proof. In this proof we will repeatedly use the bound

$$\exp\left(-\frac{2x^2}{m+1}\right)\cdot(2x)^k \leqslant \left(k\cdot\frac{m+1}{\mathrm{e}}\right)^{k/2}, \tag{49}$$

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

1. For $m \geqslant 1$,

$$\begin{aligned}
\exp\left(-\frac{2x^2}{m+1}\right)\cdot\frac{2x}{m} &\leqslant \left(\frac{m+1}{\mathrm{e}}\right)^{1/2}\cdot\frac{1}{m} && \text{(using Equation 49 with } k=1\text{)}\\
&= \left(\frac{m+1}{\mathrm{e}m}\right)^{1/2}\cdot\frac{1}{m^{1/2}}\\
&\leqslant (2/\mathrm{e})^{1/2}\cdot\frac{1}{m^{1/2}}. && \text{(bound holds for } m\geqslant 1\text{)}
\end{aligned}$$

2. For $m \geqslant 2$,

$$\begin{aligned}
\exp\left(-\frac{2x^2}{m+1}\right)\cdot\frac{\left|(2x)^2-m\right|}{m(m-1)} &\leqslant \exp\left(-\frac{2x^2}{m+1}\right)\cdot\frac{(2x)^2+m}{m(m-1)}\\
&= \exp\left(-\frac{2x^2}{m+1}\right)\cdot\frac{(2x)^2}{m(m-1)} + \exp\left(-\frac{2x^2}{m+1}\right)\cdot\frac{1}{(m-1)}\\
&\leqslant \left(2\cdot\frac{m+1}{\mathrm{e}}\right)\cdot\frac{1}{m(m-1)} + \frac{1}{m-1}\\
&&& \text{(using Equation 49 with } k\in\{2,0\}\text{)}\\
&= \left[\frac{2(m+1)}{\mathrm{e}(m-1)} + \frac{m}{m-1}\right]\cdot\frac{1}{m}\\
&\leqslant (6/\mathrm{e}+2)\cdot\frac{1}{m} && \text{(bound holds for } m\geqslant 2.\text{)}
\end{aligned}$$

□