Efficient Leakage-Resilient Secret Sharing

Peihan Miao Akshayaram Srinivasan Prashant Nalini Vasudevan

UC Berkeley

Secret Sharing [Shamir'79, Blakley'79]

$$\sigma \xrightarrow{\text{Share}} sh_1, \dots, sh_n$$

Reconstruction: Given at least t shares, can reconstruct σ

Secrecy: Given (t-1) shares, no information about σ

Several applications: MPC, threshold crypto, leakage-resilient circuit compilers, ...

Efficient constructions, e.g., Shamir, which has rate $=\frac{|\sigma|}{|sh|}=1$

Secret Sharing [Shamir'79, Blakley'79]

$$\sigma \xrightarrow{\text{Share}} sh_1, \dots, sh_n$$

Reconstruction: Given at least t shares, can reconstruct σ

Secrecy: Given (t-1) shares, no information about σ

What if there are side-channels?

What if the adversary, in addition to (t-1) full shares, has some information about the others?

Local Leakage Resilient Secret Sharing [GK'18, BDIR'18]

- 1. Adversary specifies:
 - Set $S \subseteq [n]$ of size at most (t-1)
 - For $i \notin S$, a leakage function f_i that outputs μ bits
- 2. Adversary is given shares sh_i for $i \in S$, and leakage $f(sh_i)$ for $i \notin S$
- 3. Its views for any two secrets should be statistically close

- Local each f_i depends on one share
- Bounded each f_i outputs few bits
- Otherwise arbitrary

$$leakage\ rate = \frac{\mu}{|sh_i|}$$

What was known

- Guruswami-Wootters '16: Shamir over $GF[2^k]$ not leakage-resilient
- Benhamouda et al '18: Shamir over large-characteristic fields *is* leakage-resilient with leakage rate $\Theta(1)$ for thresholds more than $n o(\log n)$
- Constructions:
 - Goyal-Kumar '18: 2-out-of-n with rate and leakage rate $\Theta\left(\frac{1}{n}\right)$
 - Badrinarayanan-Srinivasan '18: O(1)-out-of-n with rate $O\left(\frac{1}{\log n}\right)$ and leakage rate $O\left(\frac{1}{n\log n}\right)$
- Other models of leakage-resilience for secret sharing have been studied, e.g., Boyle et al '14, Dziembowski-Pietrzak '07, etc.

What we do

Leakage-resilient threshold secret sharing schemes

- for all thresholds,
- with constant rate,
- supporting any constant leakage rate

In this talk: simpler construction with slightly worse rate, supporting leakage rate up to 1/2

Our construction

Threshold t, secret $\sigma \in \mathbb{F}$, leakage bound of μ bits

Sample
$$s, w_1, ..., w_n \leftarrow \mathbb{F}^m$$
, and $r \leftarrow \mathbb{F}$

$$\sigma \xrightarrow[t\text{-out-of-}n]{shamir} shamir$$

$$(s,r) \xrightarrow[2\text{-out-of-}n]{shamir} sr_1, ..., sr_n$$

$$\text{Shamir}$$

$$i^{th} \text{ share: } (w_i, sh_i + \langle w_i, s \rangle + r, sr_i)$$

(*m* specified later)

Reconstruction

$$i^{th}$$
 share: $(\mathbf{w_i}, sh_i + \langle \mathbf{w_i}, s \rangle + r, sr_i)$

Given shares of t different i's:

- 1. Reconstruct s and r from $\{sr_i\}$
- 2. Recover sh_i from $(sh_i + \langle w_i, s \rangle + r)$
- 3. Reconstruct σ from $\{sh_i\}$

Adversary knows:

- $(\mathbf{w_i}, sh_i + \langle \mathbf{w_i}, \mathbf{s} \rangle + r, \mathbf{sr_i})$ for $i \in S$, where |S| < t
- $f_i(\mathbf{w_i}, sh_i + \langle \mathbf{w_i}, \mathbf{s} \rangle + r, \mathbf{sr_i})$ for $i \notin S$
- Possibly \boldsymbol{s} and r

Approach:

- 1. For the $i \notin S$, replace $(sh_i + \langle w_i, s \rangle)$ with random $u_i \in \mathbb{F}$
- 2. Show that adversary cannot tell this was done (by a hybrid argument)
- 3. By secrecy of t-out-of-n sharing, adversary's view is independent of secret σ

Claim: For any $i \notin S$, even given s and r,

$$f_i(\mathbf{w_i}, sh_i + \langle \mathbf{w_i}, \mathbf{s} \rangle + r, \mathbf{sr_i}) \approx f_i(\mathbf{w_i}, u_i + r, \mathbf{sr_i})$$

Leftover Hash Lemma [ILL89]:

 $\langle w_i, s \rangle$ is almost uniformly random given s and leakage $g(w_i)$, if $|g(w_i)| \ll |w_i|$

Claim: For any $i \notin S$, even given s and r,

$$f_i(\mathbf{w_i}, sh_i + \langle \mathbf{w_i}, \mathbf{s} \rangle + r, \mathbf{sr_i}) \approx f_i(\mathbf{w_i}, u_i + r, \mathbf{sr_i})$$

Leftover Hash Lemma [ILL89]:

 $\langle w_i, s \rangle$ is almost uniformly random given s and leakage $g(w_i)$, if $|g(w_i)| \ll |w_i|$

should be independent of ${m s}$

Claim: For any $i \notin S$, even given **s** and r,

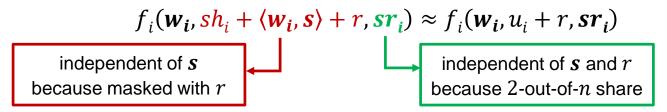
$$f_i(\boldsymbol{w_i}, sh_i + \langle \boldsymbol{w_i}, \boldsymbol{s} \rangle + r, \boldsymbol{sr_i}) \approx f_i(\boldsymbol{w_i}, u_i + r, \boldsymbol{sr_i})$$
 independent of \boldsymbol{s} and r because 2-out-of- n share

Leftover Hash Lemma [ILL89]:

 $\langle w_i, s \rangle$ is almost uniformly random given s and leakage $g(w_i)$, if $|g(w_i)| \ll |w_i|$

should be independent of ${m s}$

Claim: For any $i \notin S$, even given s and r,

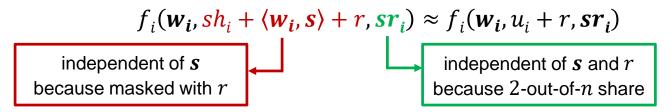


Leftover Hash Lemma [ILL89]:

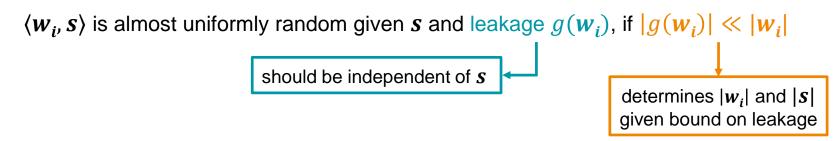
 $\langle w_i, s \rangle$ is almost uniformly random given s and leakage $g(w_i)$, if $|g(w_i)| \ll |w_i|$

should be independent of $oldsymbol{s}$

Claim: For any $i \notin S$, even given s and r,



Leftover Hash Lemma [ILL89]:



What we get

For local leakage resilient threshold secret sharing of:

- secrets in F,
- among n parties $(n \leq |\mathbb{F}|)$,
- against μ bits of leakage per share,
- with adversarial advantage at most ϵ ,

$$|\mathbf{w}_i| = |\mathbf{s}| = m \approx 1 + \frac{\mu}{\log|\mathbb{F}|} + \frac{3\log(4n/\epsilon)}{\log|\mathbb{F}|}$$

Share size: (2m + 2) field elements

Share size overhead

Share sizes for secrets in a field \mathbb{F} , with $|\mathbb{F}| \approx 2^{128}$, and $\epsilon = 1/2^{80}$

$$n = 2$$

Leakage	Share size (bits)	Overhead
1 bit	1024	8
100 bits	1280	10
10%	1280	10
30%	2560	20
45%	10240	80
49%	50688	396

$$n = 100$$

Leakage	Share size (bits)	Overhead
1 bit	1280	10
100 bits	1280	10
10%	1536	12
30%	2816	22
45%	10496	82
49%	52480	410

Computational overhead

Computational overhead in sharing time over Shamir secret sharing, for various leakage rates*

((n,t)	Shamir	0.1%	10%	30%	45%	49%
((2, 2)	$4.16~\mu \mathrm{s}$	7.08	9.78	19.6	83.5	406
(1	(00, 2)	$41.4 \ \mu s$	23.6	26.1	74.1	292	1319
(10	(00, 50)	$1.13~\mathrm{ms}$	1.72	1.75	2.83	9.78	46.1
(10	0, 100)	$2.27~\mathrm{ms}$	1.36	1.44	2.13	5.01	21.2

^{*} as observed on a machine with 4-core 2.9 GHz CPU and 16 GB of RAM

Improvements

- Generalisation to secret sharing for any monotone access structure
- Leakage rate up to 1, and constant-factor improvement in rate using better extractors than inner product

In full version:

- Rate-preserving transformation to non-malleable secret sharing
- Leakage-tolerant MPC for general interactions patterns

Concurrent work

Stronger leakage-resilient and non-malleable secret-sharing schemes for general access structures, Aggarwal et al

- general leakage-resilience transformation, with O(1/n) rate loss, constant leakage rate,
- non-malleable secret sharing against concurrent tampering,
- leakage-resilient threshold signatures

Leakage-resilient secret sharing, Kumar et al

- secret sharing schemes resilient against adaptive leakage,
- non-malleable secret sharing against tampering with leakage



Thank You!