Centrum Wiskunde & Informatica

Reconstructing a Shared Secret in the Presence of Faulty Shares

---

A Survey

Serge Fehr

CWI Amsterdam

www.cwi.nl/~fehr

(t-out-of-n) Secret Sharing

secret: $s \in \mathcal{S}$

shares: $s_1 \quad s_2 \quad \cdots \quad s_n$

- **Privacy**: any t shares give no information on s

$$s_1 \quad s_2 \quad \cdots \quad s_t \quad \longrightarrow \quad ?$$

- **Reconstructability**: any $t+1$ shares uniquely determine s

$$s_1 \quad s_2 \quad \cdots \quad s_{t+1} \quad \longrightarrow \quad s$$

Shamir's Secret Sharing Scheme [Sha79]

secret: $s \in \mathbb{F}$

$$f(X) = s + a_1 X + \ldots + a_t X^t \in \mathbb{F}[X]$$

shares: $s_1 = f(x_1) \quad \cdots \quad s_n = f(x_n) \quad (x_i \neq x_j \neq 0 \ \forall\, i \neq j)$

- **Privacy** and **reconstructability** follow from Lagrange interpolation
- Here and in general:
  reconstructability requires correct shares

Robust Secret Sharing

Note:
assume dealer to be honest

secret: s

shares: $s_1 \quad s_2 \quad \cdots \quad s_n$

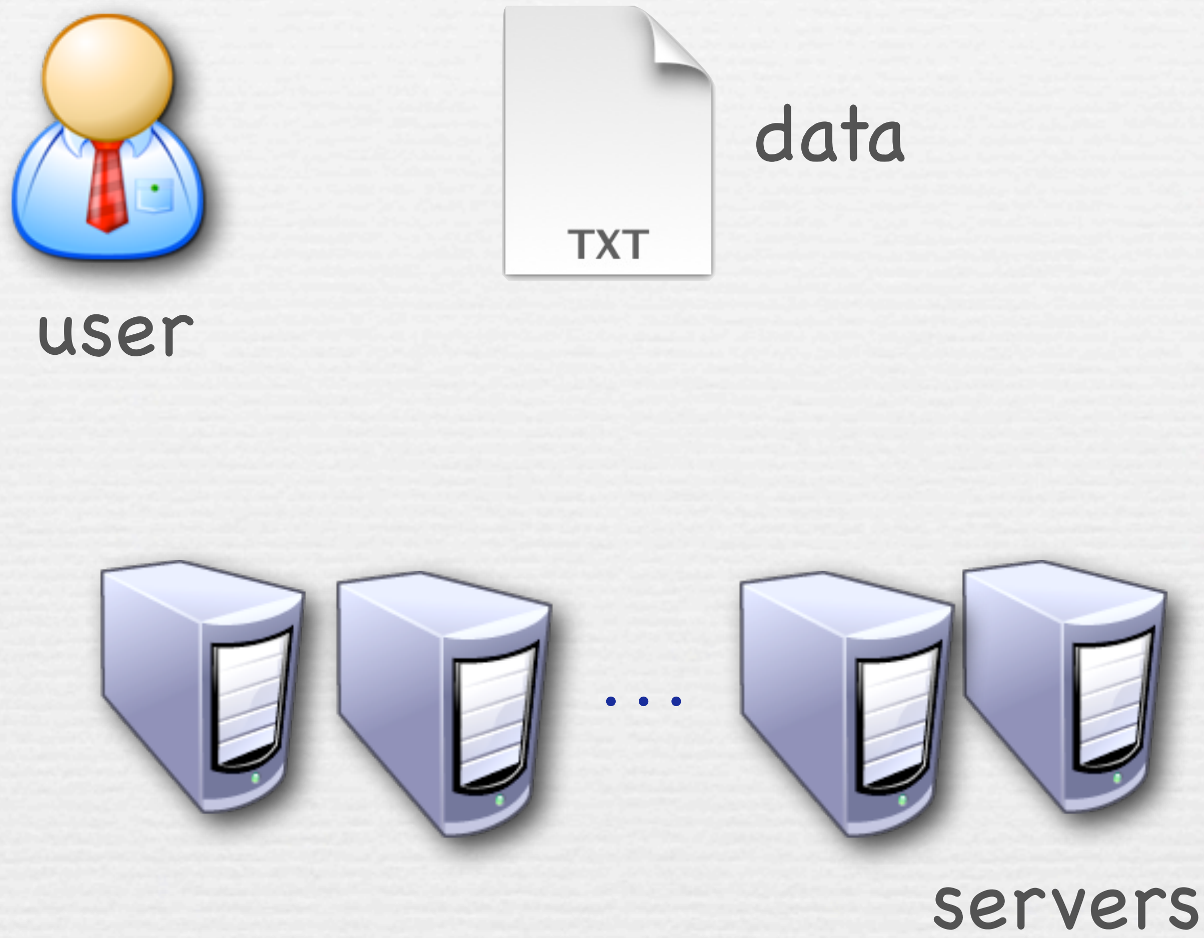
- **Privacy**: any t shares give no information on s

$$s_1 \quad \cdots \quad s_t \quad \longrightarrow \quad ?$$

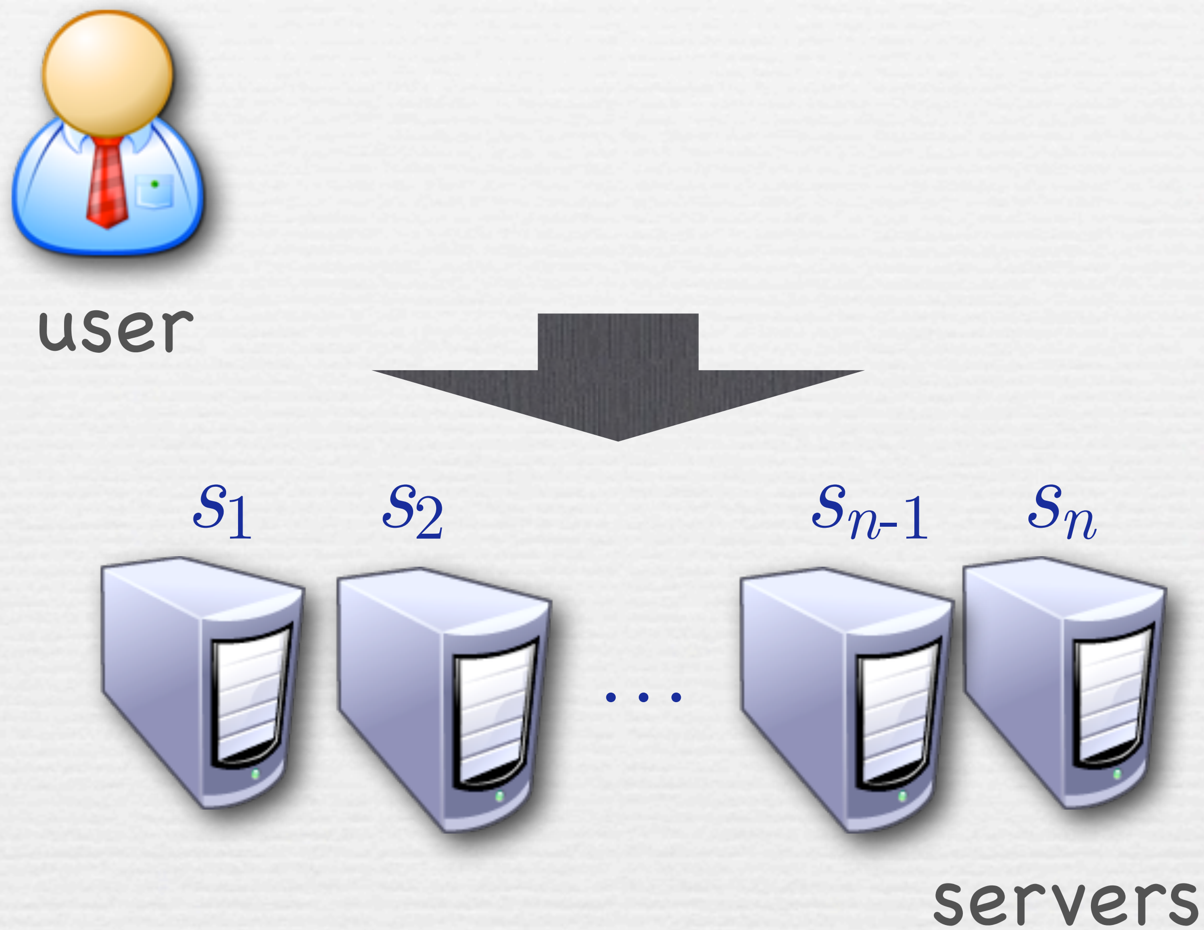
- **Robust reconstructability**:
  the set of all n shares determines s, even if t of them are faulty

$$\hat{s}_1 \quad \cdots \quad \hat{s}_t \quad s_{t+1} \quad \cdots \quad s_n \quad \longrightarrow \quad s$$

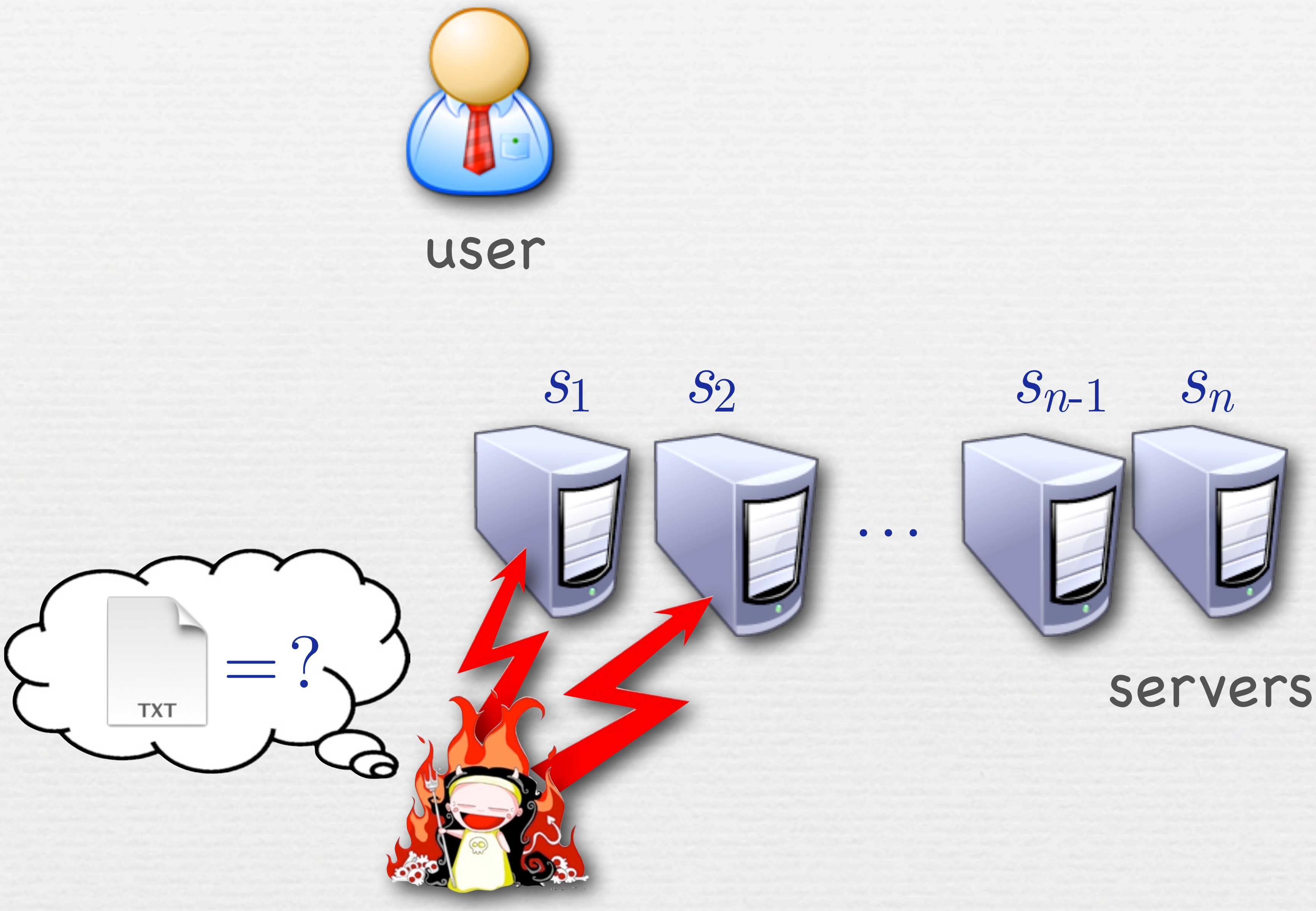
Application: Secure Data Storage



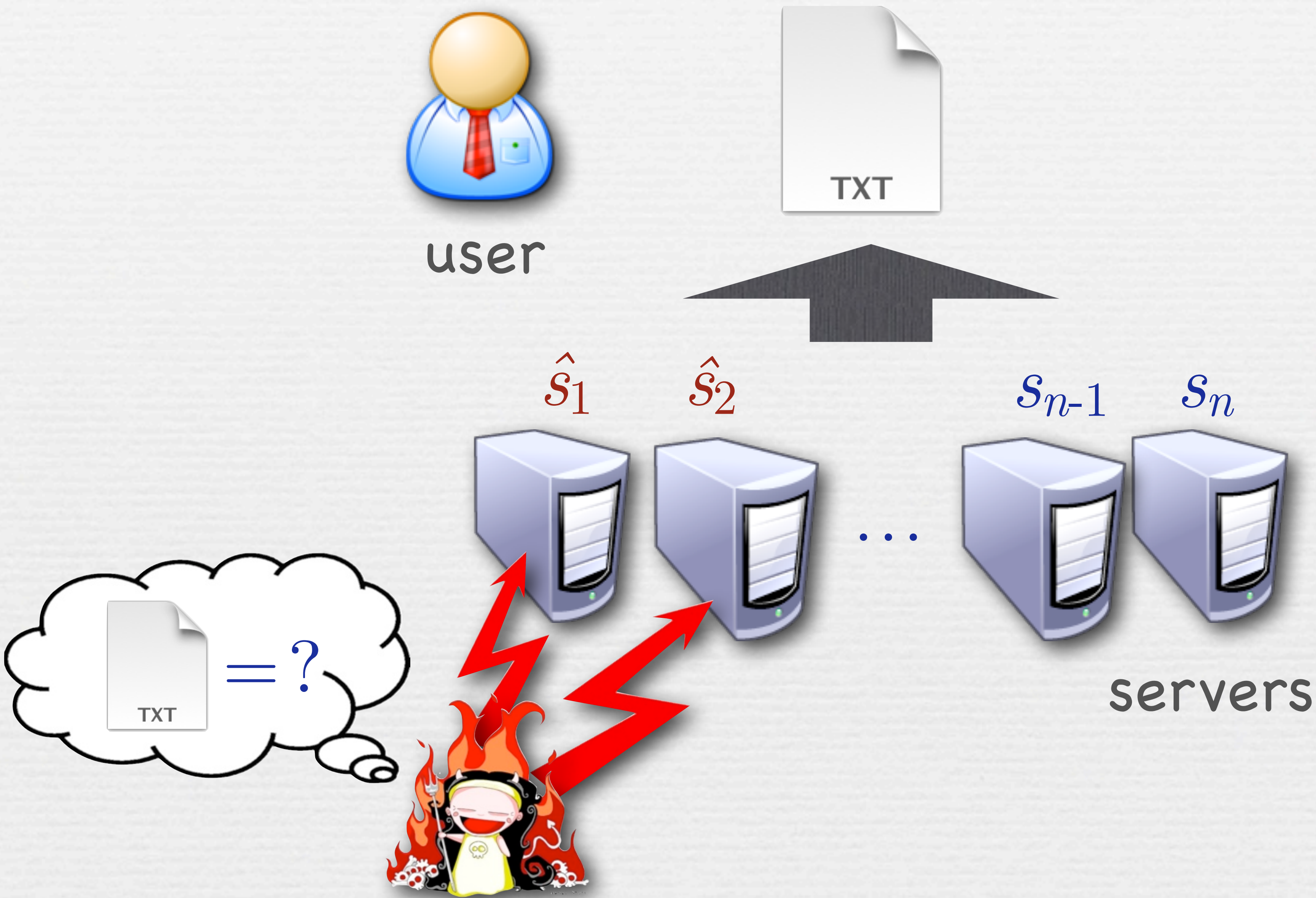
Application: Secure Data Storage



Application: Secure Data Storage

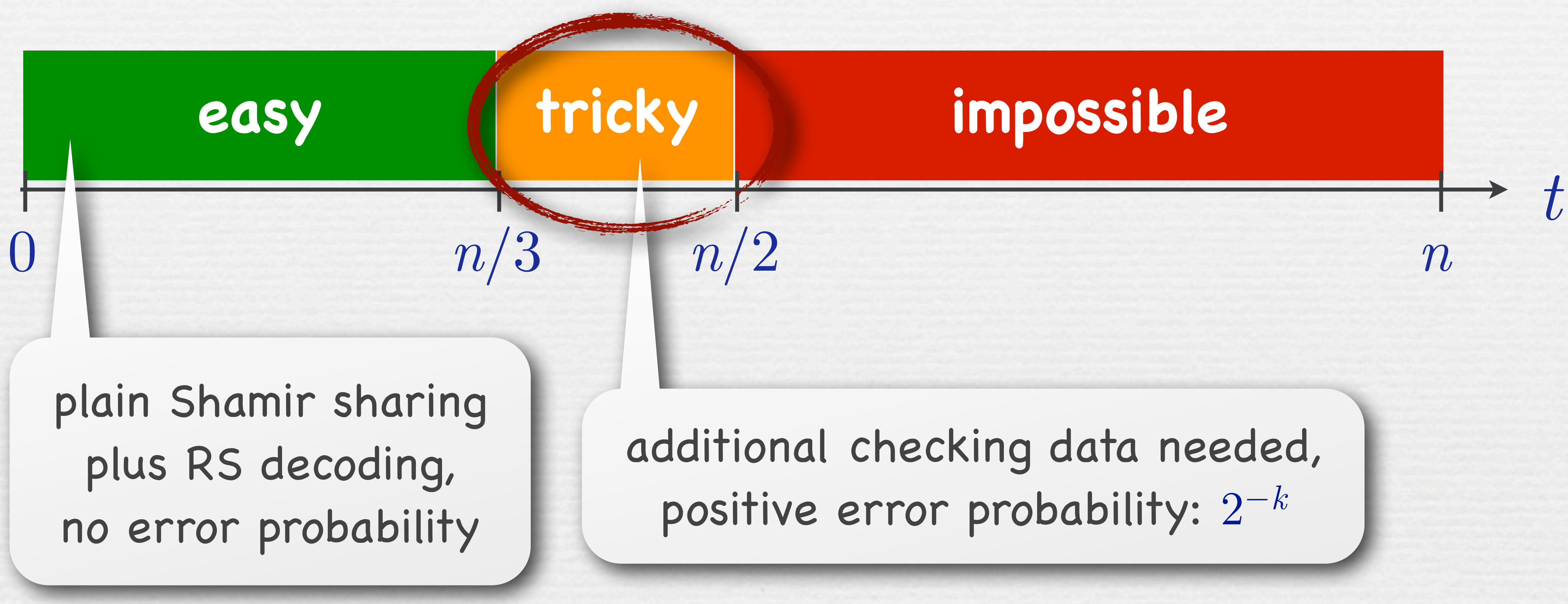


Application: Secure Data Storage



(Im)possibility

This talk: $n = 2t+1$, with unconditional security



Known Schemes

- Rabin & Ben-Or (1989):
  - Overhead in share size: $O(k{\cdot}n{\cdot}\log n)$ ▯
  - Computational complexity: $poly(k,n)$ ☺

- Cramer, Damgård & F (2001), based on Cabello, Padró & Sáez (1999), generalized by Kurosawa & Suzuki (2009):
  - Overhead in share size: $O(k{\cdot}\log n+n)$ ☺ (lower bound: $\Omega(k)$)
  - Computational complexity: $exp(n)$ ▯

- Cevallos, F, Ostrovsky & Rabani (2012):
  - Overhead in share size: $O(k+n{\cdot}\log n)$ ☺
  - Computational complexity: $poly(k,n)$ ☺

Further Outline

- Introduction
- The (simple) case $t < n/3$
- The Rabin & Ben-Or scheme
- The CDF 2001 scheme
- The CFOR 2012 scheme, and discussion of proof
- Conclusion

The (Simple) Case $n = 3t+1$

$$s \in \mathbb{F}$$

$$f(X) = s + a_1 X + \ldots + a_t X^t \in \mathbb{F}[X]$$

$s_1 = f(x_1)$ $\cdots$ s_{t+1} | s_{t+2} $\cdots$ s_{2t+1} | $\hat{s}_{n-t+1}$ $\cdots$ $\hat{s}_n$

$t+1$ correct shares -> determines f

$r=t$ redundant correct shares

$e=t$ faulty shares

Reed-Solomon decoding: If $e \leq r$ (satisfied here) then

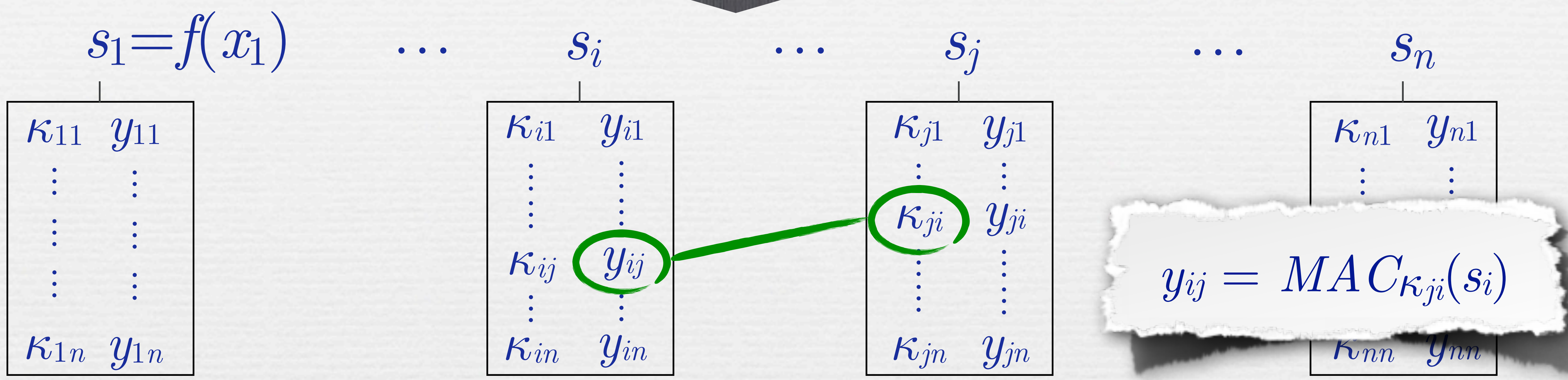
- f is uniquely determined from $s_1, \ldots, \hat{s}_n$
- f can be efficiently computed (Berlekamp-Welch)

The Rabin & Ben-Or Scheme ($n = 2t+1$)

Sharing phase:

$s \in \mathbb{F}$

$f(X) = s + a_1 X + \ldots + a_t X^t \in \mathbb{F}[X]$



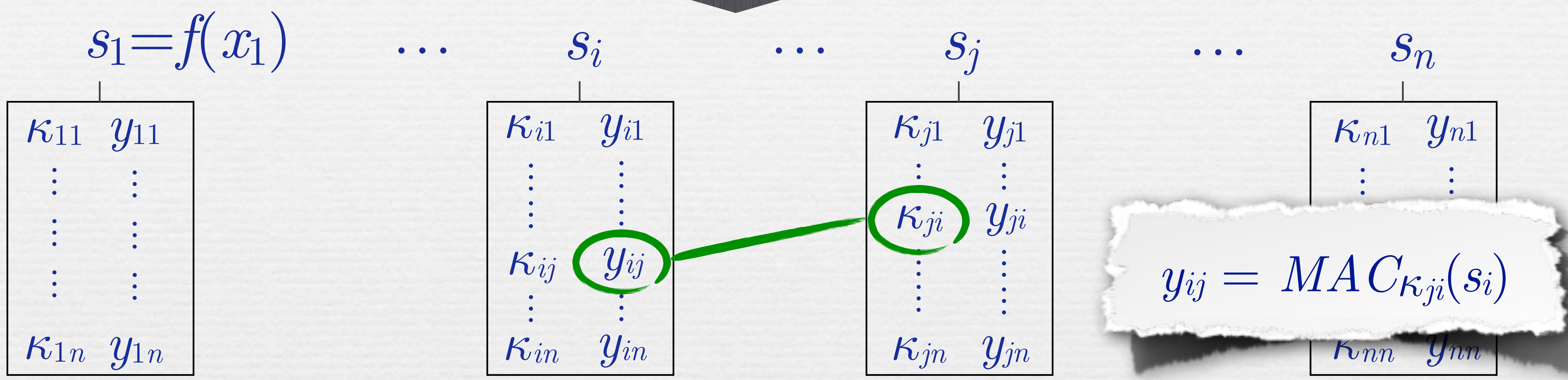
- MAC security: for any $\hat{s}_i \neq s_i$ and $\hat{y}_{ij}$: $P[\hat{y}_{ij} = MAC_{\kappa_{ji}}(\hat{s}_i)] \leq \varepsilon$.
- Example: $\kappa_{ij} = (\alpha_{ij}, \beta_{ij}) \in \mathbb{F}^2$ and $y_{ij} = MAC_{\kappa_{ji}}(s_i) = \alpha_{ij} \cdot s_i + \beta_{ij}$.
- For error probability $\varepsilon \leq 2^{-k}$:
  - bit size $|\kappa_{ij}|, |y_{ij}| \geq k$
  - overhead per share (above Shamir share): $\Omega(k \cdot n)$

The Rabin & Ben-Or Scheme ($n = 2t+1$)

Sharing phase:

$s \in \mathbb{F}$

$f(X) = s + a_1 X + \ldots + a_t X^t \in \mathbb{F}[X]$



Reconstruction phase:

1. For every share s_i:

   accept s_i iff it is consistent with keys of $\geq t+1$ players,

   (meaning $\#\{j \,|\, y_{ij} = MAC_{\kappa_{ji}}(s_i)\} \geq t+1$)

2. Reconstruct s using the accepted shares s_i.

The Rabin & Ben-Or Scheme ($n = 2t+1$)

Analysis

Correct share s_i of honest player:

will be consistent with all $t+1$ honest players

=> will be accepted

Incorrect share $\hat{s}_i$ of dishonest player:

will be consistent with $\leq t$ players (except with prob. $(t+1)\cdot\varepsilon$)

=> will be rejected

Reconstruction phase:

1. For every share s_i :

   accept s_i iff it is consistent with keys of $\geq t+1$ players,

   (meaning $\#\{j \mid y_{ij} = MAC_{K_{ji}}(s_i)\} \geq t+1$)

2. Reconstruct s using the accepted shares s_i .

The CDF 2001 Scheme

Sharing phase:

$s \in \mathbb{F}$, $r \in \mathbb{F}$ and $p = s{\cdot}r \in \mathbb{F}$

$$\begin{array}{lccccc}
s_1 = & f(x_1) & \dots & s_i & \dots & s_n \\
r_1 = & g(x_1) & \dots & r_i & \dots & r_n \\
p_1 = & h(x_1) & \dots & p_i & \dots & p_n
\end{array}$$

Reconstruction phase:

For every $A \subset \{1,\ldots,n\}$ with $|A| = t{+}1$:

- reconstruct s', r' and p' from $(s_i)_{i\in A}$, $(r_i)_{i\in A}$ and $(p_i)_{i\in A}$
- if $s'{\cdot}r' = p'$ then output s' and halt

Note: Running time is exponential in n

Analysis

For any A in the loop:

- if A contains only honest players then $s' \cdot r' = s \cdot r = p = p'$.
- if A contains an incorrect share $\hat{s}_i$ so that $s' \neq s$, then

$$P[s' \cdot r' = p'] \leq 1/|\mathbb{F}| \; .$$

Setting $|\mathbb{F}| \geq 2^{k+n}$ gives error probability $\leq 2^{-k}$.

Proof

By linearity, adversary knows $\Delta s = s' - s$, $\Delta r = r' - r$ and $\Delta p = p' - p$.
Also, we may assume that he knows s .
The equality $s' \cdot r' = p'$ implies that

$$r = (\Delta p - s \cdot \Delta r - \Delta s \cdot \Delta r) / \Delta s \; ,$$

i.e., it requires the adversary to correctly guess r .

The CDF 2001 Scheme

Sharing phase:

$s \in \mathbb{F}$, $r \in \mathbb{K}$ and $p = AMD(r,s) \in \mathbb{K}$

$$
\begin{array}{lllll}
s_1 = f(x_1) & \dots & s_i & \dots & s_n \\
r_1 = g(x_1) & \dots & r_i & \dots & r_n \\
p_1 = h(x_1) & \dots & p_i & \dots & p_n
\end{array}
$$

Generalization/Abstraction:

- algebraic manipulation detection (AMD) codes
- introduced by Cramer, Dodis, F, Padró & Wichs (2008)
- gives flexibility between $\mathbb{F}$ and $\mathbb{K}$ (and thus k)
- e.g.: $\mathbb{F}$ = degree-d extension of $\mathbb{K}$ (so that $\mathbb{F} \cong \mathbb{K}^d$ as $\mathbb{K}$-VS's), and

$$AMD(r,(s_1,\dots,s_d)) = s_1 \cdot r + s_2 \cdot r^2 + \dots + s_d \cdot r^d + r^{d+2}$$

Further Outline

- Introduction
- The (simple) case t < n/3
- The Rabin & Ben-Or scheme
- The CDF 2001 scheme
- The CFOR 2012 scheme, and discussion of proof
- Conclusion

The CFOR 2012 Scheme

Sharing phase:

$$s \in \mathbb{F}$$

$$f(X) = s + a_1 X + \ldots + a_t X^t \in \mathbb{F}[X]$$

$$s_1 = f(x_1) \quad \ldots \quad s_i \quad \ldots \quad s_j \quad \ldots \quad s_n$$

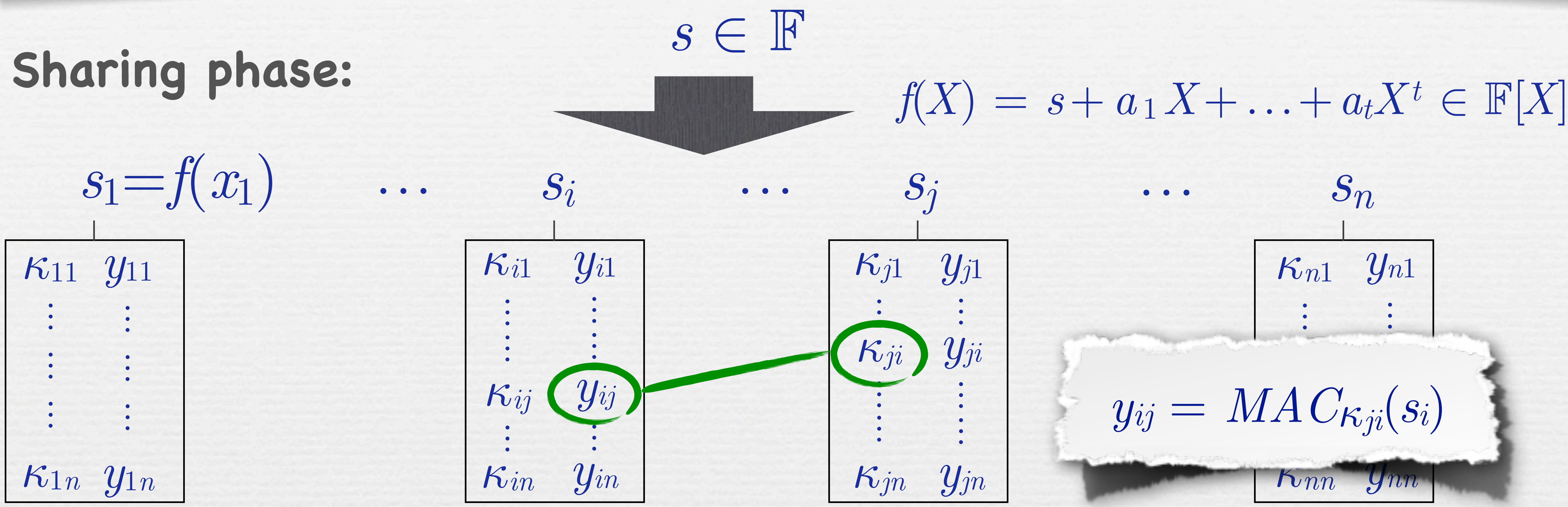
$$\begin{array}{cc} \kappa_{11} & y_{11} \\ \vdots & \vdots \\ \kappa_{1n} & y_{1n} \end{array} \qquad \begin{array}{cc} \kappa_{i1} & y_{i1} \\ \vdots & \vdots \\ \kappa_{ij} & y_{ij} \\ \vdots & \vdots \\ \kappa_{in} & y_{in} \end{array} \qquad \begin{array}{cc} \kappa_{j1} & y_{j1} \\ \vdots & \vdots \\ \kappa_{ji} & y_{ji} \\ \vdots & \vdots \\ \kappa_{jn} & y_{jn} \end{array} \qquad \begin{array}{cc} \kappa_{n1} & y_{n1} \\ \vdots & \vdots \\ \kappa_{nn} & y_{nn} \end{array}$$

$$y_{ij} = MAC_{\kappa_{ji}}(s_i)$$

- Use **small** tags and keys $|\kappa_{ij}|, |y_{ij}| = \tilde{O}(k/n+1)$ (instead of $O(k)$)
- Gives: overhead per share: $n \cdot \tilde{O}(k/n+1) = \tilde{O}(k+n)$
- Problem:
  - MAC has weak security
  - incorrect shares may be consistent with some honest players
  - Rabin & Ben-Or reconstruction fails

The CFOR 2012 Scheme

Sharing phase:



- Use **small** tags and keys $|\kappa_{ij}|, |y_{ij}| = \tilde{O}(k/n + 1)$ (instead of $O(k)$)
- Gives: overhead per share: $n \cdot \tilde{O}(k/n + 1) = \tilde{O}(k + n)$
- Problem
  - MAC
  - incorrect shares may be consistent with some honest players
  - Rabin & Ben-Or reconstruction fails

Need: better reconstruction procedure

Improving the Reconstruct Procedure

- Example: Say that
  - $\{j|\, y_{1j} = MAC_{\kappa_{j1}}(s_1)\} = \{1,\ldots,n\}$ -> accept s_1
  - $\{j|\, y_{2j} = MAC_{\kappa_{j2}}(s_2)\} = \{1,\ldots,t{+}1\}$ -> accept s_2
  - $\{j|\, y_{3j} = MAC_{\kappa_{j3}}(s_3)\} = \{2,\ldots,t{+}1\}$ -> reject s_3
  - ...
- s_2 is consistent with $\leq t$ **honest** players (as player 3 is dishonest)
  => s_2 stems from dishonest player
- Rabin & Ben-Or reconstruction: accepts s_2
- Our new reconstruction: will rejects s_2

Improving the Reconstruct Procedure

- Example: Say that
  - $\{$
  - $\{$
  - $\{$
  - .
- s_2 is … 3 is dishonest)

  =>
- Rabi…
- Our …

Rabin & Ben-Or reconstruction:

Accept every share s_i that is consistent with $t{+}1$ players.

Our new reconstruction:

Accept every share s_i that is consistent with $t{+}1$ players **with accepted shares**.

Plus: Reed-Solomon decoding.

The CFOR Reconstruction Procedure

```
(Init)  Set
```
$Good := \{1,\dots,n\}$

```
(Loop)  For every
```
$i \in Good$:

  if $\#\{j \in Good \mid y_{ij} = MAC_{\kappa_{ji}}(s_i)\} \le t$ then

  - set $Good := Good \setminus \{i\}$
  - redo (Loop)

```
(Dec)   Set
```
$s :=$ Reed-Solomon$(\{s_i\}_{i \in Good})$

Main Theorem. If MAC is ε-secure then our scheme is δ-robust with

$$\delta \le e\cdot((t+1)\cdot\varepsilon)^{(t+1)/2} \qquad \text{(where } e = \exp(1)\text{).}$$

Corollary. Using MAC with $|\kappa_{ij}|, |y_{ij}| = O(k/n + \log n)$ gives $\delta \le 2^{-\Omega(k)}$ and overhead in share size $O(k + n\cdot\log n)$.

What Makes the Proof Tricky

1. **Optimal strategy for dishonest players is unclear**

- In Rabin & Ben-Or: an incorrect share for every dishonest player
- Here: some dishonest players may hand in correct shares
- Such a passive dishonest player:
  - stays in Good
  - can support (i.e. vote for) bad shares
- **The more** such passive dishonest players:
  - **the easier it gets** for bad shares to survive
  - **the more** bad shares have to survive to fool RS decoding (# bad shares $>$ # correct shares of dishonest players)
- Optimal trade-off: unclear

What Makes the Proof Tricky

2. Circular dependencies

- Whether $\hat{s}_i$ gets accepted depends on whether $\hat{s}_j$ gets accepted …
- … and vice versa
- Cannot analyze individual bad shares
- If we try, we run into a circularity

The Proof

Notation:

- $\mathcal{A}/\mathcal{P}/\mathcal{H}$ = active/passive cheaters, and honest players where (wlog) $|\mathcal{A}|+|\mathcal{P}| = t$ and $|\mathcal{H}| = t{+}1$
- $\boldsymbol{\mathcal{S}}$ = players that survive checking phase (clearly: $\mathcal{P},\mathcal{H} \subseteq \boldsymbol{\mathcal{S}}$)

Observations:

- Error probability upper bounded by $\delta = P[\,|\mathcal{A} \cap \boldsymbol{\mathcal{S}}| > |\mathcal{P}|\,]$
- $\delta = 0$ if $|\mathcal{A}| \leq |\mathcal{P}|$. Thus: may assume $a := |\mathcal{A}| > t/2$

Actual proof:

$P[\ldots] \leq \varepsilon$

$$
\begin{aligned}
P[\,|\mathcal{A} \cap \boldsymbol{\mathcal{S}}| > |\mathcal{P}|\,] &= \sum_{\ell = |\mathcal{P}|+1}^{a} P[\,|\mathcal{A} \cap \boldsymbol{\mathcal{S}}| = \ell\,] \\
&\leq \sum_{\ell} P[\exists \mathcal{A}' \in \tbinom{\mathcal{A}}{\ell}\ \forall i \in \mathcal{A}'\ \ \exists \mathcal{H}' \in \tbinom{\mathcal{H}}{a-\ell+1}\ \forall j \in \mathcal{H}' :\ \hat{y}_{ij} = MAC_{\boldsymbol{\kappa}_{ji}}(\hat{s}_i)\,] \\
&\leq \sum_{\ell} \sum_{\mathcal{A}' \in \binom{\mathcal{A}}{\ell}} P[\forall i \in \mathcal{A}'\ \exists \ldots \forall \ldots\,] \leq \sum_{\ell} \sum_{\mathcal{A}' \in \binom{\mathcal{A}}{\ell}} \prod_{i \in \mathcal{A}'} P[\,\exists \ldots \forall \ldots\,] \leq \ldots \\
&\leq \sum_{\ell} \binom{a}{\ell} \cdot \Big(\binom{t+1}{a-\ell+1} \cdot \varepsilon^{a-\ell+1} \Big)^{\ell} \leq \ldots \leq e \cdot ((t+1) \cdot \varepsilon)^{(t+1)/2}
\end{aligned}
$$

Summary

- Three known robust secret sharing schemes for $n = 2t{+}1$
- Newest one (CFOR 2012) has
  - small overhead $O(k{+}n{\cdot}\log n)$ in share size, and
  - efficient sharing and reconstruction procedures
- Is simple and natural adaptation of Rabin & Ben-Or
- Proof is non-standard and non-trivial
- Open problems:
  - Scheme with overhead $O(k)$ (= proven lower bound)
  - Non-threshold access/adversary structure

THANK YOU