Robust Secret Sharing Schemes Against Local Adversaries

Allison Bishop Lewko   Valerio Pastro

Columbia University

April 2, 2015

Secret Sharing (Informal)

(Share, Rec) pair of algorithms:

$$s \xmapsto{\text{Share}} (s_1, \ldots, s_n) \xmapsto{\text{Rec}} s$$

t-**privacy:** $s_1, \ldots, s_t \quad \Rightarrow \quad$ no info on s

r-**reconstructability:** $s_1, \ldots, s_r \quad \Rightarrow \quad s$ uniquely determined

For **threshold schemes**: $r = t + 1$.

Example: Shamir Secret Sharing [Sha79]

$\mathbb{F}$ field, public $x_1, \ldots, x_n \in \mathbb{F}$.

Shamir.Share$_t(s)$:

1. pick uniform $a_1, \ldots, a_t \in \mathbb{F}$
2. define polynomial $f(X) := s + \sum_{j=1}^{t} a_j X^j \in \mathbb{F}[X]$
3. compute $s_i \leftarrow f(x_i)$
4. output $(s_1, \ldots, s_n)$

Shamir.Rec$_t(s_1, \ldots, s_n)$:

1. Lagrange interpolation to recover $f(X)$
2. output $f(0)$

Robust Secret Sharing – Standard Model

(Share, Rec) Secret Sharing, (t, δ)-**robust**: for any Adv,

$$s \xmapsto{\text{Share}} (s_1, \ldots, s_t, s_{t+1}, \ldots, s_n)$$

$$\downarrow (\widetilde{s}_1, \ldots, \widetilde{s}_t) = \text{Adv}(s_1, \ldots, s_t)$$

$$(\widetilde{s}_1, \ldots, \widetilde{s}_t, s_{t+1}, \ldots, s_n) \xmapsto{\text{Rec}} s'$$

$$\Pr[s' \neq s] \leq \delta$$

Robust Secret Sharing – with Local Adversaries

(Share, Rec) Secret Sharing, **locally** (t, δ)-**robust**: for any $\mathsf{Adv}_1, \ldots, \mathsf{Adv}_t$,

$$s \xmapsto{\text{Share}} (s_1, \ldots, s_t, s_{t+1}, \ldots, s_n)$$

$$\Big\downarrow\ \widetilde{s}_1 = \mathsf{Adv}_1(s_1), \ldots, \widetilde{s}_t = \mathsf{Adv}_t(s_t)$$

$$(\widetilde{s}_1, \ldots, \widetilde{s}_t, s_{t+1}, \ldots, s_n) \xmapsto{\text{Rec}} s'$$

$$\Pr[s' \neq s] \leq \delta$$

Does Locality Make Sense?

It captures the following:

Pre-Game: Players talk to each other, set their actions

Game:
- Players are given private inputs
- Players run protocol without revealing inputs to others
- Output of protocol is set

Post-Game: Players talk to each other again, possibly revealing inputs

Similar to collusion-free protocols [LMs05].

Locality – Possible Scenarios

- Corrupt parties unwilling to coordinate (e.g. different goals)
- Corrupt parties oblivious about existence of each other
- Network with (independently) faulty channels
- Data is required to travel fast, coordination impossible
- ...

Locality – Related Work

Interactive Proofs:

- Multi-prover interactive proofs:
  MIP=NEXP, [BFL91] (IP=PSPACE, [Sha92])

Multi-party Computation:

- Collusion-free protocols [LMs05, AKL+09, AKMZ12]
- Local UC [CV12]

Leakage-resilient crypto:

- Split secret state and independent leakage [DP08]

Facts about Robust Secret Sharing

$t < n/3$: perfect robustness ($\delta = 0$)

no share size overhead ($|s_i| = |s| =: m$)

e.g. Shamir share + Reed-Solomon decoding

RS decodes up to $(n - t)/2 > (3 \cdot t - t)/2 = t$ errors

$n/3 \leq t < n/2$: tricky!

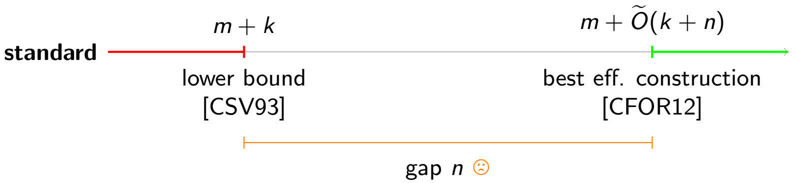
no perfect robustness ($\delta = 2^{-k}$) [Cev11]

shares larger than secret ($|s_i| > m$) [Cev11]

All of the above: independent of standard/local adv. model

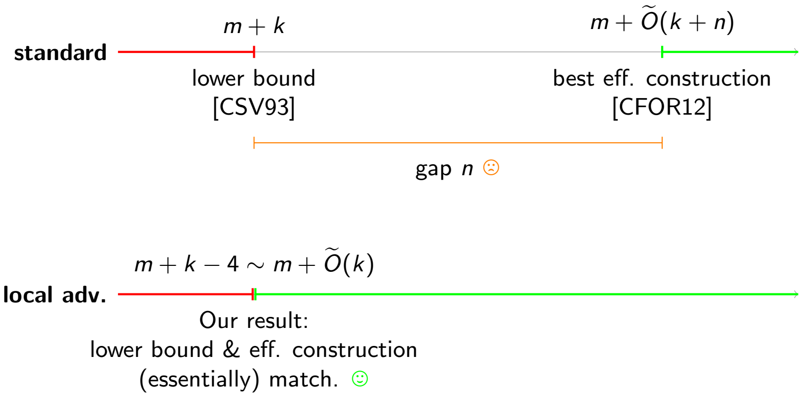
The Tricky Case

The trickiest case: $n = 2 \cdot t + 1$.
Analysis of $|s_i|$:



The Tricky Case

The trickiest case: $n = 2 \cdot t + 1$.
Analysis of $|s_i|$:



Our Construction[1]

Previous Constructions

Privacy: Shamir secret sharing, degree$=t$

Robustness: one-time MAC, $O(n)$ keys per player.

$\Rightarrow |s_i|$ inherent depends (at least) linearly on n

Our Construction

Privacy: Shamir secret sharing, degree$=t$

Robustness: one-time MAC, one key only.

[1] Conceptually simpler; thanks to Daniel Wichs for fruitful discussions.

In Detail

Share(s):

1. sample MAC key $z \in X$
2. $(s_1, \ldots, s_n) \leftarrow \text{Shamir.Share}_t(s)$
3. $(z_1, \ldots, z_n) \leftarrow \text{Shamir.Share}_1(z)$
4. $t_i \leftarrow \text{MAC}_z(s_i)$
5. output $S_i = (s_i, z_i, t_i)$ to P_i

Rec($S_1, \ldots, S_n$):

1. $z \leftarrow \text{RS.Rec}_1(z_1, \ldots, z_n)$
2. set $i \in G$ if $t_i = \text{MAC}_z(s_i)$
3. $s \leftarrow \text{Shamir.Rec}_t(s_G)$

Privacy – Proof Intuition

Share(s):

1. sample MAC key $z \in X$
2. $(s_1, \ldots, s_n) \leftarrow \text{Shamir.Share}_t(s)$
3. $(z_1, \ldots, z_n) \leftarrow \text{Shamir.Share}_1(z)$
4. $t_i \leftarrow \text{MAC}_z(s_i)$
5. output $S_i = (s_i, z_i, t_i)$ to P_i

t-**privacy:** z uniform, independent of $s, s_1, \ldots, s_n$
$s_1, \ldots, s_t$ give no info on s, (privacy of Shamir.Share_t)
$t_1, \ldots, t_t$ functions only of $z, s_1, \ldots, s_t$
$\Rightarrow S_1, \ldots, S_t$ give no info on s

Robustness – Proof Intuition

$\mathrm{Rec}(S_1, \ldots, S_n)$:

1. $z \leftarrow \mathrm{RS.Rec}_1(z_1, \ldots, z_n)$
2. set $i \in G$ if $t_i = \mathrm{MAC}_z(s_i)$
3. $s \leftarrow \mathrm{Shamir.Rec}_t(s_G)$

(t, δ)-**robustness:** z correct, because $\mathrm{RS.Rec}_1$ decodes up to $(n-1)/2 = (2t+1-1)/2 = t$ errors

Adv_i **sees only** s_i, z_i, t_i
$\Rightarrow$ no info on z (privacy of $\mathrm{Shamir.Share}_1$)

MAC ε-secure
$\Rightarrow \Pr[i \in G \mid \widetilde{s}_i \neq s_i] \leq \varepsilon$
$\Rightarrow \Pr[G \subseteq H \cup P] \geq 1 - t \cdot \varepsilon$
$\Rightarrow \delta \leq t \cdot \varepsilon$

Possible MAC and Overhead Analysis

Remember: $\delta \leq t \cdot \varepsilon$

Assume: $m = |s|, \qquad 2 \cdot c = |z|, \qquad c = |t_i|, \qquad m = 2 \cdot d \cdot c$

$$\begin{array}{rcccl} \text{MAC}: & (\mathbb{F}_{2^c})^2 & \times & \mathbb{F}_{2^m} & \to & \mathbb{F}_{2^c} \\ & (a, b), & & (m_1, \ldots, m_d) & \mapsto & \sum_{l=1}^{d} a^l \cdot m_l + b. \end{array}$$

Possible MAC and Overhead Analysis

Remember: $\delta \leq t \cdot \varepsilon$
Assume: $m = |s|, \quad 2 \cdot c = |z|, \quad c = |t_i|, \quad m = 2 \cdot d \cdot c$

$$\begin{array}{rccccl} \text{MAC}: & (\mathbb{F}_{2^c})^2 & \times & \mathbb{F}_{2^m} & \to & \mathbb{F}_{2^c} \\ & (a, b), & & (m_1, \ldots, m_d) & \mapsto & \sum_{l=1}^{d} a^l \cdot m_l + b. \end{array}$$

Fact: MAC is $\varepsilon = d \cdot 2^{-c}$-secure.

Possible MAC and Overhead Analysis

Remember: $\delta \leq t \cdot \varepsilon$
Assume: $m = |s|, \qquad 2 \cdot c = |z|, \qquad c = |t_i|, \qquad m = 2 \cdot d \cdot c$

$$\begin{array}{rccccl} \mathrm{MAC}: & (\mathbb{F}_{2^c})^2 & \times & \mathbb{F}_{2^m} & \to & \mathbb{F}_{2^c} \\ & (a, b), & & (m_1, \ldots, m_d) & \mapsto & \sum_{l=1}^{d} a^l \cdot m_l + b. \end{array}$$

Fact: MAC is $\varepsilon = d \cdot 2^{-c}$-secure.
$\Rightarrow$ construction is $\delta = t \cdot \varepsilon = t \cdot d \cdot 2^{-c} = t \cdot m \cdot 2^{-c-1} \cdot c^{-1}$-secure.

Possible MAC and Overhead Analysis

Remember: $\delta \leq t \cdot \varepsilon$
Assume: $m = |s|, \quad 2 \cdot c = |z|, \quad c = |t_i|, \quad m = 2 \cdot d \cdot c$

$$\begin{array}{llcll} \mathrm{MAC}: & (\mathbb{F}_{2^c})^2 & \times & \mathbb{F}_{2^m} & \rightarrow & \mathbb{F}_{2^c} \\ & (a, b), & & (m_1, \ldots, m_d) & \mapsto & \sum_{l=1}^{d} a^l \cdot m_l + b. \end{array}$$

Fact: MAC is $\varepsilon = d \cdot 2^{-c}$-secure.
$\Rightarrow$ construction is $\delta = t \cdot \varepsilon = t \cdot d \cdot 2^{-c} = t \cdot m \cdot 2^{-c-1} \cdot c^{-1}$-secure.

Set $c = k + \log(t \cdot m) = \widetilde{O}(k) \Rightarrow \delta \leq t \cdot m \cdot 2^{-k-\log(t \cdot m)-1} \cdot c^{-1} \leq 2^{-k}$

Overhead: $|z| + |t_i| = 2c + c = 3c = \widetilde{O}(k)$

Possible MAC and Overhead Analysis

Remember: $\delta \leq t \cdot \varepsilon$
Assume: $m = |s|, \qquad 2 \cdot c = |z|, \qquad c = |t_i|, \qquad m = 2 \cdot d \cdot c$

$$\begin{array}{rcccl} \text{MAC}: & (\mathbb{F}_{2^c})^2 & \times & \mathbb{F}_{2^m} & \rightarrow & \mathbb{F}_{2^c} \\ & (a, b), & & (m_1, \ldots, m_d) & \mapsto & \sum_{l=1}^{d} a^l \cdot m_l + b. \end{array}$$

Fact: MAC is $\varepsilon = d \cdot 2^{-c}$-secure.
$\Rightarrow$ construction is $\delta = t \cdot \varepsilon = t \cdot d \cdot 2^{-c} = t \cdot m \cdot 2^{-c-1} \cdot c^{-1}$-secure.

Set $c = k + \log(t \cdot m) = \widetilde{O}(k) \Rightarrow \delta \leq t \cdot m \cdot 2^{-k-\log(t \cdot m)-1} \cdot c^{-1} \leq 2^{-k}$

Overhead: $|z| + |t_i| = 2c + c = 3c = \widetilde{O}(k)$ ☺

Optimality of Construction

Want to show:

Scheme $(t, 2^{-k})$-robust against local advs $\Rightarrow |s_i| \geq m + k - 4$

Optimality of Construction

Want to show:

Scheme $(t, 2^{-k})$-robust against local advs $\Rightarrow |s_i| \geq m + k - 4$

What we do: prove a stronger result!

Scheme $(t, 2^{-k})$-robust against *oblivious* advs $\Rightarrow |s_i| \geq m + k - 4$

local adv: $\widetilde{s_i} = \mathsf{Adv}_i(s_i)$
oblivious adv: $\widetilde{s_i} = \mathsf{Adv}_i(\varnothing)$

Optimality of Construction

Want to show:

$$\text{Scheme } (t, 2^{-k})\text{-robust against local advs} \Rightarrow |s_i| \geq m + k - 4$$

What we do: prove a stronger result!

$$\text{Scheme } (t, 2^{-k})\text{-robust against } \textit{oblivious} \text{ advs} \Rightarrow |s_i| \geq m + k - 4$$

local adv: $\widetilde{s_i} = \mathsf{Adv}_i(s_i)$
oblivious adv: $\widetilde{s_i} = \mathsf{Adv}_i(\varnothing)$

Proof structure:

1. define an oblivious attack
2. link success of attack with share size

The Attack

Let s_{t+1} be the shortest share.

Specifications:

- "decide" whether to corrupt $P_1, \ldots, P_t$ (L) or $P_{t+2}, \ldots, P_n$ (R)
- sample secret $\widetilde{s} \leftarrow \mathcal{M}$, randomness $\widetilde{r} \leftarrow \mathcal{R}$
- run $(\widetilde{s_1}, \ldots, \widetilde{s_n}) \leftarrow \text{Share}(\widetilde{s}, \widetilde{r})$
- if L, submit $\widetilde{s_1}, \ldots, \widetilde{s_t}$; if R, submit $\widetilde{s_{t+2}}, \ldots, \widetilde{s_n}$

The Attack

Let s_{t+1} be the shortest share.

Specifications:

- "decide" whether to corrupt $P_1, \ldots, P_t$ (L) or $P_{t+2}, \ldots, P_n$ (R)
- sample secret $\widetilde{s} \leftarrow \mathcal{M}$, randomness $\widetilde{r} \leftarrow \mathcal{R}$
- run $(\widetilde{s_1}, \ldots, \widetilde{s_n}) \leftarrow \text{Share}(\widetilde{s}, \widetilde{r})$
- if L, submit $\widetilde{s_1}, \ldots, \widetilde{s_t}$; if R, submit $\widetilde{s_{t+2}}, \ldots, \widetilde{s_n}$

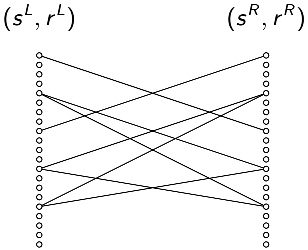
Intuition: hope that corrupt shares & s_{t+1} consistent with dishonest secret.

$$\text{Rec}\left(\overbrace{s_1,\ \ldots,\ s_t,\ s_{t+1}}^{\text{partial sharing of } s^L},\ \underbrace{\phantom{s_{t+1},}\ s_{t+2},\ \ldots,\ s_n}_{\text{partial sharing of } s^R}\right) = ?$$

The Decision

Intuitively: find out whether L is more promising than R.

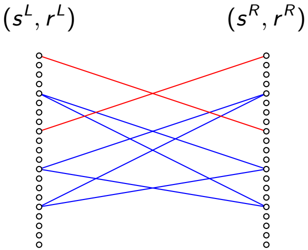
- Graph: (s^L, r^L) connected to (s^R, r^R) if: $\text{Share}(s^L, r^L)_{t+1} = y = \text{Share}(s^R, r^R)_{t+1}$, and $s^L \neq s^R$



The Decision

Intuitively: find out whether L is more promising than R.

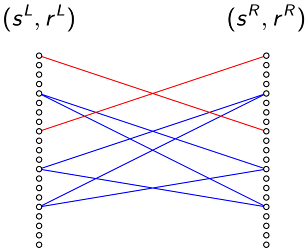
- Graph: (s^L, r^L) connected to (s^R, r^R) if:
  $\text{Share}(s^L, r^L)_{t+1} = y = \text{Share}(s^R, r^R)_{t+1}$, and $s^L \neq s^R$
- Label edge with L (resp. R) if:
  $\text{Rec}(s_1^L, \ldots, s_t^L, y, s_{t+2}^R, \ldots, s_n^R) \neq s^R$ resp. $\neq s^L$)



The Decision

Intuitively: find out whether L is more promising than R.

- Graph: (s^L, r^L) connected to (s^R, r^R) if:
  $\text{Share}(s^L, r^L)_{t+1} = y = \text{Share}(s^R, r^R)_{t+1}$, and $s^L \neq s^R$
- Label edge with L (resp. R) if:
  $\text{Rec}(s_1^L, \ldots, s_t^L, y, s_{t+2}^R, \ldots, s_n^R) \neq s^R$ resp. $\neq s^L$)
- Decide L if #L-edges $\geq$ #R-edges.



The Success (WLOG assume L)

$$\underbrace{\overbrace{s_1,\ \ldots,\ s_t}^{}}_{\widetilde{s}}\ \ldots$$

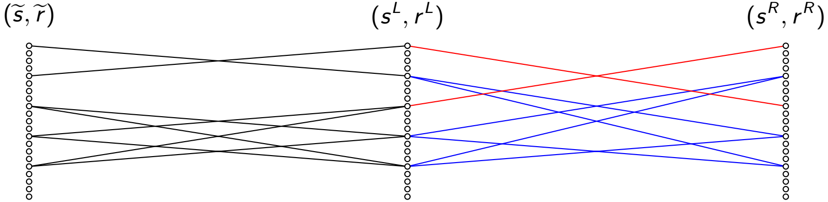
The Success (WLOG assume L)

$$\text{Rec}\left(\underbrace{\overbrace{s_1,\ \ldots,\ s_t}^{}}_{\tilde{s}}\!\!{}^{}\ \ \overbrace{s_1, \ldots, s_t, s_{t+1}}^{s^L},\ \right)$$

$$\text{Rec}\left(\overbrace{\underbrace{s_1,\ \ldots,\ s_t}_{\tilde{s}},\ \underbrace{s_{t+1}}_{}}^{s^L}\underbrace{,\ s_{t+2},\ \ldots,\ s_n}_{s^R}\right) \neq s^R$$

The Success (WLOG assume L)

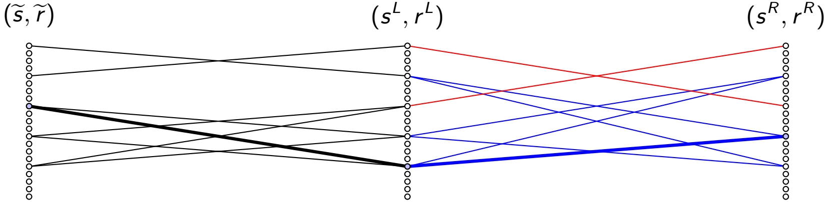
$$\mathrm{Rec}\left(\overbrace{\underbrace{s_1, \ldots, s_t}_{\widetilde{s}}, s_{t+1}}^{s^L}, \underbrace{\phantom{s_{t+1},}s_{t+2}, \ldots, s_n}_{s^R}\right) \neq s^R$$



$\mathsf{Share}(\widetilde{s}, \widetilde{r})_{\{1,\ldots,t\}} = \mathsf{Share}(s^L, r^L)_{\{1,\ldots,t\}}$ $\mathsf{Share}(s^L, r^L)_{t+1} = \mathsf{Share}(s^R, r^R)_{t+1}$

The Success (WLOG assume L)

$$\mathrm{Rec}\left(\overbrace{\underbrace{s_1, \ldots, s_t}_{\widetilde{s}}, s_{t+1}}^{s^L}\hspace{-2em}\underbrace{\phantom{s_{t+1}}, s_{t+2}, \ldots, s_n}_{s^R}\right) \neq s^R$$



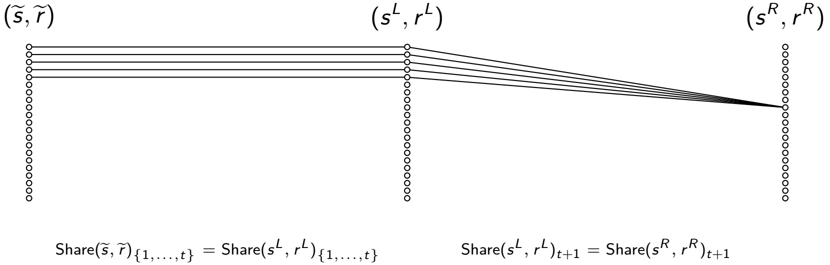
$\mathrm{Share}(\widetilde{s}, \widetilde{r})_{\{1,\ldots,t\}} = \mathrm{Share}(s^L, r^L)_{\{1,\ldots,t\}}$ $\qquad$ $\mathrm{Share}(s^L, r^L)_{t+1} = \mathrm{Share}(s^R, r^R)_{t+1}$

$$\delta = 2^{-k} \geq \Pr_{(\widetilde{s}, \widetilde{r}, s^R, r^R)}[\exists (s^L, r^L) \mid (\widetilde{s}, \widetilde{r}) \text{---} (s^L, r^L) \overset{L}{\text{---}} (s^R, r^R)]$$

Mass Distribution

For $a_1, \ldots, a_{t+1}$,
let $B_{a_1,\ldots,a_{t+1}} = \{(s^L, r^L) \mid \text{Share}(s^L, r^L)_{\{1,\ldots,t+1\}} = a_1, \ldots, a_{t+1}\}$,
let $A_{a_1,\ldots,a_{t+1}} = \{(\widetilde{s}, \widetilde{r}) \mid \text{Share}(\widetilde{s}, \widetilde{r})_{\{1,\ldots,t\}} = a_1, \ldots, a_t\}$.

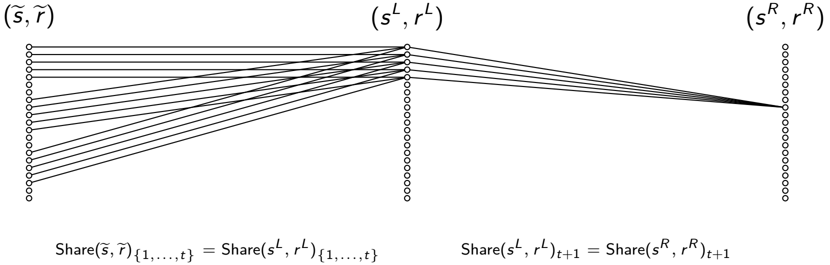
Fact 1*: by reconstructability, $(s', r'), (s'', r'') \in B_{a_1,\ldots,a_{t+1}} \Rightarrow s' = s''$.



Mass Distribution

For $a_1, \ldots, a_{t+1}$,
let $B_{a_1,\ldots,a_{t+1}} = \{(s^L, r^L) \mid \text{Share}(s^L, r^L)_{\{1,\ldots,t+1\}} = a_1, \ldots, a_{t+1}\}$,
let $A_{a_1,\ldots,a_{t+1}} = \{(\widetilde{s}, \widetilde{r}) \mid \text{Share}(\widetilde{s}, \widetilde{r})_{\{1,\ldots,t\}} = a_1, \ldots, a_t\}$.

Fact 1*: by reconstructability, $(s', r'), (s'', r'') \in B_{a_1,\ldots,a_{t+1}} \Rightarrow s' = s''$.
Fact 2: by privacy, $|A_{a_1,\ldots,a_{t+1}}| \geq 2^m \cdot |B_{a_1,\ldots,a_{t+1}}|$.



Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$2^{-k} \geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists (s^L, r^L) \mid (\widetilde{s},\widetilde{r}) \text{—} (s^L, r^L) \overset{\text{L}}{\text{—}} (s^R, r^R)]$$

Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$2^{-k} \geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists(s^L, r^L) \mid (\widetilde{s},\widetilde{r}) \text{—} (s^L, r^L) \overset{\mathsf{L}}{\text{—}} (s^R, r^R)] \qquad \text{(Fact 1\&2)}$$

$$\geq 2^m \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \overset{\mathsf{L}}{\text{—}} (s^R, r^R)]$$

Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$
\begin{aligned}
2^{-k} &\geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists (s^L, r^L) \mid (\widetilde{s}, \widetilde{r}) \text{---} (s^L, r^L) \overset{\text{L}}{\text{---}} (s^R, r^R)] && \text{(Fact 1\&2)} \\
&\geq 2^m \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \overset{\text{L}}{\text{---}} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \text{---} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s^L,r^L,s^R,r^R)}[\text{Share}(s^L, r^L) = a_{t+1}, \text{Share}(s^R, r^R) = a_{t+1}] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s, r) = a_{t+1}]^2
\end{aligned}
$$

Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$
\begin{aligned}
2^{-k} &\geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists(s^L,r^L) \mid (\widetilde{s},\widetilde{r}) — (s^L,r^L) \overset{\text{L}}{—} (s^R,r^R)] && \text{(Fact 1\&2)}\\
&\geq 2^m \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L,r^L) \overset{\text{L}}{—} (s^R,r^R)]\\
&\geq 2^{m-1} \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L,r^L) — (s^R,r^R)]\\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s^L,r^L,s^R,r^R)}[\text{Share}(s^L,r^L) = a_{t+1}, \text{Share}(s^R,r^R) = a_{t+1}]\\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s,r) = a_{t+1}]^2 && \text{(Cauchy-Schwarz)}\\
&\geq 2^{m-1} \cdot 2^{-|s_{t+1}|} \left(\sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s,r) = a_{t+1}] \cdot 1 \right)^2\\
&= 2^{m-1} \cdot 2^{-|s_{t+1}|}
\end{aligned}
$$

Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$
\begin{aligned}
2^{-k} &\geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists (s^L, r^L) \mid (\widetilde{s},\widetilde{r}) \text{—} (s^L, r^L) \overset{\text{L}}{\text{—}} (s^R, r^R)] && \text{(Fact 1\&2)} \\
&\geq 2^m \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \overset{\text{L}}{\text{—}} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \text{—} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s^L,r^L,s^R,r^R)}[\text{Share}(s^L, r^L) = a_{t+1}, \text{Share}(s^R, r^R) = a_{t+1}] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s, r) = a_{t+1}]^2 && \text{(Cauchy-Schwarz)} \\
&\geq 2^{m-1} \cdot 2^{-|s_{t+1}|} \left(\sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s, r) = a_{t+1}] \cdot 1 \right)^2 \\
&= 2^{m-1} \cdot 2^{-|s_{t+1}|}
\end{aligned}
$$

$$|s_{t+1}| \geq m + k - 1$$

Putting Things Together – Intuition

Actual analysis needs more correcting factors (loss of ~ 4 bits).

$$
\begin{aligned}
2^{-k} &\geq \Pr_{(\widetilde{s},\widetilde{r},s^R,r^R)}[\exists (s^L, r^L) \mid (\widetilde{s},\widetilde{r}) \text{---} (s^L, r^L) \overset{\text{L}}{\text{---}} (s^R, r^R)] && \text{(Fact 1\&2)} \\
&\geq 2^m \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \overset{\text{L}}{\text{---}} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \Pr_{(s^L,r^L,s^R,r^R)}[(s^L, r^L) \text{---} (s^R, r^R)] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s^L,r^L,s^R,r^R)}[\text{Share}(s^L, r^L) = a_{t+1}, \text{Share}(s^R, r^R) = a_{t+1}] \\
&\geq 2^{m-1} \cdot \sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s, r) = a_{t+1}]^2 && \text{(Cauchy-Schwarz)} \\
&\geq 2^{m-1} \cdot 2^{-|s_{t+1}|} \left(\sum_{a_{t+1}} \Pr_{(s,r)}[\text{Share}(s, r) = a_{t+1}] \cdot 1 \right)^2 \\
&= 2^{m-1} \cdot 2^{-|s_{t+1}|}
\end{aligned}
$$

$$|s_{t+1}| \geq m + k - 1 \quad ☺$$

Conclusion

Robust SS with $n = 2 \cdot t + 1$ players, eff. reconstruction. Share size:

model	construction	lower bound
standard	$m + \widetilde{O}(n + k)$	$m + k$
NEW: local adv.	$m + \widetilde{O}(k)$	$m + k - 4$

Conclusion

Robust SS with $n = 2 \cdot t + 1$ players, eff. reconstruction. Share size:

model	construction	lower bound
standard	$m + \widetilde{O}(n + k)$	$m + k$
NEW: local adv.	$m + \widetilde{O}(k)$	$m + k - 4$

Future:

- Locality in more complicated settings:
  - info theoretic MPC: circumvent lower bounds?
  - general MPC: more eff/practical protocols?
- standard RSSS: lower bound & construction matching?

Conclusion

Robust SS with $n = 2 \cdot t + 1$ players, eff. reconstruction. Share size:

model	construction	lower bound
standard	$m + \widetilde{O}(n + k)$	$m + k$
NEW: local adv.	$m + \widetilde{O}(k)$	$m + k - 4$

Future:

- Locality in more complicated settings:
  - info theoretic MPC: circumvent lower bounds?
  - general MPC: more eff/practical protocols?
- standard RSSS: lower bound & construction matching?

THANKS!

https://eprint.iacr.org/2014/909

Joël Alwen, Jonathan Katz, Yehuda Lindell, Giuseppe Persiano, abhi shelat, and Ivan Visconti.
Collusion-free multiparty computation in the mediated model.
In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 524–540. Springer, 2009.

Joël Alwen, Jonathan Katz, Ueli Maurer, and Vassilis Zikas.
Collusion-preserving computation.
In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 124–143. Springer, 2012.

László Babai, Lance Fortnow, and Carsten Lund.
Non-deterministic exponential time has two-prover interactive protocols.
Computational Complexity, 1:3–40, 1991.

Alfonso Cevallos.
Reducing the share size in robust secret sharing.
http://www.algant.eu/documents/theses/cevallos.pdf, 2011.

Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani.
Unconditionally-secure robust secret sharing with compact shares.
In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 195–208. Springer, 2012.

Marco Carpentieri, Alfredo De Santis, and Ugo Vaccaro.
Size of shares and probability of cheating in threshold schemes.
In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 118–125. Springer, 1993.

Ran Canetti and Margarita Vald.
Universally composable security with local adversaries.

In Ivan Visconti and Roberto De Prisco, editors, *Security and Cryptography for Networks - 8th International Conference, SCN 2012, Amalfi, Italy, September 5-7, 2012. Proceedings*, volume 7485 of *Lecture Notes in Computer Science*, pages 281–301. Springer, 2012.

Stefan Dziembowski and Krzysztof Pietrzak.
Leakage-resilient cryptography.
In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 293–302. IEEE Computer Society, 2008.

Matt Lepinski, Silvio Micali, and abhi shelat.
Collusion-free protocols.
In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 543–552. ACM, 2005.

Adi Shamir.
How to share a secret.
Commun. ACM, 22(11):612–613, 1979.

Adi Shamir.
IP = PSPACE.
J. ACM, 39(4):869–877, 1992.