Resilience of Inner-Product Masking Scheme Against Hamming Weight Leakage

Aniruddha Biswas
Department of Computer Science, Purdue University, West Lafayette, IN, USA

Jihun Hwang
Department of Computer Science, Purdue University, West Lafayette, IN, USA

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

Xiuyu Ye
Department of Computer Science, Purdue University, West Lafayette, IN, USA

Abstract

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

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

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

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

Digital Object Identifier 10.4230/LIPIcs.ITC.2026.9

Related Version *Full Version*: `https://www.cs.purdue.edu/homes/hmaji/papers/BHMY26.pdf`

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

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

1 Introduction

Side-channel attacks have repeatedly compromised cryptographic secrets by exploiting observable side effects of a device's physical operation. *Masking* [9,21] is a widely prevalent and effective countermeasure; it splits the secret into shares, relying on the noise in measurements from individual shares to accumulate quickly and obscure the secret.

Additive masking, a prominent masking strategy, splits a secret s into random $(s_1, s_2, \ldots, s_n)$ shares satisfying $s_1 + s_2 + \cdots + s_n = s$. The security provided by this scheme has its limitations; even with noisy measurements, a carefully chosen attack can still reveal partial information about the secret. For example, over any finite field, single-bit probes into the devices storing the shares reveal information about the secret [1, 30, 31, 33]. *Over binary*

extension fields, even power analysis and timing attacks [26, 27] *that reveal only the number of set bits of shares (a.k.a., their Hamming weight) compromise this masking – the secret's Hamming weight and the sum of all the leaked Hamming weights always have the same parity.* However, over exceptionally specialized and rare Mersenne-prime fields, weak security guarantees are known against such attacks [17].

In comparison, *inner-product masking* [2,3], a mild generalization of additive masking, has demonstrated significant potential for achieving greater security across all finite fields. Such a scheme is parameterized by its *reconstruction multipliers* $\vec{\beta} \in (F^*)^n$, where F is the ambient finite field, and the corresponding shares $(s_1, s_2, \ldots, s_n)$ satisfy $\beta_1 \cdot s_1 + \beta_2 \cdot s_2 + \cdots + \beta_n \cdot s_n = s$. Observe that $\vec{\beta} = (1, 1, \ldots, 1)$ reduces it to additive masking; however, carefully selecting these multipliers $\vec{\beta}$ can significantly enhance security. For instance, over any field, nearly all multipliers $\vec{\beta}$ offer strong security guarantees when the number of set bits of each share is revealed [18]. While nearly all multipliers offer strong security, we cannot identify them, nor can we determine the level of security provided by a specific multiplier.

This work contributes to the ongoing investigations into the security of inner product masking and, by extension, provides guidelines for NIST's ongoing standardization efforts for more secure secret-sharing schemes [7].

Summary of our results. As in [17, 18], we investigate the *local leakage resilience* [4, 5] of inner-product masking against *Hamming weight leakage* from shares, where the number of set bits in each share is revealed. This is a strong security metric, requiring statistical independence between the secret and the leakage, and it implies other security metrics in the literature, such as statistical bias [13], mutual information [19], and guessing entropy [40].

In this work, we establish that inner-product masking is *always* as secure as additive masking over any field, thereby ruling out the possibility of "vulnerable" multipliers that could undermine security – a gap left open in the analysis of [18]. Over binary extension fields, while additive masking is vulnerable, as indicated above, we prove that it is (essentially) the *only* vulnerable scheme; all other inner product masking schemes are secure. We present an efficiently computable *score function* for multipliers, where a higher score indicates greater security of the corresponding inner-product masking. Our score function enables *certifying* the security achieved by a specific multiplier, facilitating efforts similar to those in [14–16]. It helps explicitly identify multipliers with strong security, whose existence was proven in [18]. From a randomness extractor perspective: the inner product with random (public) multipliers is already a strong extractor; our contribution is to deterministically identify multipliers that yield a good inner-product extractor.

The results above stem from more general technical findings, also applicable to the local leakage resilience of secret-sharing schemes and polynomial masking [20, 39]. Our approach is Fourier-analytic and relies on spectral-norm estimates of the Hamming slice, which, in turn, require the asymptotic properties of Krawtchouk polynomials [29, 41].

1.1 Preliminaries

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

Field extensions. Elements of an extension field F_{2^λ} are represented as $F_2[Z]/\Pi(Z)$ elements, where $\Pi(Z)$ is a monic irreducible polynomial of degree λ. We can view F_{2^λ} as a vector space F_2^λ after choosing a basis $\mathcal{B} = (b_1, \ldots, b_\lambda)$. The *Hamming weight* $\mathrm{wt}_\mathcal{B}(\zeta) \in \{0, 1, \ldots, \lambda\}$ is

the number of 1's in the vector representation of $\zeta \in F_{2^\lambda}$ in F_2^λ under $\mathcal{B}$; we omit $\mathcal{B}$ unless it has to be specified. Let $\mathsf{Tr}_{F_{2^\lambda}/F_2}\colon F_{2^\lambda} \to F_2$ be the field trace of the field extension F_{2^λ}/F_2. The *trace-dual coordinate vector* of $\zeta \in F_{2^\lambda}$ is $\zeta^\vee := (\mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_1), \ldots, \mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta b_\lambda)) \in F_2^\lambda$ and its Hamming weight $\mathrm{wt}(\zeta^\vee) =: \mathrm{wt}^\vee(\zeta)$ is called the *trace-dual Hamming weight* of ζ.

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

Leakage resilience. Fix a secret sharing scheme $\mathcal{S}$. Let $\tau_i\colon F \to \Omega_i$ be a leakage function, and let $\vec{\tau}(s)$ denote the joint leakage distribution $(\tau_1(s_1), \ldots, \tau_n(s_n))$, where $\mathcal{S}$ generates shares $(s_1, \ldots, s_n)$ of s. $\vec{\tau}(U_F)$ will denote the leakage distribution when the secret is chosen uniformly at random from F. The *local leakage resilience* of $\mathcal{S}$ against the leakage attack $\vec{\tau}$ is defined by [4, 5]:

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

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

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

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

Note that this function can be computed efficiently [6, 8].

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

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

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

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

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

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

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

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

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

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

1.2 Our Results

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

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

Except for those inner product masking that are essentially equivalent to the additive masking in the local leakage resilience context, everyone else is secure. Theorem 4 states this result formally. Next, we characterize choices of $\vec{\beta} \in (F^*)^n$ that allow us to derive stronger security bounds for $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$, where insecurity decays $\lambda^{-\Theta(n)}$. This characterization builds on the following technical result.

▶ **Informal Theorem 8.** *For $n \in \{3, 4, \ldots\}$ parties and $\vec{\beta} \in (F^*)^n$, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is λ^{-cn}-insecure, where $c \in (0, 1/2 - 1/n)$ satisfies*

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

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

We leave the case $n = 2$ as an open problem for both results. For clarity of presentation, we ignore additive $\log\log\lambda$ terms in the right-hand side of the expression above (Equation 5). See Theorem 8 for the full expression.

Given $\vec{\beta}$, one can efficiently compute its trace-dual weights and test whether the minimum score is $\geqslant cn \log \lambda$ or not, i.e. verify Equation 5 (see for example [42]). For example, if all elements of $\vec{\beta}$ are identical, we know already that the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is insecure. In this case, the minimum score is 0 and our technical result cannot upper bound the insecurity by a small quantity.

▶ Remark 2 (Consequences of Theorem 4 and 8). The following corollaries are immediate:

1. If every element in $\vec{\beta}$ occurs at most m times, then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ satisfies Equation 5 with $c = (n - m)/4n$. This is because for $\zeta \in \mathcal{S}_{\vec{\beta}}$, $\beta_i \zeta$ is either equal to ζ^* or has dual weight $\in \{1, 2, \ldots, \lambda - 1\}$. Since every element in $\vec{\beta}$ occurs at most m times, at least $(n - m)$ elements in $\{\zeta\beta_1, \ldots, \zeta\beta_n\}$ have dual weight $\in \{1, 2, \ldots, \lambda - 1\}$. Therefore, the score is $\geqslant (n - m) \cdot (1/4) \log \lambda$; whence, the result. In particular, if all elements of $\vec{\beta}$ are distinct, then $m = 1$ and $c = (n - 1)/4n$. Moreover, when $\vec{\beta}$ is chosen uniformly at random from F^n, then with exponentially high probability, it consists of distinct elements from F^*.
2. A *symmetric* function $f \colon F \to \Omega$ satisfies the constraint "$\mathrm{wt}(x) = \mathrm{wt}(y)$ implies $f(x) = f(y)$" for $x, y \in F$. Let $\mathcal{F}$ denote the set of all symmetric functions. A *symmetric local leakage* leaks $f_1, \ldots, f_n$ from the shares $s_1, \ldots, s_n$, where $f_1, \ldots, f_n \in \mathcal{F}$.

Note that given only the $\mathrm{wt}(x)$, one can compute $f(x)$ for a symmetric function; i.e., $x \to \mathrm{wt}(x) \to f(x)$ is a Markov chain. Therefore, by the data processing inequality (see [10, Chapter 2]), any secret sharing scheme that has ε insecurity against the Hamming weight leakage has ε insecurity against *every* symmetric local leakage.

Theorem 8 also gives a systematic way to select reconstruction multipliers $\vec{\beta} \in (F^*)^n$.

▶ **Informal Corollary 9.** *Let $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F^*)^n$ If for every β_i there exists another β_j such that $\beta_j \zeta^* \beta_i^{-1}$ has non-extreme (close to neither 0 nor λ) dual Hamming weight, then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ satisfies Equation 5 for all sufficiently large λ.*

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

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

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

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

Corollary 9 also allows us to extend our results to the security of Shamir's secret sharing with random evaluation points; see Remark 31.

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

▶ **Informal Theorem 10.** *Let F_q be a finite field of order q and $\vec{\beta} \in (F_q^*)^n$. Then $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is secure against the leakage $\vec{\tau} = (\tau_1, \tau_2, \ldots, \tau_n)$ if Add_n is "sufficiently secure" on average over $i \in \{1, 2, \ldots, n\}$ against $\vec{\tau_i} = (\tau_i, \tau_i, \ldots, \tau_i)$.*

This result implies that one could verify the security of a generalized additive secret sharing against a certain leakage, by testing whether the additive secret sharing (i.e. when all reconstruction multipliers are 1) is *sufficiently secure* against leakage attacks where the same leakage function is applied to every share. Here, the notion of strong security comes from the fact that we need the upper bound of insecurity to be small, not the insecurity itself. See Theorem 10 for the precise statement with exact expressions.

It is worthwhile to note that Theorem 10 applies to *any* finite field. Consequently, we can also derive security guarantees against Hamming weight leakage for schemes over prime fields, including those based on Mersenne primes, by combining our generalized bound with the results of Faust et al. [17].

▶ Remark 3 (Technical subtlety in Theorem 10). Benhamouda et al. [4] introduced the quantity called *Fourier proxy* that measures the local leakage resilience (Equation 1). Proving that this proxy (or its upper bound) is small is a popular technique to demonstrate that the insecurity is small [4, 5, 24, 25, 30, 33, 34, 37].

In Theorem 10, we show that the proxy of the inner product masking is at most an upper bound of the proxy for additive masking, induced by triangle inequality, hence the terminology *sufficiently secure*. We *did not* prove that the insecurity of the inner product masking is at most the insecurity of the additive scheme directly.

1.3 Technical Overview

Our results are best interpreted by considering the number of parties $n \in \{3, 4, \dots\}$ to be a constant and determining the asymptotics of insecurity as a function of the security parameter λ. Consider $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$, for arbitrary $\vec{\beta} \in (F^*)^n$. In this section, we illustrate our analysis strategy against the Hamming weight leakage; we present formal proofs formally in Section 3.

The analysis relies on spectral-norm estimates of the Hamming slice, which in turn require the asymptotic properties of Krawtchouk polynomials [29, 41]. Existing techniques such as bounding the spectral norm of the Hamming slice via polynomial threshold function estimates, do not yield bounds sufficiently tight for our purposes. See Figure 1 for a visualization of the gap between spectral weights at each level; see full version for the further discussion. One modern tool for estimating the spectral norm of Hamming slices is the use of level-k inequalities; details are likewise deferred to the full version.

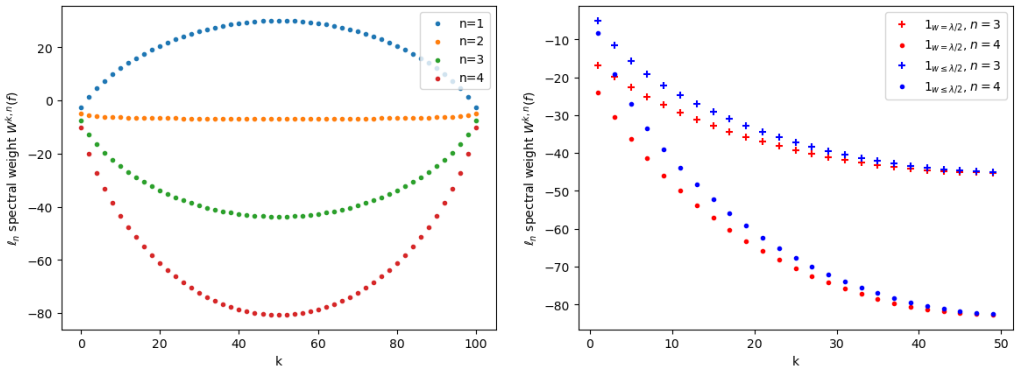

Figure 1 Distribution of ℓ_n-spectral weight at level-k of $f\colon F_{2^\lambda} \to \{0,1\}$, i.e. $W^{k,n}(f) := \sum_{S\colon \mathrm{wt}(S)=k} |\hat{f}(S)|^n$.
[Left] x-axis: $k \in \{0, 1, \dots, \lambda\}$. y-axis: $W^{k,n}(\mathbb{1}_{w=\lambda/2})$ (log-scaled) for $n = 1$ (blue), 2 (orange),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

Main Technical Result and Proof Outline

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

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

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

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

Here, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)$ denotes the distribution of shares over F^n for secret $s \in F$, and $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)$ the distribution of shares for a uniformly random secret in F. Note that each share s_i is uniformly random over F, irrespective of the secret. Therefore, the (marginal) distribution of the Hamming weight of any share is the binomial distribution $B(\lambda, 1/2)$. By Chernoff bound (Lemma 24), it is unlikely that the Hamming weight of any share is significantly far from $\lambda/2$. In particular, for a parameter $\tau \in (0, 1/2]$, the Hamming weight of a share being $\geqslant \lambda^{1/2+\tau}$ far from $\lambda/2$, is at most $2 \cdot \exp(-2\lambda^{2\tau})$. We can control this probability of "atypical weights" by setting $\tau = \frac{\log((n/4)\cdot\log\lambda)}{2\log\lambda}$ and driving the probability below $\lambda^{-n/2}$.

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

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

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

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

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

To this end, we will use Fourier analysis. Using the Poisson summation formula (Lemma 25) for the generalized additive secret sharing, we can rewrite the right-hand side expression in terms of Fourier coefficients.

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

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

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

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

To approach this estimation problem, and appreciate our key technical components, let us build some elementary intuition of the magnitude of the Fourier coefficients $\widehat{\mathbb{1}}_w(\cdot)$. We remark that $\widehat{\mathbb{1}}_w(x) = 2^{-\lambda} K_w(\mathrm{wt}^\vee(x))$ where $K_w(\cdot)$ is a Krawtchouk polynomial, as defined in [28]. Krawtchouk polynomials find extensive applications in many subfields in mathematics, theoretical computer science, and cryptography; see, for example, [41].

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

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

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

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

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

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

Second summand estimation. We prove an upper bound on the magnitude $|\widehat{\mathbb{1}}_{w_i}(x)| \leqslant B(x)$ as defined in Lemma 27, for all $x \in F \setminus \{0, \zeta^*\}$. Using this bound, we have:

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

The last equality substitutes the cardinality of the $\mathsf{Typical}(n,\tau)$ set. Now, using (generalized) Hölder's inequality (Lemma 26), we have

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

We show that this n-th norm, for $n \geqslant 3$, is small. Roughly speaking, Lemma 27 upper bounds the right-hand side expression as follows:

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

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

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

▶ Remark 5. Determining the estimates $B(x)$ is equivalent to estimating the evaluations of Krawtchouk polynomials. We require concrete estimates, not asymptotics such as the one in [12]. Elementary estimates suffice for our applications; tighter estimates, for example, those in [28, Section 3], do not yield any qualitative improvement of our results. We present upper bounds on such estimates in the appendix of the full version.

▶ Remark 6 (A world without estimating the higher order spectral norm). Suppose we upper bound the second summation using prior techniques as used in [4, 5, 17, 32, 34]; they did not analyze the ℓ_n norm. They upper bound the second summand using the ℓ_∞ norm and the ℓ_2 norm of the Fourier coefficients. Using our tight estimate of $B(x) = \lambda^{-1}$, when $\mathrm{wt}^{\vee}(x) = 1$, the old strategy will yield an upper bound of $\mathsf{poly}(\log\lambda) \cdot \lambda^{-(n-2)-(1/2)+n/2}$, which will be $o(1)$ only for $n \geqslant 4$. Our upper bound is tighter; it is $o(1)$ for $n \geqslant 3$. Detailed discussions are available in the appendix of the full version.

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

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

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

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

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

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

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

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

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

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

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

Define $\zeta' := \beta_i\zeta$. Observe that $\zeta' \in F\setminus\{0,\zeta^*\}$. A standard application of the Parseval's identity (Fact 22) yields the estimate (see Lemma 27 for details):

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

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

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

Using this upper bound on the Fourier coefficient, we have

$$\begin{aligned}\sum_{w_i\in\{0,1,\ldots,\lambda\}}\left|\widehat{\mathbb{1}}_{w_i}(\zeta')\right| &\leqslant 2^{-\lambda/2}\lambda^{-1/2}\sum_{w_i\in\{0,1,\ldots,\lambda\}}\binom{\lambda}{w_i}^{1/2}\\ &< 2^{-\lambda/2}\lambda^{-1/2}\ \cdot\ \pi 2^{\lambda/2}\lambda^{1/4} = \pi\lambda^{-1/4} \qquad \text{(by Claim 29)}\end{aligned}$$

which is what we set out to prove.

▶ Remark 7 (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

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

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

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

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

The "small" quantity in the insecurity upper-bound is (roughly) $\lambda^{-n/2+1}$, which is o(1), for $n \geqslant 3$. This wraps up the proof overview of Theorem 4.

Which schemes are most secure?

Theorem 4 shows that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is secure against Hamming weight leakage as long as the reconstruction multiplier $\vec{\beta}$ is not a constant vector; in other words, the only instance where the generalized additive secret sharing becomes insecure is when it is equivalent to the additive secret sharing. Does this mean all choices of $\vec{\beta}$ are equally secure, or can some choices offer even stronger security? In other words:

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

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

▶ **Theorem 8.** *For $\vec{\beta} \in (F^*)^n$, the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ secret sharing scheme is ε insecure against the Hamming weight leakage, where*

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

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

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

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

Choosing $\vec{\beta}$ more carefully, by maximizing the minimum score, can lead to a faster reduction in insecurity (as shown in Corollary 9). We now present a different strategy to upper bound the first summand. Below is a brief overview of the proof of this theorem.

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

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

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

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

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

Equation 3 presents the definition of our score function and Lemma 30 proves that it satisfies the equation above. This definition does not depend on w_i, only on the dual Hamming weights $\mathrm{wt}^\vee(\zeta\beta_i)$, where $i \in \{1, 2, \dots n\}$. As a consequence, we get the following upper bound for the first summand, upon substituting our value of τ:

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

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

Theorem 8 then yields a way to choose reconstruction multipliers $\vec{\beta} \in (F^*)^n$ ensuring the security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$.

▶ **Corollary 9.** *Let $n \geqslant 3$ and $\vec{\beta} = (\beta_1, \dots, \beta_n) \in (F^*)^n$ where for every β_i, there exists some $\beta_j \neq \beta_i$ such that*

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

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

Over arbitrary fields

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

▶ **Theorem 10** (Diagonalization)**.** *Let F_q be a finite field of order q. Let $\vec{\beta} = (\beta_1, \dots, \beta_n) \in (F_q^*)^n$ be multipliers and $\vec{\tau} = (\tau_1, \dots, \tau_n)$ be the leakage. Define*

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

Then,

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

▶ Remark 11. Combining Theorem 10 with the result of Faust et al. [17], we immediately obtain that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ over F_p, where $p = 2^\lambda - 1$ is a Mersenne prime, is $\mathcal{O}\big(\lambda^{-n/4}\big)$-insecure against Hamming weight leakage whenever $n \geqslant 5$, for all $\vec{\beta} \in (F_p^*)^n$.

We defer the proof of Theorem 10 and further discussion to the full version.

2 Preliminaries

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

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

2.1 Secret Sharing (Masking) Schemes

▶ **Definition 12** (Additive Secret Sharing). *Let F be a finite field and n a positive integer. Given a secret $s \in F$, additive secret sharing Add_n shares s by sampling $(s_1, \ldots, s_n) \in F^n$ uniformly at random conditioned on $s_1 + \cdots + s_n = s$. More concretely, Add_n consists of the following two algorithms: given $s \in F$,*

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

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

▶ **Definition 13** (Generalized Additive Secret Sharing). *Let F be a finite field and n a positive integer. Given reconstruction multipliers $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F^*)^n$ and a secret $s \in F$, the generalized additive secret sharing $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ shares s by sampling $(s_1, \ldots, s_n) \in F^n$ uniformly at random conditioned on $\beta_1 s_1 + \cdots + \beta_n s_n = s$. More concretely, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ consists of the following two algorithms:*

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

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

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

The term *generalized* secret sharing was chosen in line with notational conventions in coding theory literature. Observe that, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ can be seen as Add_n generating the shares $(s'_1, \ldots, s'_n)$ such that $s'_1 + \cdots + s'_n = s$, then postprocessing them into $(\beta_1^{-1}s'_1, \ldots, \beta_n^{-1}s'_n)$. Interpreting the shares as codewords of a linear code [35], this postprocessing corresponds to the notion of generalized linear codes; see, for example, [22, Chapter 5].

▶ **Definition 14** (Shamir Secret Sharing). *Let F be a finite field and n and k be positive integers such that $k \leqslant n$. Denote by $F[X]_{<k}$ the set of polynomials over F of degree less than k [11, Definition 11.6]. Given evaluation places $\vec{X} = (X_1, \ldots, X_n) \in (F^*)^n$ with $X_i \neq X_j$ for all $i \neq j$ and a secret $s \in F$, Shamir secret sharing $\mathsf{Shamir}(n, k, \vec{X})$ shares s by:*

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

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

▶ **Proposition 15.** *Shamir secret sharing with $k = n$ is an instance of generalized additive secret sharing. Therefore, proving security of* $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ *automatically translates to the security of* $\mathsf{Shamir}(n, n, \vec{X})$.

The proof of Proposition 15 is provided in the full version.

2.2 Leakage-Resilient Secret Sharing

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

▶ **Definition 16** (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 17** (Local Leakage [4, 5]). *Let F be a finite field and n be a positive integer. Let $\mathcal{S}$ be a secret sharing scheme with sharing algorithm* Share. *Let $\vec{\tau} = (\tau_1, \ldots, \tau_n)$ be a collection of n functions whose domains are F. For any secret $s \in F$, the leakage distribution $\vec{\tau}(\mathsf{Share}(s))$ is defined by the following experiment:*
1. *Sample shares $\vec{s} = (s_1, \ldots, s_n)$ from* $\mathsf{Share}(s)$.
2. *Output $(\tau_1(s_1), \ldots, \tau_n(s_n))$.*

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

▶ **Definition 18** (ε-insecurity). *A secret sharing scheme $\mathcal{S}$ is said to be ε-insecure against a local leakage $\vec{\tau}$ if for all secret $s \in F$,*

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

Roughly speaking, if $\mathcal{S}$ has small insecurity against a leakage attack, then the joint distribution of leakage of shares is statistically independent of the secret. In this paper, we primarily focus on the setting where all leakage functions are the Hamming weight, i.e. $\tau_1 = \cdots = \tau_n = \mathrm{wt}$. And in this case, $\vec{\tau}(\vec{s}) = \overrightarrow{\mathrm{wt}}(\vec{s})$ corresponds to the joint Hamming weight leakage of the shares of s.

▶ **Definition 19** (Typical Weights). *We call $w \in \{0, 1, \ldots, \lambda\}$ to be typical if $|w - \lambda/2| \leqslant \lambda^{1/2+\tau}$ for some $\tau > 0$. And we say a vector $\vec{w} = (w_1, w_2, \ldots, w_n) \in \{0, 1, \ldots, \lambda\}^n$ is in a typical set* $\mathsf{Typical}(n, \tau)$ *if every w_i is typical:*

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

2.3 Extension Fields and Hamming Weight

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

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

▶ **Definition 20** (Field Trace). *The trace of an extension field F_{p^d} over the base field F_p, denoted by $\mathsf{Tr}_{F_{p^d}/F_p}\colon F_{p^d} \to F_p$, is defined as*

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

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

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

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

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

We hence also have $\mathsf{Tr}_{F_{2^\lambda}/F_2}(\zeta x) = \langle \zeta^\vee, x\rangle$ for all $\zeta, x \in F_{2^\lambda}$ (the x in the inner product $\langle \alpha^\vee, x\rangle$ is the vector representation of x). The *trace-dual Hamming weight* of ζ is then the Hamming weight of $\zeta^\vee$, i.e. $\mathrm{wt}^\vee(\zeta) = \mathrm{wt}(\zeta^\vee)$. The map $\zeta \mapsto \zeta^\vee$ is an invertible F_2-linear map, and also efficiently computable [42].

2.4 Fourier Analysis on Finite Fields

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

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

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

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

▶ **Example 21.** For $p = 2$, we have $\omega := \omega_2 = \exp(\pi\imath) = -1$ and Fourier coefficients are

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

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

▶ **Fact 22** (Parseval's Identity). *For any function $f\colon F \to \mathbb{C}$,*

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

▶ **Fact 23** (Character Sum). *For all $\alpha \in F$,*

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

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

2.5 Imported Lemmas

▶ **Lemma 24** (Chernoff Bound [36, Theorem 2.1]). *Let $X_1, X_2, \ldots, X_\lambda$ be independent Bernoulli random variables with $\mathbb{E}(X_i) = p$ for each i. Then for any $t \geqslant 0$,*

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

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

▶ **Lemma 25** (Poisson Summation Formula [38, Chapter 3.3]). *Let $C \subseteq F^n$ denote the set of all shares of the secret $0 \in F = F_{p^d}$. Let $\vec{v} \in F^n$ denote an arbitrary secret share of the secret $1 \in F$. Consider an arbitrary local leakage $\vec{\tau}\colon F^n \to \Omega^n$. For any secret $s \in F$, let $\vec{\tau}(s)$ denote the distribution of the leakage $\vec{\tau}(\vec{x})$, where $\vec{x}$ is sampled uniformly at random from the set $s \cdot \vec{v} + C$. The following identity holds for any leakage value $\vec{\ell} \in \Omega^n$.*

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

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

▶ **Lemma 26** (Generalized Hölder's Inequality [23, Theorem 11]). *Let $p_1, \ldots, p_n$ be positive real numbers such that $p_1 + \cdots + p_n = 1$, and $(x_i^{(1)})_{i=1}^k$, $(x_i^{(2)})_{i=1}^k$, $\ldots$, $(x_i^{(n)})_{i=1}^k$ be sequences of real numbers. Then,*

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

3 Insecurity Analysis

In this section, we formally state the technical results introduced in Section 1.2 and their proofs outlined in the overview (Section 1.3). For succinctness, we omit the calculations in the proofs of both theorems; see the full version for complete derivations of each equation.

3.1 Worst-case Analysis (Theorem 4)

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

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

The proof of Theorem 4 relies on the following lemma that upper bounds our Fourier coefficients; we present its proof in the appendix of the full version.

▶ **Lemma 27.** *For $\lambda \geqslant 2$, $w \in \{1, \ldots, \lambda\}$, and $\zeta \in F$, we have $|\widehat{\mathbb{1}}_w(\zeta)| \leqslant B(\zeta)$ where*

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

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

Proof of Theorem 4. By Definition 18, it suffices to prove that $2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big)$ is upper bounded by ε. Recall from Definition 19 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 $\tau > 0$. Chernoff bound (Lemma 24) implies that the probability mass on atypical weights contribute only negligibly to the statistical distance. Hence, the expression for the statistical distance (Definition 18) becomes a summation over the set of typical weights $\mathsf{Typical}(n, \tau)$ plus a negligible quantity.

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

If $\vec{s} \in F^n$ is a share of secret 0, i.e. $\vec{s} \in C := \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; 0)$, then $\beta_1 s_1 + \cdots + \beta_n s_n = 0$, and for any $\zeta \in F$, we have $\zeta\beta_1 s_1 + \cdots + \zeta\beta_n s_n = \zeta \cdot 0 = 0$. From this, we can deduce $C^\perp = \{\zeta\vec{\beta} \mid \zeta \in F\}$, then by Poisson summation formula (Lemma 25),

$$\Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] = \sum_{\zeta \in F} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right) \cdot \chi_\zeta(s) \qquad (14)$$

and by Fact 23,

$$\Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] = \sum_{\zeta \in \{0\}} \left(\prod_{i=1}^{n} \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right) \qquad (15)$$

Plugging these into the summand in Equation 13 and applying triangle inequality, we get

$$\begin{aligned} &\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \left| \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; s)} \left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] - \Pr_{\vec{s} \leftarrow \mathsf{Gen}(\mathsf{Add}_n, \vec{\beta}; U_F)} \left[\overrightarrow{\mathrm{wt}}(\vec{s}) = \vec{w}\right] \right| \\ &\quad \leqslant \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^*} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \qquad (16) \end{aligned}$$

Let $\mathcal{S}_{\vec{\beta}} := \left\{\zeta^* \beta_1^{-1}, \zeta^* \beta_2^{-1}, \ldots, \zeta^* \beta_n^{-1}\right\}$. Then for any $\zeta \in \mathcal{S}_{\vec{\beta}}$, at least one of β_i's should give $\beta_i \zeta = \zeta^*$. Consider the following separation of the summation.

(Equation 16)

$$= \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| + \sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \qquad (17)$$

Let us upper bound the second summand (the summation over $F^* \setminus \mathcal{S}_{\vec{\beta}}$). As stated in Lemma 27, we denote $B(\zeta)$ to be a function that upper bounds $|\widehat{\mathbb{1}}_w(\zeta)|$. Then, by Hölder's inequality (Lemma 26) and Lemma 27,

$$\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in F^* \setminus \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \leqslant 2^{n+2} \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{n\tau} \cdot \lambda^{-\frac{n}{2}+1} \qquad (18)$$

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

$$\begin{aligned} &\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \\ &\quad \leqslant \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \left(\prod_{i \in H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \right) \cdot \left(\prod_{i \notin H(\zeta;\vec{\beta})} \sum_{w_i=0}^{\lambda} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \right) \qquad (19) \end{aligned}$$

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

▷ Claim 28. For all $\lambda \in \{1, 2, \dots\}$, $w \in \{1, 2, \dots, \lambda\}$, and $\zeta \in F$,

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

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

▷ Claim 29. For $m \in \{1, 2, \dots\}$, the following bound holds.

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

Case 1. Consider $i \in H(\zeta; \vec{\beta})$. This is the non-trivial case, we want a non-trivial upper bound. By Claim 28 and Claim 29,

$$\sum_{w_i=0}^{\lambda}\left|\widehat{\mathbb{1}}_{w_i}(\beta_i\zeta)\right| < \binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4}$$

Case 2. Consider $i \notin H(\zeta; \vec{\beta})$. In this case, we have the trivial estimate from Claim 28.

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

Substituting these values into Equation 19 and continuing the upper bound, we have:

$$(\text{Equation 19}) < \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\prod_{i\in H(\zeta;\vec{\beta})}\binom{\lambda}{\mathrm{wt}^\vee(\beta_i\zeta)}^{-1/2} \cdot \pi \cdot \lambda^{1/4} \tag{20}$$

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

$$(\text{Equation 20}) \leqslant \sum_{\zeta\in\mathcal{S}_{\vec{\beta}}}\lambda^{-\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{2}} \cdot \pi^{\mathrm{card}(H(\zeta;\vec{\beta}))} \cdot \lambda^{\frac{\mathrm{card}(H(\zeta;\vec{\beta}))}{4}} \leqslant (\widetilde{h}+1)\cdot\left(\frac{\pi^4}{\lambda}\right)^{\frac{\widetilde{h}}{4}} \tag{21}$$

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

Therefore, for a sufficiently large λ, the above sum is small as long as we have $\mathrm{card}(H(\zeta; \vec{\beta})) \geqslant 1$; that is, unless $\beta_1 = \beta_2 = \cdots = \beta_n$ (i.e., unless the secret sharing is the additive secret sharing), the above sum would be at most $\lambda^{-1/4}$. More precisely, Equation 18 and 21 add up to:

$$2 \cdot \mathrm{SD}\big(\overrightarrow{\mathrm{wt}}(s)\ ,\ \overrightarrow{\mathrm{wt}}(U_F)\big) \leqslant 2\pi \cdot \frac{c_n}{\lambda^{1/4}} + 2^{n+2} \cdot 5^{\frac{5n}{2}-4} \cdot \lambda^{n\tau} \cdot \lambda^{-\frac{n}{2}+1} + 2 \cdot 2n \cdot \exp(-2\lambda^{2\tau})$$

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

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

3.2 Security Characterization (Theorem 8)

▶ **Theorem 8.** *For $\vec{\beta} \in (F^*)^n$, the $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ secret sharing scheme is ε insecure against the Hamming weight leakage, where*

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

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

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

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

For the proof of Theorem 8, we use the following lemma that relates the product of Fourier coefficients to our Score function. Its proof can be found in the full version.

▶ **Lemma 30.** *For any $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_n) \in (F^*)^n$ and $\vec{w} = (w_1, w_2, \ldots, w_n) \in \{1, 2, \ldots, \lambda\}^n$,*

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

Proof of Theorem 8. The proof goes in the same way as for Theorem 4, with the estimation of the second summand unchanged. The only difference lies in the first summand, which naturally gives rise to the score function quantifying the security of $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$.

The first summand (the summation over $\mathcal{S}_{\vec{\beta}}$) can be rewritten as follows, using Lemma 30.

$$\sum_{\vec{w} \in \mathsf{Typical}(n,\tau)} \sum_{\zeta \in \mathcal{S}_{\vec{\beta}}} \prod_{i=1}^{n} \left| \widehat{\mathbb{1}}_{w_i}(\beta_i \zeta) \right| \leqslant (2\lambda^{\tau})^n \cdot n \cdot \exp\left(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right) \tag{22}$$

because the maximum of a sequence is at least as large as its average. Hence, upon choosing τ such that $2\lambda^{\tau} = (n \log \lambda)^{1/2}$, we get

(Equation 17)

$$\leqslant (n \log \lambda)^{n/2} \cdot n \cdot \exp\left(- \min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \right) + 4 \cdot 5^{\frac{5n}{2}-4} \cdot (n \log \lambda)^{n/2} \cdot \lambda^{-\frac{n}{2}+1} \tag{23}$$

by Equation 18 and 22, and in summary, for sufficiently large λ,

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

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

$$\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \geqslant \left(\frac{n}{2} + 1 \right) \log(n \log \lambda) + cn \log \lambda \tag{24}$$

for some constant $c > 0$. Then,

$$2 \cdot \mathrm{SD}\left(\overrightarrow{\mathrm{wt}}(s) \, , \, \overrightarrow{\mathrm{wt}}(U_F) \right) \leqslant \lambda^{-cn} + \mathcal{O}\left(\lambda^{-c'n} \right) = \mathcal{O}\left(\lambda^{-cn} \right)$$

because $\frac{\log \lambda}{\lambda} \leqslant \lambda^{-c'}$ holds for all $c' \in (0, 1/2)$. This concludes the proof of Theorem 8. ◀

Note that Theorem 8 provides an insecurity bound in terms of reconstruction multipliers $\vec{\beta} \in (F^*)^n$. This consequently gives a method for choosing $\vec{\beta}$ such that $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is guaranteed to be secure, by choosing one that makes the bound small.

▶ **Corollary 9.** *Let $n \geqslant 3$ and $\vec{\beta} = (\beta_1, \ldots, \beta_n) \in (F^*)^n$ where for every β_i, there exists some $\beta_j \neq \beta_i$ such that*

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

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

Proof of Corollary 9. Consider any $\zeta \in \mathcal{S}_{\vec{\beta}}$. Then, by definition of $\mathcal{S}_{\vec{\beta}}$, we can write $\zeta = \zeta^* \beta_i^{-1}$ for some distinct multiplier β_i in $\vec{\beta}$. By condition, there is another distinct multiplier value $\beta_j \neq \beta_i$ appearing in $\vec{\beta}$ that gives $4cn \leqslant \mathrm{wt}^\vee(\beta_j \zeta^* \beta_i^{-1}) \leqslant \lambda - 4cn$. Therefore,

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

The last inequality follows from the definition (Equation 2), and provided that λ is sufficiently large say, $\lambda \geqslant (4cn)^5$. Since $\zeta \in \mathcal{S}_{\vec{\beta}}$ was arbitrary, we get $\min_{\zeta \in \mathcal{S}_{\vec{\beta}}} \mathsf{Score}(\zeta; \vec{\beta}) \geqslant \left(\frac{8}{5}cn - \frac{1}{4}\right) \log \lambda$. It satisfies Equation 24 in the proof of Theorem 8 (as long as $cn > 5/12$ which by choosing $c > 5/36$ it always holds for all $n \geqslant 3$). Therefore, $\mathsf{Gen}(\mathsf{Add}_n, \vec{\beta})$ is at most λ^{-cn}-insecure by Theorem 8. ◀

▶ Remark 31. In light of Proposition 15, Corollary 9 also implies the security of $\mathsf{Shamir}(n, n, \vec{X})$ when the evaluation places $\vec{X} = (X_1, \ldots, X_n)$ are chosen uniformly at random. See the full version for details.

References

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

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

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

4 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.

5 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.

6 Peter B Borwein. On the complexity of calculating factorials. *Journal of Algorithms*, 6(3):376–380, 1985. doi:10.1016/0196-6774(85)90006-9.

7 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.

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

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

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

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

12 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.

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

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

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

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

17 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32 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.

33 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.

34 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.

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

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

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

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

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

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

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

42 Joachim von zur Gathen and Victor Shoup. Computing frobenius maps and factoring polynomials. *Computational Complexity*, 2:187–224, September 1992. doi:10.1007/BF01272074.