Scale, Round, Break: Simple Leakage Attacks on Secret Sharing Schemes

Katharina Boudgoust[1⋆] and Mark Simkin[2,3⋆⋆]

[1] CNRS, Univ Montpellier, LIRMM
[2] Flashbots
[3] Aarhus University

Abstract. We study the local leakage resilience of t-out-of-n threshold secret sharing schemes. We present a remarkably simple, perfectly correct attack that fully breaks any scheme with linear reconstruction over a finite field using $\lg t + \mathcal{O}(1)$ bits of leakage per share. In particular, this yields concretely efficient attacks on additive secret sharing and on Shamir's scheme for arbitrarily large thresholds over arbitrarily large finite fields. Our key technical idea is an approximately linear scale-and-round function that maps shares from an arbitrarily large field into a much smaller ring, while preserving the distance of well-separated secrets. Our results provides two surprising insights: Bigger finite fields do not necessarily improve leakage resilience and increasing the reconstruction threshold in Shamir's scheme does not help too much either.

1 Introduction

Threshold secret sharing schemes, first introduced by Shamir [Sha79] and Blakley [Bla79], allow a dealer to split a message m into n shares $s_1, \ldots, s_n$, such that any subset of t shares can be used to recover the message, whereas any $t-1$ shares reveal no information about m. Secret sharing schemes in general, and Shamir's secret sharing scheme [Sha79] in particular, are ubiquitous in modern cryptography and for this reason it is important to understand their precise security guarantees. The security of Shamir's scheme is well understood in the presence of an all-or-nothing adversary, i.e. one that learns some shares in full and nothing about the remaining ones. Far less is known when the adversary obtains partial information leakage from *every* share simultaneously. Such leakage models are motivated by side-channel attacks, where an attacker may extract limited information from otherwise honest devices through side-channel leakages, such as a device's computation time [Koc96] or power consumption [KJJ99].

Existing research on the leakage resilience of secret sharing schemes broadly splits into two directions: Works that study how to construct secret sharing schemes that are leakage-resilient by design [DP07; GK18b; GK18a; ADN+19; KMS19; SV19; CKO+21; CKO+22] and works that study whether existing schemes, specifically Shamir's scheme, already provide some inherent amount of leakage resilience out of the box [GW16; BDI+18; NS20; MPS+21; MNPC+22; MNP+21; MNP+22; CST+23; KK23; HS23; Kas24; Ngu24; Ngu25].

A popular way to model leakage is to allow the adversary to extract ℓ bits independently from each share. Concretely, the adversary chooses messages m_0 and m_1, a vector of local leakage functions $\textsc{Leak}_1, \ldots, \textsc{Leak}_n$ with $\textsc{Leak}_i : \{0,1\}^* \to \{0,1\}^\ell$, obtains leakages $\textsc{Leak}_1(s_1), \ldots, \textsc{Leak}_n(s_n)$, where $(s_1, \ldots, s_n)$ are shares of either message m_0 or message m_1. The adversary has to correctly guess which messages was shared. If no such adversary exists, we call the secret sharing scheme local leakage resilient.

The first results on local leakage resilience for Shamir's scheme were due to Guruswami and Wootters [GW16] and Benhamouda et al. [BDI+18]. Shamir's scheme is defined over a finite field $\mathbb{F}$ with $|\mathbb{F}| \geq n$ and to share a message $m \in \mathbb{F}$ one picks a uniformly random polynomial $f \in \mathbb{F}[X]$ of degree $t-1$ with $f(0) = m$ and defines the i-th share s_i to be $f(i)$. Guruswami and Wootters showed that, for certain parameters over characteristic-two fields, even 1 bit of leakage per share suffices to fully recover m. In contrast, Benhamouda et al. proved that over prime fields, Shamir's scheme is 1-bit local leakage resilient whenever $t \geq 0.92n$. They further conjectured that the same should hold for every $t = cn$, where c is an arbitrary constant, when n is sufficiently large. Subsequent works [MPS+21; MNPC+22; KK23; Kas24] lowered the provable constant from 0.92 to 0.668. At the same time a work by Nielsen and

⋆ katharina.boudgoust@lirmm.fr
⋆⋆ mark@univariate.org

Simkin [NS20] proved that the conjecture is false, when $t \in \mathcal{O}(n/\lg n)$ and $|\mathbb{F}| = \mathcal{O}(n)$. Several other works [MNP+21; MNP+22; Ngu24; Ngu25] studied possible attacks on the local leakage resilience of Shamir's scheme. The works of Maji et al. [MNP+21; MNP+22] presented 1-bit local leakage attacks that have a distinguishing advantage of $\mathcal{O}(2^{-t})$. More recently, Con et al. [CST+23] and Nguyen [Ngu24] showed that $\mathcal{O}(1)$-bits of leakage are sufficient to break local leakage resilience with probability 1, when $t = \mathcal{O}(\sqrt{n})$ and $|\mathbb{F}| = \mathcal{O}(n)$.

Yet, despite substantial progress in recent years, our understanding of the local leakage resilience of Shamir's scheme is far from complete and for many parameter regimes, we still have neither security proofs nor attacks.

1.1 Our Contribution

In this work, we present a surprisingly simple, but powerful attack on a broad class of t-out-of-n threshold secret sharing schemes. Our attack applies to every scheme with linear reconstruction, that is, every scheme in which the secret can be recovered as a linear combination of shares over a finite field This family includes additive secret sharing and Shamir's scheme with arbitrary thresholds t over arbitrarily large finite fields. Our attack succeeds with probability 1 while requiring only $\ell \in \lg t + \mathcal{O}(1)$ bits of leakage per share. Moreover, both the leakage functions and the adversary processing the leakage run in quasi-linear time in the size of their respective inputs, making the attack not only general but also highly efficient. For completeness, we provide a SageMath script implementing the attack.

Conceptually, our results provide two important insights: The first one is that increasing the field size, thereby increasing the entropy in a secret sharing scheme, does not necessarily improve its leakage resilience. The second one is that Shamir's scheme with large thresholds and additive secret sharing are much less leakage resilient than previously thought.

The core technical idea behind our attack is an approximately linear scale-and-round map that takes shares over an arbitrarily large finite field $\mathbb{F}$ and compresses them into shares over a much smaller ring. Importantly, this map preserves separation: If two well-separated messages are independently secret shared over $\mathbb{F}$, then applying the map share-wise yields two independent additive sharings of two well-separated messages in the smaller ring. Since the target ring is small, the leakage functions can reveal these compressed shares in full.

1.2 Putting our Result into Context

Benhamouda et al. [BDI+18] show that for some parameter ranges additive and Shamir secret sharing over $\mathbb{F}_p$ are indeed local leakage resilient. For additive secret sharing, the authors prove that the adversary's distinguishing advantage is upper bounded by $p \cdot 2^{-\Omega(n/p^2)}$, when $\ell = \lg p - 1$. One the one hand, this is a very strong result, since it effectively allows leaking all but one bit from each single share. On the other hand, the bound on the adversary's advantage only becomes effective, when $n \in \Omega(p^2)$, meaning that the number of shares needs to be *quadratic* in the field size! For Shamir's scheme, the authors prove that the adversary's advantage is upper bounded by $\mathcal{O}(2^{-n})$, when $\ell = \mathcal{O}(1)$ and $t \geq cn$ for some sufficiently large constant c.

For the case of additive secret sharing, our attack requires $\ell = \lg n + \mathcal{O}(1)$, which is only interesting when the number of shares is smaller than the field size. For Shamir's scheme we require $\ell = \omega(1)$ bits of leakage per share. Thus our attacks live in parameter regimes outside of those considered by Benhamouda et al.

2 Preliminaries

Notation. We write $[n]$ to denote the set $\{1, \ldots, n\}$. For a vector $\boldsymbol{v} \in \mathcal{X}^\ell$ of length ℓ over some domain $\mathcal{X}$, we write $\boldsymbol{v}_i$ to denote the vector's i-th component. For a set $S \subset [n]$, we write $\boldsymbol{v}_S$ to denote the vector $(w_1, \ldots, w_n)$ where $w_i = v_i$ for all $i \in S$ and $w_i = \perp$ for $i \notin S$. We say an algorithm is efficient, if its runtime is polynomial in its input length.

2.1 Finite Fields

Let p be an odd prime and let $\mathbb{F}_p$ be the finite field with p elements, defined as the quotient ring $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Its elements are residue classes defined modulo p. For every $x \in \mathbb{F}_p$, we define by $\textsc{IntRep}_p(x) \in I_p$ its unique centered integer representative in $I_p := \{-(p-1)/2, \ldots, (p-1)/2\} \subset \mathbb{Z}$. Concretely, let $\{0, \ldots, p-1\}$ denote the usual residue classes modulo p. Then $\textsc{IntRep}_p(x) = x$ if $0 \leq x \leq (p-1)/2$ and $\textsc{IntRep}_p(x) = x - p$ if $(p+1)/2 \leq x \leq p-1$.

2.2 Secret Sharing

We recall the definitions of a correct and perfectly private threshold secret sharing scheme with linear reconstruction.

Definition 1 (Threshold Secret Sharing Scheme). *Let $t, n \in \mathbb{N}$ with $t \leq n$. A t-out-of-n threshold secret sharing scheme with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ is a pair $(\textsc{Share}, \textsc{Rec})$ of efficient algorithms, which are defined as follows:*

- $\textsc{Share}(m) \to (s_1, \ldots, s_n)$*: The randomized sharing algorithm takes a message $m \in \mathcal{X}$ as input and returns shares $s_1, \ldots, s_n \in \mathcal{Y}$.*
- $\textsc{Rec}(s_1, \ldots, s_n) \to m$*: The deterministic reconstruction algorithm takes shares $s_1, \ldots, s_n \in \mathcal{Y} \cup \{\perp\}$ as input and returns a message $m \in \mathcal{X} \cup \{\perp\}$.*

Definition 2 (Correctness). *Let $t, n \in \mathbb{N}$ with $t \leq n$. We say a t-out-of-n threshold secret sharing scheme $(\textsc{Share}, \textsc{Rec})$ with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ is correct, if for all $m \in \mathcal{X}$ and all $T \subset [n]$ with $|T| \geq t$, it holds that*

$$\Pr\left[\textsc{Rec}(\textsc{Share}(m)_T) = m\right] = 1.$$

Definition 3 (Privacy). *Let $t, n \in \mathbb{N}$ with $t \leq n$. We say a t-out-of-n threshold secret sharing scheme $(\textsc{Share}, \textsc{Rec})$ with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ is perfectly private, if for all adversaries $\mathcal{A}$ and all $m_0, m_1 \in \mathcal{X}$, and all $T \subset [n]$ with $|T| < t$, it holds that*

$$\Pr\left[b = b' : \begin{array}{r} b \leftarrow \{0,1\} \\ \boldsymbol{s} \leftarrow \textsc{Share}(m_b) \\ b' \leftarrow \mathcal{A}(\boldsymbol{s}_T) \end{array}\right] = 1/2,$$

where the probability is taken over the random coins of the experiment and the adversary.

Definition 4 (Linear Reconstruction). *Let $t, n \in \mathbb{N}$ with $t \leq n$. We say a t-out-of-n threshold secret sharing scheme $(\textsc{Share}, \textsc{Rec})$ with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ has linear reconstruction, if $\mathcal{Y}$ is a finite field and there exists an efficiently computable function $\textsc{Coeff} : [n]^t \to \mathcal{Y}^t$, such that for all $S \subset [n]$ with $|S| = t$ and all $m \in \mathcal{X}$, it holds that*

$$\Pr\left[m = \sum_{i \in S} \lambda_i \cdot s_i : \begin{array}{r} (s_1, \ldots, s_n) \leftarrow \textsc{Share}(m) \\ \{\lambda_i\}_{i \in S} \leftarrow \textsc{Coeff}(S) \end{array}\right] = 1,$$

where the probability is taken over the random coins of the experiment.

Shamir Secret Sharing. Shamir's construction [Sha79] is a t-ouf-of-n secret sharing scheme where both message and share space are a finite field $\mathbb{F}_p$ for some prime $p > n$. It is parameterized by n distinct non-zero elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$. To share a message $m \in \mathbb{F}_p$, the dealer picks a uniformly random polynomial $f \in \mathbb{F}_p[X]$ of degree $t-1$ with $f(0) = m$ and computes the vector of shares $(f(\alpha_1), \ldots, f(\alpha_n))$. Shamir's secret sharing scheme is correct, perfectly private, and has linear reconstruction.

2.3 Leakage-Resilient Secret Sharing

We define local leakage resilience of threshold secret sharing schemes similarly to how it was done by Nielsen and Simkin [NS20].

Definition 5 (Leakage Functions). *Let $n, t, \ell \in \mathbb{N}$ with $t \leq n$ and $\ell > 0$. Let $(\textsc{Share}, \textsc{Rec})$ be a t-out-of-n threshold secret sharing scheme with input domain $\mathcal{X}$ and share space $\mathcal{Y}$. We say a vector $\textsc{Leak} = (\textsc{Leak}_1, \ldots, \textsc{Leak}_n)$ is a vector of ℓ-bit leakage functions for $(\textsc{Share}, \textsc{Rec})$, if for all $i \in [n]$, we have that $\textsc{Leak}_i : \mathcal{Y} \to \{0,1\}^\ell$. For a share vector $(s_1, \ldots, s_n) \in \mathcal{Y}$, we write $\textsc{Leak}(s_1, \ldots, s_n)$ to denote $(\textsc{Leak}_1(s_1), \ldots, \textsc{Leak}_n(s_n))$.*

Definition 6 (Weak Local Leakage Resilience). *Let $t, n, \ell \in \mathbb{N}$ with $t \leq n$ and $\ell > 0$. We say a t-out-of-n threshold secret sharing scheme $(\textsc{Share}, \textsc{Rec})$ with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ is (ϵ, ℓ)-weakly-local-leakage-resilient, if for every vector $\textsc{Leak}$ of ℓ-bit leakage functions for $(\textsc{Share}, \textsc{Rec})$, every pair $m_0, m_1 \in \mathcal{X}$, and any adversary $\mathcal{A}$, it holds that*

$$\Pr\left[b = b' : \begin{array}{r} b \leftarrow \{0,1\} \\ \boldsymbol{s} \leftarrow \textsc{Share}(m_b) \\ \boldsymbol{L}_b = \textsc{Leak}(\boldsymbol{s}) \\ b' \leftarrow \mathcal{A}(\boldsymbol{L}_b) \end{array}\right] \leq \frac{1}{2} + \epsilon,$$

where the probability is taken over the random coins of the experiment and the adversary.

Definition 7 (Local Leakage Resilience). *Let $t, n, \ell \in \mathbb{N}$ with $t \leq n$ and $\ell > 0$. We say a t-out-of-n threshold secret sharing scheme $(\textsc{Share}, \textsc{Rec})$ with input domain $\mathcal{X}$ and share space $\mathcal{Y}$ is (ϵ, ℓ, θ)-local-leakage-resilient, if for every vector $\textsc{Leak}$ of ℓ-bit leakage functions for $(\textsc{Share}, \textsc{Rec})$, every pair $m_0, m_1 \in \mathcal{X}$, any adversary $\mathcal{A}$, and every $T \subset [n]$ with $|T| \leq \theta$, it holds that*

$$\Pr\left[b = b' : \begin{array}{r} b \leftarrow \{0,1\} \\ \boldsymbol{s} \leftarrow \textsc{Share}(m_b) \\ \boldsymbol{L}_b = \textsc{Leak}(\boldsymbol{s}) \\ b' \leftarrow \mathcal{A}(\boldsymbol{L}_b, \boldsymbol{s}_T) \end{array}\right] \leq \frac{1}{2} + \epsilon.$$

3 A Perfect Distinguisher with $\lg t + \mathcal{O}(1)$-Bit Leakages

In this section, we show how $\ell \in \lg t + \mathcal{O}(1)$ bits of leakage per share are sufficient to break the weak local leakage resilience of any secret sharing scheme with linear reconstruction.

3.1 Scale and Round

The main hero of this paper is the scale and round function $\mathrm{SR} : \mathbb{N}_+^2 \times \mathbb{Z} \to \mathbb{Z}$, which is defined as

$$\mathrm{SR}(p, q, \bar{x}) := \left\lfloor \frac{q}{p} \cdot \bar{x} \right\rceil,$$

where $\lfloor \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ takes a real number and rounds it to the nearest integer, with 0.5 being rounded upwards. Let us make some basic observations.

Lemma 1. *For any $x \in \mathbb{R}$, it holds that*

$$x = \lfloor x \rceil + e,$$

where $e \in \mathbb{R}$ with $|e| \leq 1/2$.

Lemma 2. *Let $p, q \in \mathbb{N}$, defining $I_p = \left\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right\} \subset \mathbb{Z}$. For $x \in \mathbb{F}_p$ let $\bar{x} = \textsc{IntRep}_p(x) \in I_p \subset \mathbb{Z}$ be its centered integer representative. Then it holds that*

$$\mathrm{SR}\,(p, q, \bar{x}) \in \left\{-\left\lfloor \frac{q}{2} \right\rceil, \ldots, \left\lceil \frac{q}{2} \right\rceil\right\}.$$

Proof. For $x \in \mathbb{F}_p$, we have that

$$\bar{x} = \textsc{IntRep}_p(x) \in I_p = \left\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right\} \subset \mathbb{Z}$$

and therefore

$$\mathrm{SR}(p, q, \bar{x}) = \left\lfloor \frac{q}{p} \cdot \bar{x} \right\rceil \leq \left\lceil \frac{q(p-1)}{2p} \right\rceil = \left\lceil \frac{pq}{2p} - \frac{q}{2p} \right\rceil < \left\lceil \frac{q}{2} \right\rceil.$$

By symmetry, it directly follows that

$$\mathrm{SR}(p, q, \bar{x}) \in \left\{-\left\lfloor \frac{q}{2} \right\rfloor, \ldots, \left\lceil \frac{q}{2} \right\rceil\right\}.$$

□

Corollary 3. *Let $p, q \in \mathbb{N}$. For $x \in \mathbb{F}_p$ let $\bar{x} \in I_p$ be its centered integer representative. The value $\mathrm{SR}(p, q, \bar{x})$ can be uniquely represented by $\lg q + \mathcal{O}(1)$ bits.*

3.2 Distinguisher

We now describe our simple, yet remarkably powerful distinguishing attack.

DISTINGUISHER

let $m_0 = 0$ **and** $m_1 = (p-1)/2$
$\{\lambda_i\}_{i\in[t]} \leftarrow \textsc{Coeff}([t])$
for $i \in [t]$:
  let $\textsc{Leak}_i(s_i) :=$
    $\tilde{s}_i = \lambda_i \cdot s_i \in \mathbb{F}_p$
    $\bar{s}_i = \textsc{IntRep}_p(\tilde{s}_i)$
    return $\mathrm{SR}(p, q, \bar{s}_i)$
for $i \in [n-t]$:
  let $\textsc{Leak}_{t+i} := 0$
return $(m_0, m_1), (\textsc{Leak}_1, \ldots, \textsc{Leak}_n)$
receive $L_1, \ldots, L_t \in \mathbb{Z}$
compute $v = \sum_{i=1}^{t} L_i$
compute $\alpha, \beta \in \mathbb{Z}$ **s.t.** $v = \alpha \cdot q + \beta$ **and** $0 \leq \beta < q$
if $\beta \leq t/2 \vee q - \beta \leq t/2$ **then return** 0
else return 1

Fig. 1. Deterministic distinguisher with perfect correctness using $\ell \in \lg t + \mathcal{O}(1)$ bits of leakage.

Theorem 4. *Let $n, t \in \mathbb{N}_+$ with $t \leq n$ and t being even. Let $p \in \mathbb{N}_+$ be an odd prime. Let $q \in \mathbb{N}_+$ with $q \in \mathcal{O}(t)$ and $p > q > 4t$. Let $\epsilon \in \mathbb{R}$ be an arbitrary constant with $\epsilon < 1/2$. Let $\ell \in \mathbb{N}$ with $\ell \in \lg t + \mathcal{O}(1)$. Let $(\textsc{Share}, \textsc{Rec})$ be a t-out-of-n secret sharing scheme with linear reconstruction with message and share space being $\mathbb{F}_p$. Then the distinguisher in Figure 1 breaks the (ϵ, ℓ)-weak-local-leakage-resilience of $(\textsc{Share}, \textsc{Rec})$.*

Remark 1. For the sake of clarity, our theorem makes some simplifying assumption. We assume that t is even, but our result trivially generalizes to uneven values of t. Our attack specifically considers secret sharing schemes with linear reconstruction over prime order finite fields. Our attack easily generalizes to secret sharing schemes over rings as long as they have an appropriate linear reconstruction property. We further assume that $p > q > 4t$, but note that if $p \in \Omega(t)$, then $\lg(p) = \lg(t) + \mathcal{O}(()1)$. In this regime, no scheme is leakage resilience since the adversary can leak all shares in full.

Proof. Let us start by making some basic observations. Since each leakage is an integer, the value v is also an integer. Since $(\text{SHARE}, \text{REC})$ is a t-out-of-n secret sharing with linear reconstruction and since $(s_1, \ldots, s_n)$ is a secret sharing of m_b over $\mathbb{F}_p$, it holds that $(\tilde{s}_1, \ldots, \tilde{s}_t)$ is an additive sharing of m_b, i.e.

$$\sum_{i=1}^{t} \tilde{s}_i = m_b \in \mathbb{F}_p.$$

As $(\bar{s}_1, \ldots, \bar{s}_t) \in I_p \subset \mathbb{Z}$ is the vector of centered integer representatives of the shares $(\tilde{s}_1, \ldots, \tilde{s}_t)$, over the integers we have

$$\sum_{i=1}^{t} \bar{s}_i = \bar{m}_b + kp \in \mathbb{Z}, \tag{1}$$

for some integer $k \in \mathbb{Z}$.

Since our distinguisher makes the decision on which bit to guess solely based upon the value of the integer $v \in \mathbb{Z}$, let us now have a closer look at this value. Let us view the computation of v as computation over $\mathbb{R}$. The distinguisher computes

$$\begin{aligned}
v = \sum_{i=1}^{t} L_i &= \sum_{i=1}^{t} \mathrm{SR}(p, q, \bar{s}_i) \\
&= \sum_{i=1}^{t} \left\lfloor \frac{q}{p} \cdot \bar{s}_i \right\rceil \\
&= \sum_{i=1}^{t} \left(\frac{q}{p} \cdot \bar{s}_i + e_i \right) \\
&= \frac{q}{p} \cdot \sum_{i=1}^{t} \bar{s}_i + \sum_{i=1}^{t} e_i \\
&= \frac{q}{p} \cdot (\bar{m}_b + kp) + \sum_{i=1}^{t} e_i \\
&= \frac{q}{p} \cdot \bar{m}_b + q \cdot k + \sum_{i=1}^{t} e_i,
\end{aligned} \tag{2}$$

where the $e_i \in \mathbb{R}$ are the noise terms that come from rounding and we used Equation 1. By Lemma 1, we know that for all $i \in [n]$ it holds $|e_i| \leq 1/2$ and thus

$$-t/2 \leq \sum_{i=1}^{t} e_i \leq t/2.$$

Let us now consider the two possible choices for the challenge bit separately:

Challenge bit $b = 0$. When $b = 0$, then $\bar{m}_b = 0$ and thus Equation 2 simplifies to

$$v = q \cdot k + \sum_{i=1}^{t} e_i,$$

and because v is an integer and t even, we have that

$$v \in \{q \cdot k - t/2, \ldots, q \cdot k + t/2\}.$$

Challenge bit $b = 1$. When $b = 1$, then $\bar{m}_b = (p-1)/2$, which is an integer by assumption on p, and thus Equation 2 simplifies to

$$v = \frac{q}{p} \cdot \frac{p-1}{2} + q \cdot k + \sum_{i=1}^{t} e_i = \frac{q}{2} + q \cdot k - \frac{q}{2p} + \sum_{i=1}^{t} e_i.$$

We observe that

$$\left| -\frac{q}{2p} + \sum_{i=1}^{t} e_i \right| \leq \frac{q}{2p} + t/2 < \frac{q}{8} + \frac{q}{8} = \frac{q}{4},$$

since $p > q > 4t \geq 4$. Using the fact that v is an integer, we can conclude that

$$v \in \left\{ q \cdot k + \left\lfloor \frac{q}{4} \right\rfloor, \ldots, q \cdot k + \left\lceil 3 \cdot \frac{q}{4} \right\rceil \right\}.$$

From this we can make two conclusions. First,

$$v \geq q \cdot k + \left\lfloor \frac{q}{4} \right\rfloor \geq q \cdot k + t > q \cdot k + \frac{t}{2},$$

and second

$$v \leq q \cdot k + \left\lceil 3 \cdot \frac{q}{4} \right\rceil = q \cdot k + q + \left\lceil -\frac{q}{4} \right\rceil \leq q \cdot (k+1) - t < q \cdot (k+1) - \frac{t}{2},$$

and thus, we have that

$$q \cdot k + \frac{t}{2} < v < q \cdot (k+1) - \frac{t}{2}.$$

From the above, we can conclude that when the challenge bit equals $b = 0$, then v is at most an additive factor of $\pm t/2$ away from a multiple of q. On the other hand, if $b = 1$, then v is strictly more than $\pm t/2$ away from a multiple of q. Since $q > t$, for any value v only one of those statements can be true. The decision of our distinguisher in Figure 1 of which bit to guess is made exactly upon which of those two cases we are in. Thus our distinguisher always correctly determines the challenge bit.

The last thing to show is that our leakage functions satisfy the requirement of being ℓ-bit leakages for $\ell = \lg t + \mathcal{O}(1)$. This follows from Corollary 3 and the fact that $q \in \mathcal{O}(t)$. That is, $\ell = \lg q + \mathcal{O}(1) = \lg t + \mathcal{O}(1)$. □

The above theorem considers a distinguisher that only gets leakages, but no shares in full (as in Definition 6). When considering an adversary that additionally receives θ shares in the full, as in Definition 7, our attack improves in a straightforward manner. If the adversary is given shares $s_1, \ldots, s_\theta$ in full and the same leakages as above from shares $s_{\theta+1}, \ldots, s_t$, then over $\mathbb{R}$ we can compute

$$v = \sum_{i=1}^{\theta} \frac{q}{p} \bar{s}_i + \sum_{i=\theta+1}^{t} L_i = \frac{q}{p} \sum_{i=1}^{t} \bar{s}_i + \sum_{i=\theta+1}^{t} e_i$$

and importantly

$$-\frac{t-\theta}{2} \leq \sum_{i=\theta+1}^{t} e_i \leq \frac{t-\theta}{2}.$$

The proof from above goes through identically with the only part changing being the conclusion that $q > 4(t-\theta)$ needs to hold. Thus we get the following corollary.

Corollary 5. *Let $n, t, \theta \in \mathbb{N}_+$ with $\theta < t \leq n$ and $t - \theta$ being even. Let $p \in \mathbb{N}_+$ be an odd prime. Let $q \in \mathbb{N}_+$ with $q \in \mathcal{O}(t)$ and let $p > q > 4(t-\theta)$. Let $\epsilon \in \mathbb{R}$ be an arbitrary constant with $\epsilon < 1/2$. Let $\ell \in \mathbb{N}$ with $\ell \in \lg t + \mathcal{O}(1)$. Let $(\textsc{Share}, \textsc{Rec})$ be a t-out-of-n secret sharing scheme with linear reconstruction with message and share space being $\mathbb{F}_p$. Then $(\textsc{Share}, \textsc{Rec})$ does not satisfy (ϵ, ℓ, θ)-local-leakage-resilience.*

From Theorem 4 and Corollary 5 we immediately obtain attacks on the leakage-resilience of Shamir's scheme and additive secret sharing, since both have linear reconstructions. Notably, our attacks succeed with probability 1 using the same amount of leakage, regardless of how big the chosen finite field is.

Corollary 6 (Shamir). *Let $n, t \in \mathbb{N}_+$ with $t \leq n$ and t being even. Let $p \in \mathbb{N}_+$ be an odd prime. Let $q \in \mathbb{N}_+$ with $q \in \mathcal{O}(t)$ and $p > q > 4t$. Let $\epsilon \in \mathbb{R}$ be an arbitrary constant with $\epsilon < 1/2$. Let $\ell \in \lg t + \mathcal{O}(1)$. Then t-ouf-of-n Shamir secret sharing over $\mathbb{F}_p$ does not satisfy (ϵ, ℓ)-weak-local-leakage-resilience.*

Corollary 7 (Additive). *Let $n \in \mathbb{N}_+$ with n being even. Let $p \in \mathbb{N}_+$ be an odd prime. Let $q \in \mathbb{N}_+$ with $q \in \mathcal{O}(n)$ and $p > q > 4n$. Let $\epsilon \in \mathbb{R}$ be an arbitrary constant with $\epsilon < 1/2$. Let $\ell \in \lg n + \mathcal{O}(1)$. Then additive secret sharing over $\mathbb{F}_p$ does not satisfy (ϵ, ℓ)-weak-local-leakage-resilience.*

We provide a SageMath script that implements the distinguisher from Figure 1. The script can be accessed via the following url, https://github.com/KatinkaBou/Leakage-Attacks-Linear-Secret-Sharing.

Acknowledgement

We thank Maciej Obremski for useful discussions surrounding our result. Katharina Boudgoust is supported by the French National Research Agency (ANR), under the projects ANR-22-PECY-003 SecureCompute and ANR-25-CE39-4214-01 RELATE. Mark Simkin is supported by the Villum Young Investigator Programme as part of the "Building Secure and Scalable Cryptocurrencies" project.

References

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. "Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures". In: *CRYPTO 2019, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. LNCS. Springer, Cham, Aug. 2019, pp. 510–539. DOI: 10.1007/978-3-030-26951-7_18.

[BDI+18] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. "On the Local Leakage Resilience of Linear Secret Sharing Schemes". In: *CRYPTO 2018, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. LNCS. Springer, Cham, Aug. 2018, pp. 531–561. DOI: 10.1007/978-3-319-96884-1_18.

[Bla79] G. R. Blakley. "Safeguarding Cryptographic Keys". In: *Proceedings of AFIPS 1979 National Computer Conference* 48 (1979), pp. 313–317.

[CKO+21] Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. "Adaptive Extractors and Their Application to Leakage Resilient Secret Sharing". In: *CRYPTO 2021, Part III*. Ed. by Tal Malkin and Chris Peikert. Vol. 12827. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 595–624. DOI: 10.1007/978-3-030-84252-9_20.

[CKO+22] Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. "Short Leakage Resilient and Non-malleable Secret Sharing Schemes". In: *CRYPTO 2022, Part I*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13507. LNCS. Springer, Cham, Aug. 2022, pp. 178–207. DOI: 10.1007/978-3-031-15802-5_7.

[CST+23] Roni Con, Noah Shutty, Itzhak Tamo, and Mary Wootters. "Repairing Reed-Solomon Codes over Prime Fields via Exponential Sums". In: *IEEE International Symposium on Information Theory, ISIT 2023, Taipei, Taiwan, June 25-30, 2023*. IEEE, 2023, pp. 1330–1335.

[DP07] Stefan Dziembowski and Krzysztof Pietrzak. "Intrusion-Resilient Secret Sharing". In: *48th FOCS*. IEEE Computer Society Press, Oct. 2007, pp. 227–237. DOI: 10.1109/FOCS.2007.63.

[GK18a] Vipul Goyal and Ashutosh Kumar. "Non-malleable secret sharing". In: *50th ACM STOC*. Ed. by Ilias Diakonikolas, David Kempe, and Monika Henzinger. ACM Press, June 2018, pp. 685–698. DOI: 10.1145/3188745.3188872.

[GK18b] Vipul Goyal and Ashutosh Kumar. "Non-malleable Secret Sharing for General Access Structures". In: *CRYPTO 2018, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. LNCS. Springer, Cham, Aug. 2018, pp. 501–530. DOI: 10.1007/978-3-319-96884-1_17.

[GW16] Venkatesan Guruswami and Mary Wootters. "Repairing Reed-solomon codes". In: *48th ACM STOC*. Ed. by Daniel Wichs and Yishay Mansour. ACM Press, June 2016, pp. 216–226. DOI: 10.1145/2897518.2897525.

[HS23] Charlotte Hoffmann and Mark Simkin. "Stronger Lower Bounds for Leakage-Resilient Secret Sharing". In: *LATINCRYPT 2023*. Ed. by Abdelrahaman Aly and Mehdi Tibouchi. Vol. 14168. LNCS. Springer, Cham, Oct. 2023, pp. 215–228. DOI: 10.1007/978-3-031-44469-2_11.

[Kas24] Dustin Kasser. "An Improvement Upon the Bounds for the Local Leakage Resilience of Shamir's Secret Sharing Scheme". In: *TCC 2024, Part IV*. Ed. by Elette Boyle and Mohammad Mahmoody. Vol. 15367. LNCS. Springer, Cham, Dec. 2024, pp. 395–422. DOI: 10.1007/978-3-031-78023-3_13.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *CRYPTO'99*. Ed. by Michael J. Wiener. Vol. 1666. LNCS. Springer, Berlin, Heidelberg, Aug. 1999, pp. 388–397. DOI: 10.1007/3-540-48405-1_25.

[KK23] Ohad Klein and Ilan Komargodski. "New Bounds on the Local Leakage Resilience of Shamir's Secret Sharing Scheme". In: *CRYPTO 2023, Part I*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14081. LNCS. Springer, Cham, Aug. 2023, pp. 139–170. DOI: 10.1007/978-3-031-38557-5_5.

[KMS19] Ashutosh Kumar, Raghu Meka, and Amit Sahai. "Leakage-Resilient Secret Sharing Against Colluding Parties". In: *60th FOCS*. Ed. by David Zuckerman. IEEE Computer Society Press, Nov. 2019, pp. 636–660. DOI: 10.1109/FOCS.2019.00045.

[Koc96] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In: *CRYPTO'96*. Ed. by Neal Koblitz. Vol. 1109. LNCS. Springer, Berlin, Heidelberg, Aug. 1996, pp. 104–113. DOI: 10.1007/3-540-68697-5_9.

[MNP+21] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. "Leakage-Resilience of the Shamir Secret-Sharing Scheme Against Physical-Bit Leakages". In: *EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Cham, Oct. 2021, pp. 344–374. DOI: 10.1007/978-3-030-77886-6_12.

[MNP+22] 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: *ITC 2022*. Ed. by Dana Dachman-Soled. Vol. 230. LIPIcs. Schloss Dagstuhl, July 2022, 16:1–16:19. DOI: 10.4230/LIPIcs.ITC.2022.16.

[MNPC+22] Hemanta K Maji, Hai H Nguyen, Anat Paskin-Cherniavsky, and Mingyuan Wang. "Improved bound on the local leakage-resilience of Shamir's secret sharing". In: *2022 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2022, pp. 2678–2683.

[MPS+21] Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang. "Constructing Locally Leakage-Resilient Linear Secret-Sharing Schemes". In: *CRYPTO 2021, Part III*. Ed. by Tal Malkin and Chris Peikert. Vol. 12827. LNCS. Virtual Event: Springer, Cham, Aug. 2021, pp. 779–808. DOI: 10.1007/978-3-030-84252-9_26.

[Ngu24] Hai H. Nguyen. "Towards Breaking the Half-Barrier of Local Leakage-Resilient Shamir's Secret Sharing". In: *CRYPTO 2024, Part V*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14924. LNCS. Springer, Cham, Aug. 2024, pp. 257–285. DOI: 10.1007/978-3-031-68388-6_10.

[Ngu25] Hai H. Nguyen. "Physical-Bit Leakage Resilience of Linear Code-Based Secret Sharing". In: *EUROCRYPT 2025, Part VIII*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. LNCS. Springer, Cham, May 2025, pp. 64–93. DOI: 10.1007/978-3-031-91101-9_3.

[NS20] Jesper Buus Nielsen and Mark Simkin. "Lower Bounds for Leakage-Resilient Secret Sharing". In: *EUROCRYPT 2020, Part I*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12105. LNCS. Springer, Cham, May 2020, pp. 556–577. DOI: 10.1007/978-3-030-45721-1_20.

[Sha79] Adi Shamir. "How to Share a Secret". In: *Communications of the Association for Computing Machinery* 22.11 (Nov. 1979), pp. 612–613. DOI: 10.1145/359168.359176.

[SV19] Akshayaram Srinivasan and Prashant Nalini Vasudevan. "Leakage Resilient Secret Sharing and Applications". In: *CRYPTO 2019, Part II*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. LNCS. Springer, Cham, Aug. 2019, pp. 480–509. DOI: 10.1007/978-3-030-26951-7_17.