Showing Improved Security for Shamir's Secret Sharing Scheme

Dustin Kasser

University of Georgia

UNIVERSITY OF GEORGIA

The Scheme

- The secret sharer has $n \in \mathbb{N}$ parties to distribute their secret s among and some security parameter $0 < t < 1$.

The Scheme

- The secret sharer has $n \in \mathbb{N}$ parties to distribute their secret s among and some security parameter $0 < t < 1$.
- They choose a finite field $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ of $p = 2^{o(n)}$ elements to embed their secret in.

The Scheme

- The secret sharer has $n \in \mathbb{N}$ parties to distribute their secret s among and some security parameter $0 < t < 1$.
- They choose a finite field $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ of $p = 2^{o(n)}$ elements to embed their secret in.
- They choose a random polynomial $p(y) \in \mathbb{Z}_p[y]$ with $p(0) = s$ and degree tn. Let $x \in \mathbb{Z}_p^{tn}$ be the vector of its coefficients.

The Scheme

- The secret sharer has $n \in \mathbb{N}$ parties to distribute their secret s among and some security parameter $0 < t < 1$.
- They choose a finite field $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ of $p = 2^{o(n)}$ elements to embed their secret in.
- They choose a random polynomial $p(y) \in \mathbb{Z}_p[y]$ with $p(0) = s$ and degree tn. Let $x \in \mathbb{Z}_p^{tn}$ be the vector of its coefficients.
- To each party i they send the pair $(i, p(i))$ as the share of their secret. We may instead construct some vectors $\{\ell_i\}_{i=0}^{n} \in \mathbb{Z}_p^{tn}$ such that $\ell_i \cdot x = p(i)$ and send the shares $(i, p(i))$.

The Scheme

- The secret sharer has $n \in \mathbb{N}$ parties to distribute their secret s among and some security parameter $0 < t < 1$.
- They choose a finite field $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ of $p = 2^{o(n)}$ elements to embed their secret in.
- They choose a random polynomial $p(y) \in \mathbb{Z}_p[y]$ with $p(0) = s$ and degree tn. Let $x \in \mathbb{Z}_p^{tn}$ be the vector of its coefficients.
- To each party i they send the pair $(i, p(i))$ as the share of their secret. We may instead construct some vectors $\{\ell_i\}_{i=0}^{n} \in \mathbb{Z}_p^{tn}$ such that $\ell_i \cdot x = p(i)$ and send the shares $(i, p(i))$.

Definition (Security)

We consider each party $i > 0$ to receive the share $(i, \ell_i \cdot x)$. In this context, the secret is secure against any $tn - 1$ shares being totally corrupted and can be retrieved from tn shares.

One-Bit Leakage Results

- Let $f_i : \mathbb{Z}_p \to \{-1, 1\}$ represent the leakage functions.

Definition (Leakage)

The adversary receives all of the shares $(i, f_i(\ell_i \cdot x))$. The question of interest is how much information can be reconstructed about $\ell_0 \cdot x$ from these shares.

Theorem (Klein and Komargodski 2023)

Shamir's Secret Sharing Scheme is one-bit leakage resilient for $t > 0.688$.

Theorem (K. 2024)

Shamir's Secret Sharing Scheme is one-bit leakage resilient for $t > 0.668$.

The Analytic Proxy

Definition

Let $S \subseteq [n]$. Then we define the function $f_S : \mathbb{Z}_p^{tn} \to \{-1, 1\}$ as

$$f_S(x) = \prod_{i \in S} f_i(\ell_i \cdot x)\,.$$

Theorem (Klein and Komargodski 2023)

If

$$\sum_{S \subseteq [n]} \left| \widehat{f_S}(\ell_0) \right|^2$$

decays exponentially quickly in n for a fixed $0 < t < 1$, the scheme is one-bit leakage resilient.

Bounding $\left|\widehat{f_S}(\ell_0)\right|$

- Let $|S| = (t+a)n$.
- Let $V(S) \subseteq \mathbb{Z}_p^S$ be the set of all vectors v with $\sum_{i\in S} v_i \ell_i = \ell_0$.
- For $w \in \mathbb{Z}_p^{an}$, let $v(w)$ be the unique vector in $V(S)$ where $v_i = w_i$ for each $i \leq an$.

$$\widehat{f_S}(\ell_0) = \sum_{v\in V(S)} \prod_{i\in S} \widehat{f_i}(v_i) = \sum_{w\in\mathbb{Z}_p^{an}} \prod_{i\in S} \widehat{f_i}(v_i(w_i))$$

Bounding $\left|\widehat{f_S}(\ell_0)\right|$

- Let $|S| = (t+a)n$.
- Let $V(S) \subseteq \mathbb{Z}_p^S$ be the set of all vectors v with $\sum_{i \in S} v_i \ell_i = \ell_0$.
- For $w \in \mathbb{Z}_p^{an}$, let $v(w)$ be the unique vector in $V(S)$ where $v_i = w_i$ for each $i \le an$.

$$\widehat{f_S}(\ell_0) = \sum_{v \in V(S)} \prod_{i \in S} \widehat{f_i}(v_i) = \sum_{w \in \mathbb{Z}_p^{an}} \prod_{i \in S} \widehat{f_i}(v_i(w_i))$$

Lemma

If $a < t/3$, then

$$\left|\widehat{f_S(\ell_0)}\right| \le \left(\prod_{i=1}^{4an} \left\|\widehat{f_i}\right\|_{\mathrm{L}^4}\right) \cdot \left(\prod_{i=4an+1}^{(t+a)n} \left\|\widehat{f_i}\right\|_{\mathrm{L}^\infty}\right)$$

Bounding $\left\|\widehat{f_i}\right\|_{L^4}$

Theorem

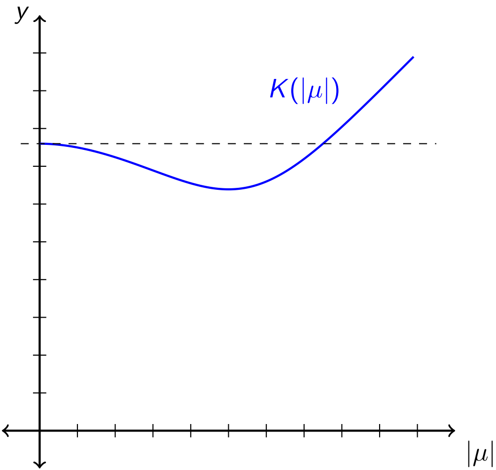
If $f_i : \mathbb{Z}_p \to \{-1, 1\}$ has k entries with $f_i(y) = 1$, then if $g : \mathbb{Z}_p \to \{-1, 1\}$ with $g(y) = 1$ if and only if $y \in [1, k]$, then

$$\left\|\widehat{f_i}\right\|_{L^{2q}} \leq \|\widehat{g}\|_{L^{2q}}$$

For each such g with mean μ, we may explicitly compute the L^{2q} norm as

$$K_{2q}(|\mu|) = \left(|\mu|^{2q} + 2 \sum_{k=1}^{\sqrt{p}} \left| \frac{2}{\pi} \cdot \frac{\sin\left(\pi k \frac{\mu+1}{2}\right)}{k} \right|^{2q} \right)^{1/2q}$$

Graph of $K_4(|\mu|)$



A graph of $K_4(|\mu|)$ on $[0, 1]$ with increments at 0.1 intervals.

Handling When μ Is Not Too Large

Definition ("Mean 0 Set")

We define our good set G to be the set where $|\mu| < 2/\pi$, which is when our L^∞ and L^4 norms are bounded by $K_4(0)$ and $K_\infty(0)$.

Definition (The Good L^4 Set)

We define the set D to be when $|\mu| \in [2/\pi, 0.75]$, and so the L^4 norm is bounded by $K_4(0)$.

Definition (The Bad L^4 Set)

We define the set C to be when $|\mu| \in [0.75, 0.782]$, which is when our bounds on L^4 are not as good as the mean-zero case, but there is little that we can do to fix it.

Handling when μ is Very Large

When μ is large, from an information theoretic perspective, f_i is not conveying very much to the adversary.

Definition (The Weak Induction Set)

We define the set B to be when $|\mu| \in [0.782, 0.836]$, and in this case we can use an induction argument to claim that its L^4 can be replaced by a value no worse than our Bad L^4 set.

Definition (The Strong Induction Set)

We define the set A to be when $|\mu| \in [0.836, 1]$, and in this case we can use an induction argument to replace the L^4 norm with $K(0)$, our mean-zero value.

Using the L^2 induction argument of Klein and Komargodski, we can also say that

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{tn-an+0.555|A|+0.4|B|+\frac{|C|}{3}+0.1238|D|}.$$

Bounds on $\left|\widehat{f_S}(\ell_0)\right|$

Lemma (Klein and Komargodski 2023)

$$\left|\widehat{f_S}(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-a)n}$$

Lemma (K. 2024)

$$\left|\widehat{f_S}(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-0.66a)n}$$

Remark

One should not expect this induction argument to do much better than

$$\left|\widehat{f_S}(\ell_0)\right| \leq 2^{an}\left(\frac{2}{\pi}\right)^{(t+a)n} \leq \left(\frac{2}{\pi}\right)^{(t-0.53a)n} .$$

Setting Up For the Averaging Argument

- Let $a > 0$, and $a \leq K \leq t/2 - a$ be a parameter.
- Let $S' \subseteq [n]$ be of size $(t-K)n$, and we will take it to be fixed.
- Let $\tilde{S} \subseteq S'$ be of size $(K+2a)n$, and we will take it to be a fixed choice.
- Let T be of size $(K+a)n$ with $T \cap S' = \emptyset$, and we will average over all sets of this form.

Definition

We define $\lambda(T)$ to be a vector in $\mathbb{Z}_p^{T \cup S'}$ that fulfills

$$\sum_{i \in S' \cup T} \lambda_i(T)\ell_i = \ell_0$$

and maximizes

$$\prod_{i \in \tilde{S}} \left| \widehat{f_i}(\lambda_i(T)) \right|$$

Peaks Are Far Apart

Lemma

If two sets T and T' share N elements, then there exists some set $B \subseteq \tilde{S}$ of size $N+1$ such that for each $i \in B$,

$$\lambda_i(T) \neq \lambda_i(T')$$

Averaging

Lemma

$$\left|\widehat{f}_{S'\cup T}\right| \le \prod_{i\in\tilde{S}} \left|\widehat{f}_i\left(\lambda_i(T)\right)\right| \cdot \left(\frac{2}{\pi}\right)^{n(t-K-3a)} .$$

$$\sum_T \left|\widehat{f_{S'\cup T}}(\ell_0)\right|^2 \le \sum_T \prod_{i\in\tilde{S}} \left|\widehat{f}_i\left(\lambda_i(T)\right)\right|^2 \cdot \left(\frac{2}{\pi}\right)^{2n(t-K-3a)}$$

Since for each T, λ_i takes different values over $\mathbb{Z}_p^{\tilde{S}}$, we may expand our sum to range over all vectors in $\mathbb{Z}_p^{\tilde{S}}$. Then

$$\sum_T \left|\widehat{f}_S(\ell_0)\right|^2 \le \left(\frac{2}{\pi}\right)^{2n(t-K-3a)} \sum_{\varphi\in\mathbb{Z}_p^{\tilde{S}}} \prod_{i\in\tilde{S}} \left|\widehat{f}_i\left(\lambda_i(T)\right)\right|^2 =$$

$$\left(\frac{2}{\pi}\right)^{2n(t-K-3a)} \prod_{i\in\tilde{S}} \left\|\widehat{f}_i\right\|_{\mathsf{L}^2} = \left(\frac{2}{\pi}\right)^{2n(t-K-3a)}$$

Averaging Bound

We know that

$$\sum_{T} \left|\widehat{f_S}(\ell_0)\right|^2 \le \left(\frac{2}{\pi}\right)^{2n(t-K-3a)}$$

and so

$$\sum_{S'} \sum_{T} \left|\widehat{f_S}(\ell_0)\right|^2 \le \binom{n}{(t-k)n} \left(\frac{2}{\pi}\right)^{2n(t-K-3a)}$$

However, there are many more ways to write a set of size $(t+a)$ as $S' \cup T$ than as simply S, and so when we cancel out over-counting we obtain the following lemma.

Lemma (K. 2024)

$$\sum_{|S|=(t+a)n} \left|\widehat{f_S}(\ell_0)\right|^2 \le O\left(\binom{(t+a)n}{(t-k)n}^{-1} \cdot \binom{n}{(t-k)n} \cdot \left(\frac{2}{\pi}\right)^{2n(t-k-3a)}\right).$$

Thank You