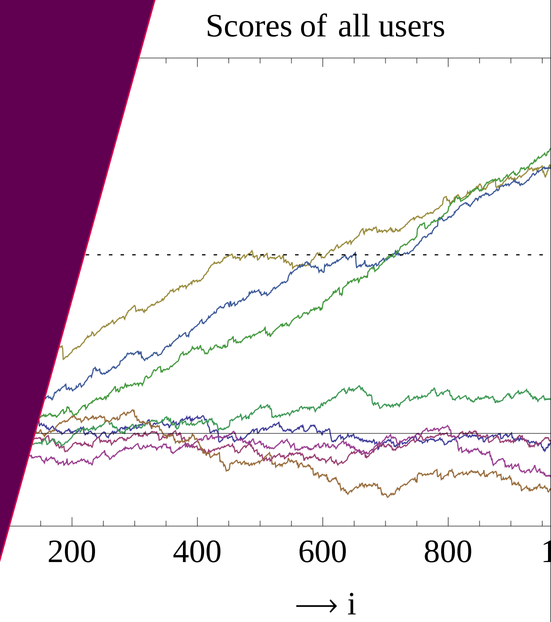
# Collusion-resistant traitor tracing schemes

*Final presentation of Thijs Laarhoven*




May 26th, 2011

# Contents

# Introduction: Illegal redistribution

Digital content is easy to reproduce, so it is easy for people who purchased copyrighted content to distribute it among non-authorized users.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Bob | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Charlie | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Dave | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Eve | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Fred | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| George | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Forgery | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |

Since the content of each copy is the same, it is impossible to find out which of the users is guilty.

# Introduction: Embed watermarks

Embed unique watermarks in each copy so that copies can be identified and traced back to the guilty users.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | w | | | w | w | | | | w | | w | w | w | | |
| Alice | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| Bob | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | ... |
| Charlie | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | ... |
| Dave | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | ... |
| Eve | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |
| Fred | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | ... |
| George | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Forgery | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

This works only if it is hard to detect, edit or remove the watermarks.

# Introduction: Embed watermarks

Embed unique watermarks in each copy so that copies can be identified and traced back to the guilty users.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | w | | | w | w | | | | w | | w | w | w | | |
| Alice | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| Bob | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | ... |
| Charlie | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | ... |
| Dave | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | ... |
| Eve | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |
| Fred | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | ... |
| George | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Forgery | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

This works only if it is hard to detect, edit or remove the watermarks.

# Introduction: Collusion-attacks

Colluders compare their copies, searching for differences. Since their data is the same, the differences must be part of the watermark.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | w | | | w | w | | | | w | | w | w | w | | |
| Alice | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | ... |
| Bob | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | ... |
| Charlie | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | ... |
| Dave | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | ... |
| Eve | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |
| Fred | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | ... |
| George | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| Forgery | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |
| Forgery' | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | ... |

Colluders can then detect and edit that part of the watermark, making it hard to trace them.

# Introduction: Traitor tracing schemes

Construct collusion-resistant traitor tracing codes. What makes the problem hard?

- If the watermarks are very different, then it is easy for colluders to detect and edit big parts of the watermark.
- If the watermarks are very similar, then it is hard to distinguish between users and get accurate accusations.

But using certain mathematical techniques, we can construct schemes resistant against collusion attacks: Even if the output is some mix of coalition codewords, we can identify (part of) the coalition.

# Introduction: What do we want?

In general: Low cost, high efficiency.

- Resistance against all pirate strategies.
- Resistance against large coalitions.
- Short watermarks.
- Small alphabet sizes (large alphabet sizes impractical).
- Low complexity for accusations ($O(n)$ is ok, $O(n^2)$ is not).
- Avoid accusing innocent users.
- Find at least one guilty user (preferably more).

# Model: Traitor tracing codes

Only focus on the watermarks, not on the data itself.

- Users: $j = 1, \ldots, n$.
- Set of users: $U = \{1, \ldots, n\}$.
- Coalition: $C \subseteq U$ of $c$ colluders/traitors/pirates/attackers.
- Traitor tracing code: $\mathcal{C} = \{\vec{x}_j\}$.
  - ▷ Alphabet: $Q = \{0, \ldots, q-1\}$.
  - ▷ Positions: $i = 1, \ldots, \ell$.
  - ▷ Codewords: $\vec{x}_1, \ldots, \vec{x}_n$.

The code $\mathcal{C}$ can also be represented in matrix form by $X_{ji} = (\vec{x}_j)_i$.

$$X = \begin{pmatrix} \longleftarrow & \vec{x}_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & \vec{x}_n & \longrightarrow \end{pmatrix} \text{ e.g. } X = \begin{pmatrix} 0 & 2 & 1 & 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 0 & 0 & 0 & 2 \\ 3 & 3 & 2 & 0 & 1 & 0 & 1 \\ 2 & 3 & 1 & 2 & 2 & 2 & 1 \end{pmatrix} \in \{0, \ldots, 3\}^{4 \times 7}.$$

A coalition generates a forgery $\vec{y}$ using some pirate strategy $\rho : X(C) \mapsto \vec{y}$.

# Model: Pirate strategies

Marking assumption: If the whole coalition sees the same symbol $\omega \in Q$ on position $i$, then also $y_i = \omega$.

Further restrictions: If a coalition sees the symbols $\omega_1, \ldots, \omega_c \in Q$ on position $i$ (not all the same), then...

- Restricted digit model: $y_i \in \{\omega_1, \ldots, \omega_c\}$.
- Arbitrary digit model: $y_i \in Q$.
- Allowing erasures: $y_i \in \ldots$ or $y_i = ?$.
- Binary alphabet: All equivalent.

Most common: Restricted digit model.

Example:

$$\begin{aligned} X(C) &= \begin{pmatrix} 0 & 2 & \mathbf{1} & 1 & \mathbf{2} & 1 & 3 \\ 2 & 3 & \mathbf{1} & 2 & \mathbf{2} & 2 & 1 \end{pmatrix} \\ \vec{y} &\in \left\{\begin{pmatrix} * & * & \mathbf{1} & * & \mathbf{2} & * & * \end{pmatrix}\right\} \\ \text{e.g. } \vec{y}_0 &= \begin{pmatrix} 0 & 3 & \mathbf{1} & 2 & \mathbf{2} & 1 & 3 \end{pmatrix} \end{aligned}$$

# Model: Pirate strategies

Let $q = 2$, let $\omega_1, \dots, \omega_c$ be the symbols seen on position $i$, and let $0 < m < c$ be the number of ones seen by the coalition $C$.

- Random: $y_i \in_R \{0, 1\}$.
- Scapegoat: $y_i = \omega_j$ for some $j$.
- Always 0: $y_i = 0$ whenever possible.
- Majority voting: If $m < c/2$ then $y_i = 0$ and if $m > c/2$ then $y_i = 1$.
  - ▷ If $m = c/2$ then $y_i \in_R \{0, 1\}$.
  - ▷ If $m = c/2$ then $y_i = \omega_j$ for some $j$.
  - ▷ If $m = c/2$ then $y_i = 0/1$.
- Minority voting: If $m < c/2$ then $y_i = 1$ and if $m > c/2$ then $y_i = 0$.
  - ▷ If $m = c/2$ then ...
- Interleaving attack: $y_i \in_R \{\omega_1, \dots, \omega_c\}$ (so $\mathbb{P}[y_i = 1] = m/c$).
- ...

A scheme should be secure against all strategies.

# Model: Static schemes

Construction:

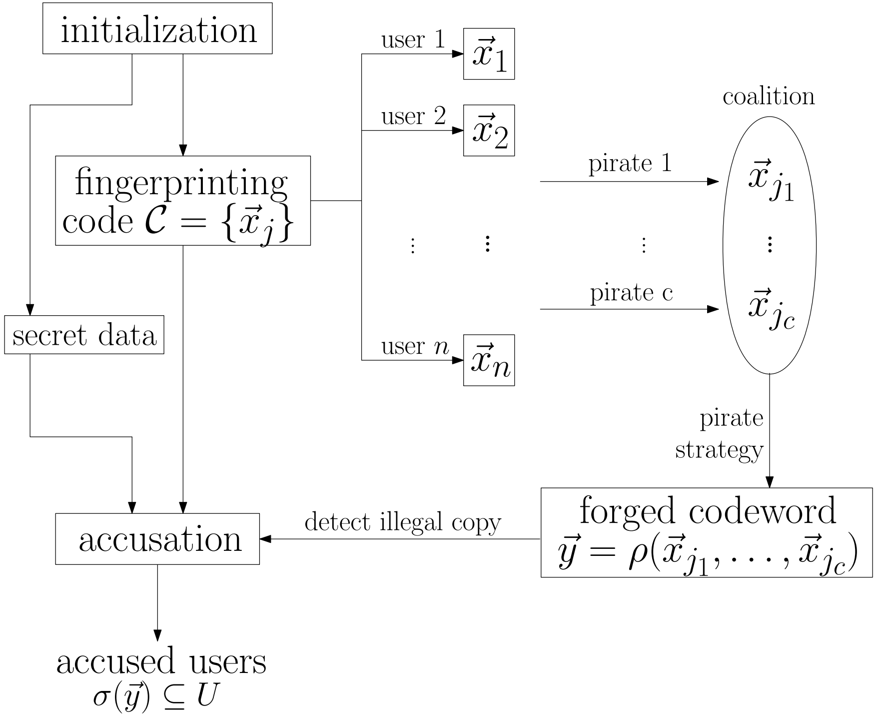
1. Initialization
2. Send codewords
3. Coalition produces some forgery $\vec{y}$
4. Intercept forgery
5. Accuse certain users

Advantages:

- Many applications
- Only one codeword

Disadvantages:

- Catch only one or few colluders



# Model: Dynamic schemes

Construction:

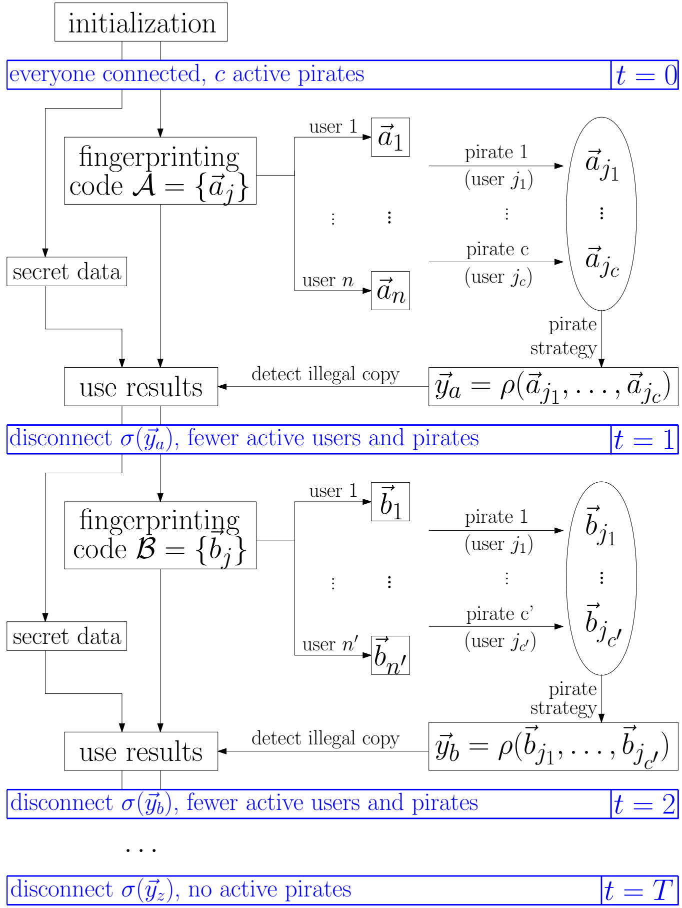
1. Initialization
2. Send first codewords
3. Receive first forgery
4. Disconnect certain users
5. Send new codewords
6. (repeat until no forgeries appear)

Advantages:

- Less total data needed.
- Catch all colluders.

Disadvantages:

- Fewer applications.
- Computations required during the broadcast.



# Model: Deterministic vs. probabilistic

Deterministic schemes: No error.

- Always absolute certainty.
- Soundness: Never accuse any innocent users.
- Completeness: Always accuse at least one guilty user.
- Always alphabet size $q \geq c + 1$.
- Works only in restricted digit model.

Probabilistic schemes: Errors bounded by $\epsilon_1, \epsilon_2 > 0$.

- Small probability of error.
- Soundness: Accuse no innocent users with probability at least $1 - \epsilon_1$.
- Completeness: Accuse a guilty user with probability at least $1 - \epsilon_2$.
- Usually soundness is more important: $\epsilon_1 \ll \epsilon_2$.
- Alphabet size $q \geq 2$.
- Works against any attack model.

# Previous results: All schemes

First half of the project and report: Extensive literature study.

| | $q$ (alphabet size) | $\ell, t$ (codelength,time) |
|---|---|---|
| Deterministic, static | $q \geq c+1$ | $\ell \geq \Omega(c^2 \log(n))$ |
| - Staddon et al. | $q = \mathcal{O}(c^2 k)$ | $\ell = \mathcal{O}(c^2 \log(n))$ |
| - Alon et al. | $q = c+1$ | $\ell = \mathcal{O}(c^2 \log(n))$ |
| Probabilistic, static | $q \geq 2$ | $\ell \geq \Omega(c^2 \ln(n/\epsilon))$ |
| - Boneh and Shaw | $q = 2$ | $\ell = \mathcal{O}(n^3 \ln(n/\epsilon))$ |
| - Boneh and Shaw | $q = 2$ | $\ell = \mathcal{O}(c^4 \ln(n/\epsilon) \ln(c/\epsilon))$ |
| - Tardos | $q = 2$ | $\ell = \mathcal{O}(c^2 \ln(n/\epsilon))$ |
| Deterministic, dynamic | $q \geq c+1$ | $t \geq \Omega(\frac{c^2}{q-c} + c \log(n))$ |
| - Fiat and Tassa | $q = 2c+1$ | $t = \mathcal{O}(c \log(n))$ |
| - Berkman et al. | $q = c+1$ | $t = \mathcal{O}(c^3 \log(n))$ |
| - Berkman et al. | $q = c+1$ | $t = \mathcal{O}(c^2 + c \log(n))$ |
| Probabilistic, dynamic | $q \geq 2$ | ? |
| - Tassa | $q = 2$ | $\ell \cdot t = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon))$ |

# Previous results: Probabilistic schemes

| (probabilistic, $q = 2$) | $\ell$ (for small $c$) | $\ell$ (for large $c$) |
|---|---|---|
| Static schemes | $\ell \geq \Omega(c^2 \ln(n/\epsilon))$ | $\ell \geq 1.38c^2 \ln(n/\epsilon)$ |
| - Boneh and Shaw | $\ell \approx 2n^3 \ln(n/\epsilon)$ | $\ell \approx 2n^3 \ln(n/\epsilon)$ |
| - Boneh and Shaw | $\ell \approx 32c^4 \ln(n/\epsilon) \ln(c/\epsilon)$ | $\ell \approx 32c^4 \ln(n/\epsilon) \ln(c/\epsilon)$ |
| - Tardos | $\ell = 100c^2 \ln(n/\epsilon)$ | $\ell = 100c^2 \ln(n/\epsilon)$ |
| - Vladimirova et al. | $\ell = 90c^2 \ln(n/\epsilon)$ | $\ell \approx 39.48c^2 \ln(n/\epsilon)$ |
| - Blayer and Tassa | $\ell = 85c^2 \ln(n/\epsilon)$ | $\ell \approx 19.74c^2 \ln(n/\epsilon)$ |
| - Skoric et al. | (vague) | $\ell \approx 9.87c^2 \ln(n/\epsilon)$ |
| - Nuida et al. | $\ell \approx 5c^2 \ln(n/\epsilon)$ | $\ell \approx 5.35c^2 \ln(n/\epsilon)$ |
| Dynamic schemes | ? | ? |
| - Tassa | $\ell \cdot t = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon))$ | $\ell \cdot t = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon))$ |

# New results

| (probabilistic, $q = 2$) | $\ell$ (for small $c$) | $\ell$ (for large $c$) |
|---|---|---|
| Static schemes | $\ell \geq \Omega(c^2 \ln(n/\epsilon))$ | $\ell \geq 1.38c^2 \ln(n/\epsilon)$ |
| - Boneh and Shaw | $\ell \approx 2n^3 \ln(n/\epsilon)$ | $\ell \approx 2n^3 \ln(n/\epsilon)$ |
| - Boneh and Shaw | $\ell \approx 32c^4 \ln(n/\epsilon) \ln(c/\epsilon)$ | $\ell \approx 32c^4 \ln(n/\epsilon) \ln(c/\epsilon)$ |
| - Tardos | $\ell = 100c^2 \ln(n/\epsilon)$ | $\ell = 100c^2 \ln(n/\epsilon)$ |
| - Vladimirova et al. | $\ell = 90c^2 \ln(n/\epsilon)$ | $\ell \approx 39.48c^2 \ln(n/\epsilon)$ |
| - Blayer and Tassa | $\ell = 85c^2 \ln(n/\epsilon)$ | $\ell \approx 19.74c^2 \ln(n/\epsilon)$ |
| - Skoric et al. | (vague) | $\ell \approx 9.87c^2 \ln(n/\epsilon)$ |
| - Nuida et al. | $\ell \approx 5c^2 \ln(n/\epsilon)$ | $\ell \approx 5.35c^2 \ln(n/\epsilon)$ |
| **- Laarhoven (1)** | $\ell \approx \mathbf{24}c^2 \ln(n/\epsilon)$ | $\ell \approx \mathbf{4.93}c^2 \ln(n/\epsilon)$ |
| Dynamic schemes | ? | ? |
| - Tassa | $\ell \cdot t = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon))$ | $\ell \cdot t = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon))$ |
| **- Laarhoven (2)** | $\ell \cdot t \approx \mathbf{26}c^2 \ln(n/\epsilon)$ | $\ell \cdot t \approx \mathbf{4.93}c^2 \ln(n/\epsilon)$ |
| **- Laarhoven (3)** | $\ell \cdot t \approx \mathbf{26}c^2 \ln(nc^2/\epsilon)$ | $\ell \cdot t \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon)$ |
| **- Laarhoven (4)** | $\ell \cdot t \approx \mathbf{26}c^2 \ln(nc^2/\epsilon)$ | $\ell \cdot t \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon)$ |

# The Tardos scheme: Outline

Initialization:

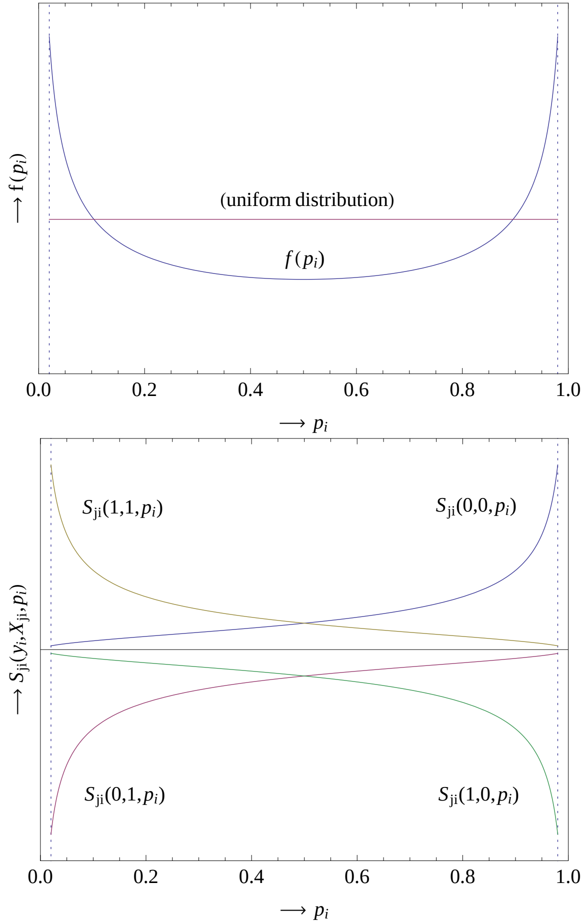
- Take $\ell = \mathcal{O}(c^2 \ln(n/\epsilon_1))$.
- Take $\delta = \mathcal{O}(c^{-4/3})$.
- Take $Z = \mathcal{O}(c \ln(n/\epsilon_1))$.

Codeword generation:

- Generate $p_i \in [\delta, 1-\delta]$ from $f(p)$.
- Generate $X_{ji}$ using $\mathbb{P}[X_{ji} = 1] = p_i$.

Accusation: (after intercepting $\vec{y}$)

- Calculate $S_{ji} = S_{ji}(y_i, X_{ji}, p_i)$.
- Calculate $S_j = \sum_{i=1}^{\ell} S_{ji}$.
- Accuse user $j$ if $S_j > Z$.



# The Tardos scheme: Example

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $\dots$ | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | $X_{1,1}$ | $X_{1,2}$ | $X_{1,3}$ | $X_{1,4}$ | $X_{1,5}$ | $X_{1,6}$ | $\dots$ | $X_{1,1208}$ |
| Bob | $X_{2,1}$ | $X_{2,2}$ | $X_{2,3}$ | $X_{2,4}$ | $X_{2,5}$ | $X_{2,6}$ | $\dots$ | $X_{2,1208}$ |
| Charlie | $X_{3,1}$ | $X_{3,2}$ | $X_{3,3}$ | $X_{3,4}$ | $X_{3,5}$ | $X_{3,6}$ | $\dots$ | $X_{3,1208}$ |
| Dave | $X_{4,1}$ | $X_{4,2}$ | $X_{4,3}$ | $X_{4,4}$ | $X_{4,5}$ | $X_{4,6}$ | $\dots$ | $X_{4,1208}$ |
| Eve | $X_{5,1}$ | $X_{5,2}$ | $X_{5,3}$ | $X_{5,4}$ | $X_{5,5}$ | $X_{5,6}$ | $\dots$ | $X_{5,1208}$ |
| Fred | $X_{6,1}$ | $X_{6,2}$ | $X_{6,3}$ | $X_{6,4}$ | $X_{6,5}$ | $X_{6,6}$ | $\dots$ | $X_{6,1208}$ |
| George | $X_{7,1}$ | $X_{7,2}$ | $X_{7,3}$ | $X_{7,4}$ | $X_{7,5}$ | $X_{7,6}$ | $\dots$ | $X_{7,1208}$ |
| Henry | $X_{8,1}$ | $X_{8,2}$ | $X_{8,3}$ | $X_{8,4}$ | $X_{8,5}$ | $X_{8,6}$ | $\dots$ | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $\dots$ | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | $X_{1,2}$ | $X_{1,3}$ | $X_{1,4}$ | $X_{1,5}$ | $X_{1,6}$ | $\dots$ | $X_{1,1208}$ |
| Bob | 1 | $X_{2,2}$ | $X_{2,3}$ | $X_{2,4}$ | $X_{2,5}$ | $X_{2,6}$ | $\dots$ | $X_{2,1208}$ |
| Charlie | 1 | $X_{3,2}$ | $X_{3,3}$ | $X_{3,4}$ | $X_{3,5}$ | $X_{3,6}$ | $\dots$ | $X_{3,1208}$ |
| Dave | 0 | $X_{4,2}$ | $X_{4,3}$ | $X_{4,4}$ | $X_{4,5}$ | $X_{4,6}$ | $\dots$ | $X_{4,1208}$ |
| Eve | 0 | $X_{5,2}$ | $X_{5,3}$ | $X_{5,4}$ | $X_{5,5}$ | $X_{5,6}$ | $\dots$ | $X_{5,1208}$ |
| Fred | 1 | $X_{6,2}$ | $X_{6,3}$ | $X_{6,4}$ | $X_{6,5}$ | $X_{6,6}$ | $\dots$ | $X_{6,1208}$ |
| George | 0 | $X_{7,2}$ | $X_{7,3}$ | $X_{7,4}$ | $X_{7,5}$ | $X_{7,6}$ | $\dots$ | $X_{7,1208}$ |
| Henry | 0 | $X_{8,2}$ | $X_{8,3}$ | $X_{8,4}$ | $X_{8,5}$ | $X_{8,6}$ | $\dots$ | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $\dots$ | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | $X_{1,3}$ | $X_{1,4}$ | $X_{1,5}$ | $X_{1,6}$ | $\dots$ | $X_{1,1208}$ |
| Bob | 1 | 0 | $X_{2,3}$ | $X_{2,4}$ | $X_{2,5}$ | $X_{2,6}$ | $\dots$ | $X_{2,1208}$ |
| Charlie | 1 | 0 | $X_{3,3}$ | $X_{3,4}$ | $X_{3,5}$ | $X_{3,6}$ | $\dots$ | $X_{3,1208}$ |
| Dave | 0 | 0 | $X_{4,3}$ | $X_{4,4}$ | $X_{4,5}$ | $X_{4,6}$ | $\dots$ | $X_{4,1208}$ |
| Eve | 0 | 0 | $X_{5,3}$ | $X_{5,4}$ | $X_{5,5}$ | $X_{5,6}$ | $\dots$ | $X_{5,1208}$ |
| Fred | 1 | 0 | $X_{6,3}$ | $X_{6,4}$ | $X_{6,5}$ | $X_{6,6}$ | $\dots$ | $X_{6,1208}$ |
| George | 0 | 0 | $X_{7,3}$ | $X_{7,4}$ | $X_{7,5}$ | $X_{7,6}$ | $\dots$ | $X_{7,1208}$ |
| Henry | 0 | 0 | $X_{8,3}$ | $X_{8,4}$ | $X_{8,5}$ | $X_{8,6}$ | $\dots$ | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | 0.88 | $p_4$ | $p_5$ | $p_6$ | $\dots$ | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | $X_{1,4}$ | $X_{1,5}$ | $X_{1,6}$ | $\dots$ | $X_{1,1208}$ |
| Bob | 1 | 0 | 1 | $X_{2,4}$ | $X_{2,5}$ | $X_{2,6}$ | $\dots$ | $X_{2,1208}$ |
| Charlie | 1 | 0 | 0 | $X_{3,4}$ | $X_{3,5}$ | $X_{3,6}$ | $\dots$ | $X_{3,1208}$ |
| Dave | 0 | 0 | 1 | $X_{4,4}$ | $X_{4,5}$ | $X_{4,6}$ | $\dots$ | $X_{4,1208}$ |
| Eve | 0 | 0 | 1 | $X_{5,4}$ | $X_{5,5}$ | $X_{5,6}$ | $\dots$ | $X_{5,1208}$ |
| Fred | 1 | 0 | 1 | $X_{6,4}$ | $X_{6,5}$ | $X_{6,6}$ | $\dots$ | $X_{6,1208}$ |
| George | 0 | 0 | 1 | $X_{7,4}$ | $X_{7,5}$ | $X_{7,6}$ | $\dots$ | $X_{7,1208}$ |
| Henry | 0 | 0 | 0 | $X_{8,4}$ | $X_{8,5}$ | $X_{8,6}$ | $\dots$ | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | $p_5$ | $p_6$ | $\dots$ | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | $X_{1,5}$ | $X_{1,6}$ | $\dots$ | $X_{1,1208}$ |
| Bob | 1 | 0 | 1 | 1 | $X_{2,5}$ | $X_{2,6}$ | $\dots$ | $X_{2,1208}$ |
| Charlie | 1 | 0 | 0 | 1 | $X_{3,5}$ | $X_{3,6}$ | $\dots$ | $X_{3,1208}$ |
| Dave | 0 | 0 | 1 | 1 | $X_{4,5}$ | $X_{4,6}$ | $\dots$ | $X_{4,1208}$ |
| Eve | 0 | 0 | 1 | 0 | $X_{5,5}$ | $X_{5,6}$ | $\dots$ | $X_{5,1208}$ |
| Fred | 1 | 0 | 1 | 0 | $X_{6,5}$ | $X_{6,6}$ | $\dots$ | $X_{6,1208}$ |
| George | 0 | 0 | 1 | 0 | $X_{7,5}$ | $X_{7,6}$ | $\dots$ | $X_{7,1208}$ |
| Henry | 0 | 0 | 0 | 1 | $X_{8,5}$ | $X_{8,6}$ | $\dots$ | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | $p_6$ | ... | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | $X_{1,6}$ | ... | $X_{1,1208}$ |
| Bob | 1 | 0 | 1 | 1 | 1 | $X_{2,6}$ | ... | $X_{2,1208}$ |
| Charlie | 1 | 0 | 0 | 1 | 0 | $X_{3,6}$ | ... | $X_{3,1208}$ |
| Dave | 0 | 0 | 1 | 1 | 1 | $X_{4,6}$ | ... | $X_{4,1208}$ |
| Eve | 0 | 0 | 1 | 0 | 1 | $X_{5,6}$ | ... | $X_{5,1208}$ |
| Fred | 1 | 0 | 1 | 0 | 1 | $X_{6,6}$ | ... | $X_{6,1208}$ |
| George | 0 | 0 | 1 | 0 | 1 | $X_{7,6}$ | ... | $X_{7,1208}$ |
| Henry | 0 | 0 | 0 | 1 | 1 | $X_{8,6}$ | ... | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | $p_\ell$ |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | $X_{1,1208}$ |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | $X_{2,1208}$ |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | $X_{3,1208}$ |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | $X_{4,1208}$ |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | $X_{5,1208}$ |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | $X_{6,1208}$ |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | $X_{7,1208}$ |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | $X_{8,1208}$ |

# The Tardos scheme: Codewords

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $X_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | | | | | | | | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | | | | | | | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | | | | | | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | 0 | | | | | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | 0 | 1 | | | | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | 0 | 1 | 1 | | | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Coalition

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $y_i$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 |
|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 | 0 |
| Bob | 1 | 0 | 1 | 1 | 1 | 0 | ... | 0 | 0 |
| Charlie | 1 | 0 | 0 | 1 | 0 | 1 | ... | 0 | 0 |
| Dave | 0 | 0 | 1 | 1 | 1 | 0 | ... | 0 | 0 |
| Eve | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 | 0 |
| Fred | 1 | 0 | 1 | 0 | 1 | 1 | ... | 0 | 0 |
| George | 0 | 0 | 1 | 0 | 1 | 0 | ... | 0 | 0 |
| Henry | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | 0 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | 0 | 1 | 1 | 1 | 0 | ... | 0 | +0.5 |
| Bob | −2.0 | 0 | 1 | 1 | 1 | 0 | ... | 0 | −2.0 |
| Charlie | −2.0 | 0 | 0 | 1 | 0 | 1 | ... | 0 | −2.0 |
| Dave | +0.5 | 0 | 1 | 1 | 1 | 0 | ... | 0 | +0.5 |
| Eve | +0.5 | 0 | 1 | 0 | 1 | 0 | ... | 0 | +0.5 |
| Fred | −2.0 | 0 | 1 | 0 | 1 | 1 | ... | 0 | −2.0 |
| George | +0.5 | 0 | 1 | 0 | 1 | 0 | ... | 0 | +0.5 |
| Henry | +0.5 | 0 | 0 | 1 | 1 | 0 | ... | 0 | +0.5 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | +0.2 | 1 | 1 | 1 | 0 | ... | 0 | +0.7 |
| Bob | −2.0 | +0.2 | 1 | 1 | 1 | 0 | ... | 0 | −1.8 |
| Charlie | −2.0 | +0.2 | 0 | 1 | 0 | 1 | ... | 0 | −1.8 |
| Dave | +0.5 | +0.2 | 1 | 1 | 1 | 0 | ... | 0 | +0.7 |
| Eve | +0.5 | +0.2 | 1 | 0 | 1 | 0 | ... | 0 | +0.7 |
| Fred | −2.0 | +0.2 | 1 | 0 | 1 | 1 | ... | 0 | −1.8 |
| George | +0.5 | +0.2 | 1 | 0 | 1 | 0 | ... | 0 | +0.7 |
| Henry | +0.5 | +0.2 | 0 | 1 | 1 | 0 | ... | 0 | +0.7 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | $\ldots$ | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | $+0.5$ | $+0.2$ | $-0.4$ | 1 | 1 | 0 | $\ldots$ | 0 | $+0.4$ |
| Bob | $-2.0$ | $+0.2$ | $-0.4$ | 1 | 1 | 0 | $\ldots$ | 0 | $-2.1$ |
| Charlie | $-2.0$ | $+0.2$ | $+2.7$ | 1 | 0 | 1 | $\ldots$ | 0 | $+1.0$ |
| Dave | $+0.5$ | $+0.2$ | $-0.4$ | 1 | 1 | 0 | $\ldots$ | 0 | $+0.4$ |
| Eve | $+0.5$ | $+0.2$ | $-0.4$ | 0 | 1 | 0 | $\ldots$ | 0 | $+0.4$ |
| Fred | $-2.0$ | $+0.2$ | $-0.4$ | 0 | 1 | 1 | $\ldots$ | 0 | $-2.1$ |
| George | $+0.5$ | $+0.2$ | $-0.4$ | 0 | 1 | 0 | $\ldots$ | 0 | $+0.4$ |
| Henry | $+0.5$ | $+0.2$ | $+2.7$ | 1 | 1 | 0 | $\ldots$ | 0 | $+3.5$ |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | $\ldots$ | 0 | |

$$C = \{\text{Charlie}, \text{Eve}, \text{Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | +0.2 | −0.4 | +0.5 | 1 | 0 | ... | 0 | +0.9 |
| Bob | −2.0 | +0.2 | −0.4 | +0.5 | 1 | 0 | ... | 0 | −1.6 |
| Charlie | −2.0 | +0.2 | +2.7 | +0.5 | 0 | 1 | ... | 0 | +1.5 |
| Dave | +0.5 | +0.2 | −0.4 | +0.5 | 1 | 0 | ... | 0 | +0.9 |
| Eve | +0.5 | +0.2 | −0.4 | −1.9 | 1 | 0 | ... | 0 | −1.6 |
| Fred | −2.0 | +0.2 | −0.4 | −1.9 | 1 | 1 | ... | 0 | −4.1 |
| George | +0.5 | +0.2 | −0.4 | −1.9 | 1 | 0 | ... | 0 | −1.6 |
| Henry | +0.5 | +0.2 | +2.7 | +0.5 | 1 | 0 | ... | 0 | +4.0 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | 0 | ... | 0 | +1.0 |
| Bob | −2.0 | +0.2 | −0.4 | +0.5 | +0.1 | 0 | ... | 0 | −1.5 |
| Charlie | −2.0 | +0.2 | +2.7 | +0.5 | −7.2 | 1 | ... | 0 | −5.7 |
| Dave | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | 0 | ... | 0 | +1.0 |
| Eve | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | 0 | ... | 0 | −1.4 |
| Fred | −2.0 | +0.2 | −0.4 | −1.9 | +0.1 | 1 | ... | 0 | −3.9 |
| George | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | 0 | ... | 0 | −1.4 |
| Henry | +0.5 | +0.2 | +2.7 | +0.5 | +0.1 | 0 | ... | 0 | +4.1 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | $+0.5$ | $+0.2$ | $-0.4$ | $+0.5$ | $+0.1$ | $+0.3$ | ... | 0 | $+1.3$ |
| Bob | $-2.0$ | $+0.2$ | $-0.4$ | $+0.5$ | $+0.1$ | $+0.3$ | ... | 0 | $-1.2$ |
| Charlie | $-2.0$ | $+0.2$ | $+2.7$ | $+0.5$ | $-7.2$ | $-3.3$ | ... | 0 | $-9.0$ |
| Dave | $+0.5$ | $+0.2$ | $-0.4$ | $+0.5$ | $+0.1$ | $+0.3$ | ... | 0 | $+1.3$ |
| Eve | $+0.5$ | $+0.2$ | $-0.4$ | $-1.9$ | $+0.1$ | $+0.3$ | ... | 0 | $-1.1$ |
| Fred | $-2.0$ | $+0.2$ | $-0.4$ | $-1.9$ | $+0.1$ | $-3.3$ | ... | 0 | $-7.2$ |
| George | $+0.5$ | $+0.2$ | $-0.4$ | $-1.9$ | $+0.1$ | $+0.3$ | ... | 0 | $-1.1$ |
| Henry | $+0.5$ | $+0.2$ | $+2.7$ | $+0.5$ | $+0.1$ | $+0.3$ | ... | 0 | $+4.4$ |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Scores

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +14 |
| Bob | −2.0 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | −19 |
| Charlie | −2.0 | +0.2 | +2.7 | +0.5 | −7.2 | −3.3 | ... | +0.5 | +291 |
| Dave | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +29 |
| Eve | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | +0.3 | ... | +0.5 | +292 |
| Fred | −2.0 | +0.2 | −0.4 | −1.9 | +0.1 | −3.3 | ... | +0.5 | −53 |
| George | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | +0.3 | ... | +0.5 | −42 |
| Henry | +0.5 | +0.2 | +2.7 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +269 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

# The Tardos scheme: Accusation

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

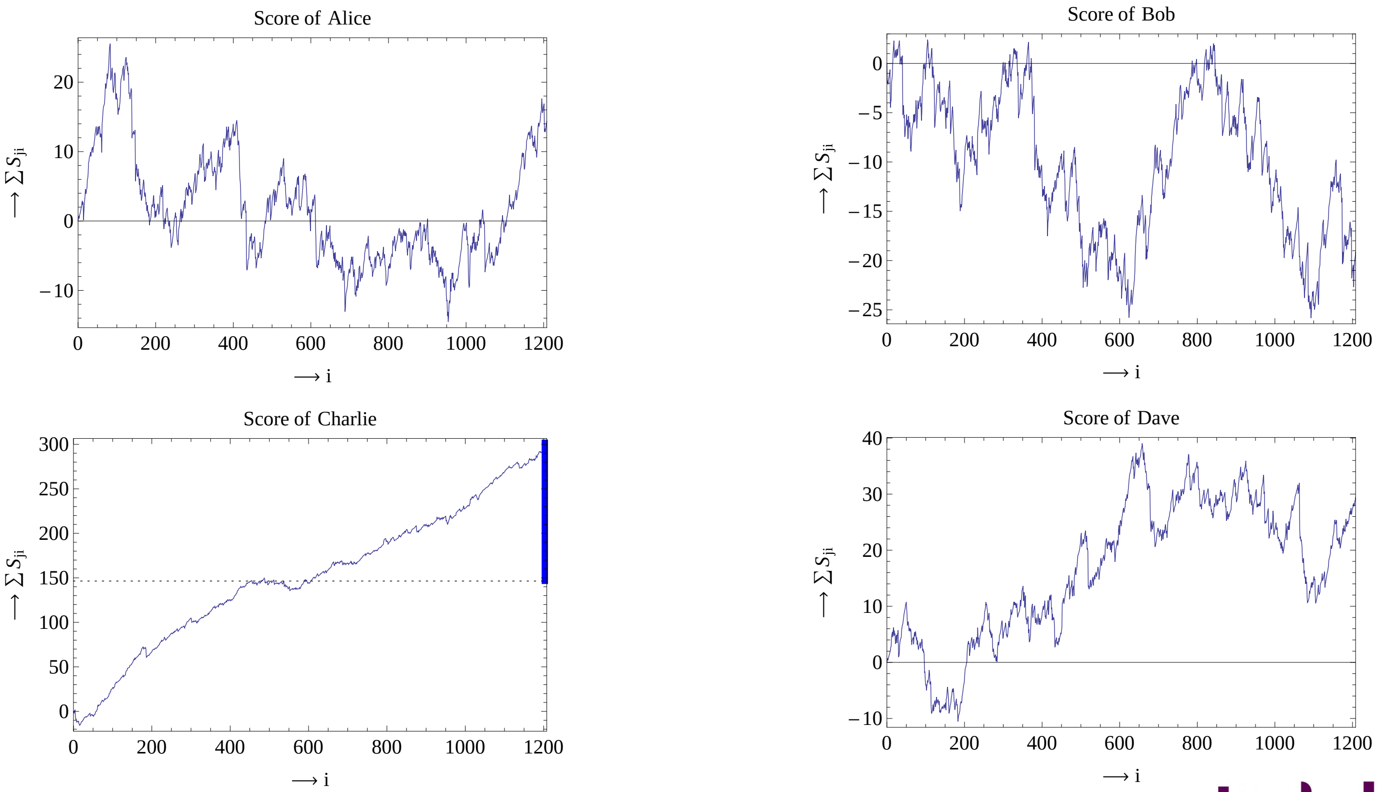
| $S_{j,i}$ | 0.20 | 0.05 | 0.88 | 0.79 | 0.98 | 0.09 | ... | 0.18 | $\sum S_{j,i}$ |
|---|---|---|---|---|---|---|---|---|---|
| Alice | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +14 |
| Bob | −2.0 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | −19 |
| Charlie | −2.0 | +0.2 | +2.7 | +0.5 | −7.2 | −3.3 | ... | +0.5 | +291 |
| Dave | +0.5 | +0.2 | −0.4 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +29 |
| Eve | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | +0.3 | ... | +0.5 | +292 |
| Fred | −2.0 | +0.2 | −0.4 | −1.9 | +0.1 | −3.3 | ... | +0.5 | −53 |
| George | +0.5 | +0.2 | −0.4 | −1.9 | +0.1 | +0.3 | ... | +0.5 | −42 |
| Henry | +0.5 | +0.2 | +2.7 | +0.5 | +0.1 | +0.3 | ... | +0.5 | +269 |
| Forgery | 0 | 0 | 0 | 1 | 1 | 0 | ... | 0 | |

$$C = \{\text{Charlie, Eve, Henry}\}$$

$$\sigma(\vec{y}) = \{\text{Charlie, Eve, Henry}\}$$

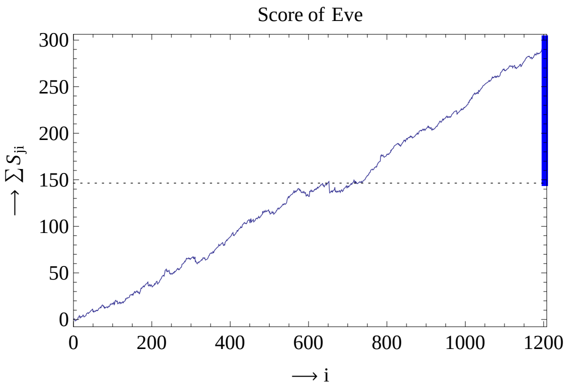
# The Tardos scheme: Accusation

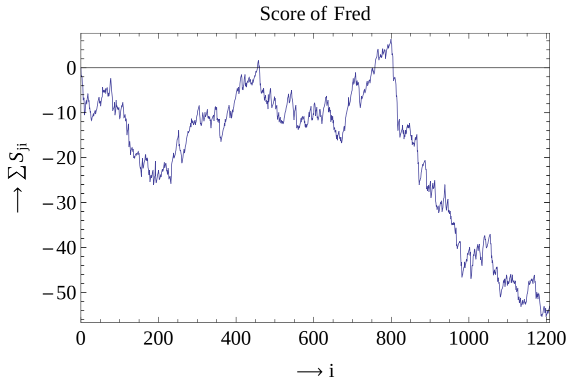
Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.

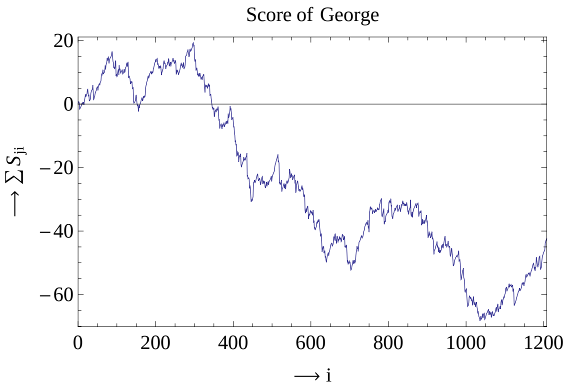


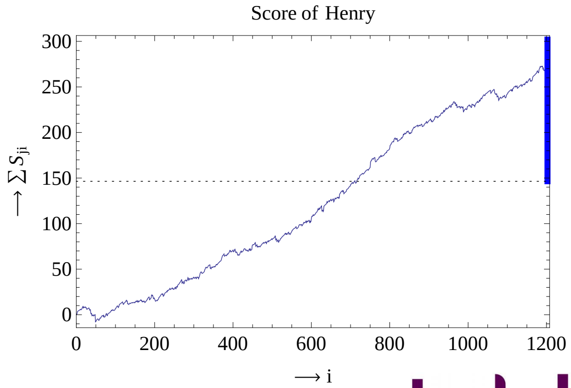
# The Tardos scheme: Accusation

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.



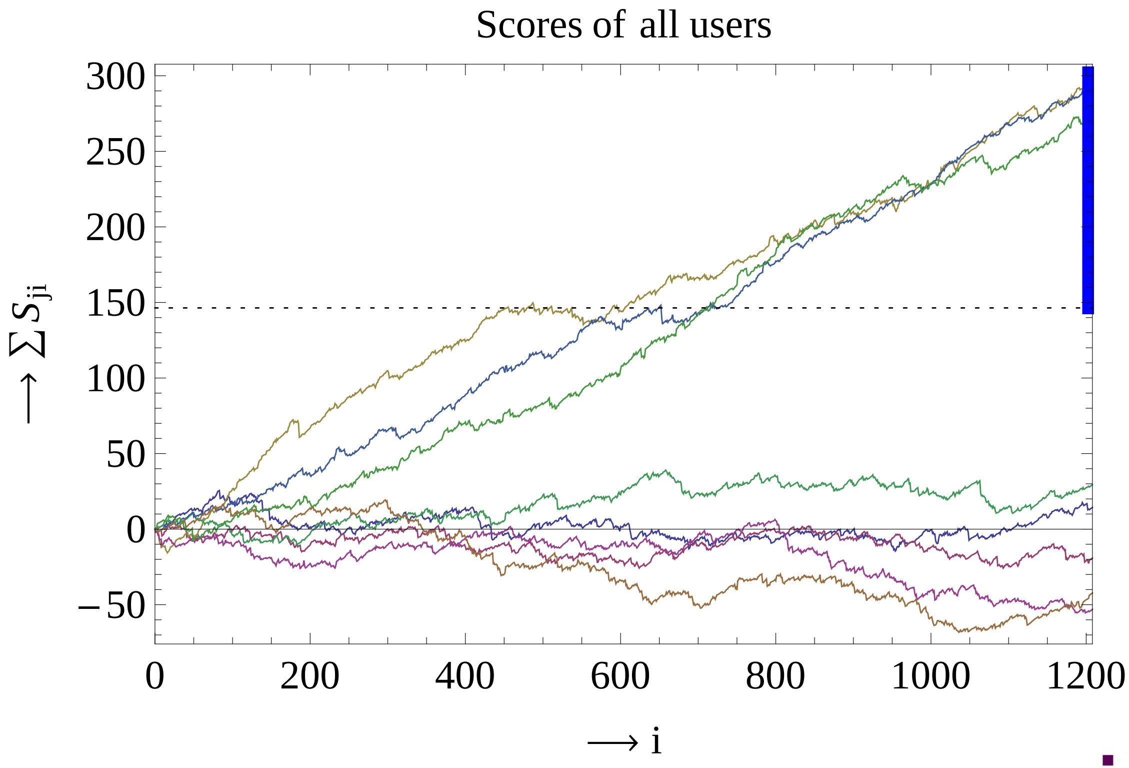



# The Tardos scheme: Accusation

Let $n = 8$, let $c = 3$ and let the error probabilities be given by $\epsilon_1 = \epsilon_2 = 0.01$. From the initialization we get $\ell = 1208$, $Z = 146.4$, $\delta = 0.0115$ and $f(p) = 0.368811 \cdot p^{-1/2}(1-p)^{-1/2}$.



# The Tardos scheme: Why does it work?

Why are no innocent users accused?

- All codewords are independent, so it is impossible to frame anyone.
- The probability that a random walk exceeds $Z$ is sufficiently small.

Why are guilty users accused?

- On undetectable positions, $S = \sum_{j \in C} S_j$ increases a lot.
- On other positions, pirates cannot decrease $S$ by a lot. (Even if $p_i$ is known!)
- If $S > cZ$ then at least one user is accused.

Note: Never guarantee of catching multiple colluders!

# The Tardos scheme: Improvements

Suggested improvements:

- Use a symmetric accusation function. (Škorić et al.)
- Tighten the analysis in the proofs. (Škorić et al., Blayer and Tassa)
- Use the Gaussian approximation to estimate error probabilities. (Simone and Škorić)
- Use an optimal discrete distribution function $f(p)$. (Nuida et al.)

With the last optimization, one can achieve $\ell \approx 5.35c^2 \ln(n/\epsilon_1)$ for large $c$.

# The improved Tardos scheme: Intro

Combine earlier improvements:

- Use a symmetric accusation function. (Škorić et al.)
- Tighten the analysis in the proofs. (Škorić et al., Blayer and Tassa)

Basically: Apply analysis of Blayer and Tassa to improved scheme of Škorić et al.

# The improved Tardos scheme: Intro

Original Tardos scheme: No parametrization:

- Constant 100: $\ell = 100c^2 \ln(n/\epsilon_1)$
- Constant 20: $Z = 20c \ln(n/\epsilon_1)$
- Constant 300: $\delta = 1/(300c)$
- Constant $c/4$: $\epsilon_2 = (\epsilon_1/n)^{c/4}$

Proof of soundness:

- Constant 10: $\alpha = 1/(10c)$
- Constant 1.7: $\alpha/\sqrt{\delta} \leq 1.7$

Proof of completeness:

- Constant 1: $\beta = 1\sqrt{\delta}/c$
- Constant 0.25: $\frac{1-2c\delta}{\pi-4\delta'} + \beta c \geq 0.25$

# The improved Tardos scheme: B&T

Blayer and Tassa's improvement: Full parametrization:

- Introduce $d_\ell$: $\ell = d_\ell c^2 \ln(n/\epsilon_1)$
- Introduce $d_z$: $Z = d_z c \ln(n/\epsilon_1)$
- Introduce $d_\delta$: $\delta = 1/(d_\delta c)$
- Introduce $\eta$: $\epsilon_2 = (\epsilon_1/n)^\eta$

Proof of soundness:

- Introduce $d_\alpha$: $\alpha = 1/(d_\alpha c)$
- Introduce $r$: $\alpha/\sqrt{\delta} \leq h(r)$ (where $h^{-1}(x) = (e^x - 1 - x)/x^2$)

Proof of completeness:

- Introduce $s$: $\beta = s\sqrt{\delta}/c$
- Introduce $g$: $\frac{1-2c\delta}{\pi-4\delta'} + h^{-1}(s)\beta c \geq g$

# The improved Tardos scheme: B&T

**Theorem (Blayer and Tassa)**

For $c \geq 2$ and $\epsilon_2 \geq \epsilon_1/n$ one can prove secureness with scheme parameters:

$$\ell = 81.25c^2 \ln(n/\epsilon_1), \quad Z = 14.15c \ln(n/\epsilon_1), \quad \delta = 1/(39.19c).$$

**Theorem (Blayer and Tassa)**

For large $c$ one can prove soundness and completeness with scheme parameters:

$$\ell \approx 2\pi^2 c^2 \ln(n/\epsilon_1), \quad Z \approx 2\pi c \ln(n/\epsilon_1), \quad \delta \approx 0.$$

**Theorem (Škorić et al.)**

For large $c$ one can prove soundness and completeness with scheme parameters:

$$\ell \approx \pi^2 c^2 \ln(n/\epsilon_1), \quad Z \approx 2\pi c \ln(n/\epsilon_1), \quad \delta \approx 0.$$

# The improved Tardos scheme: Results

**Theorem (Laarhoven, ...)**

For $c \geq 2$ and $\epsilon_2 \geq \epsilon_1/n$ we can prove secureness with scheme parameters:

$$\ell = 23.79c^2 \ln(n/\epsilon_1), \quad Z = 8.06c \ln(n/\epsilon_1), \quad \delta = 1/(28.31c).$$

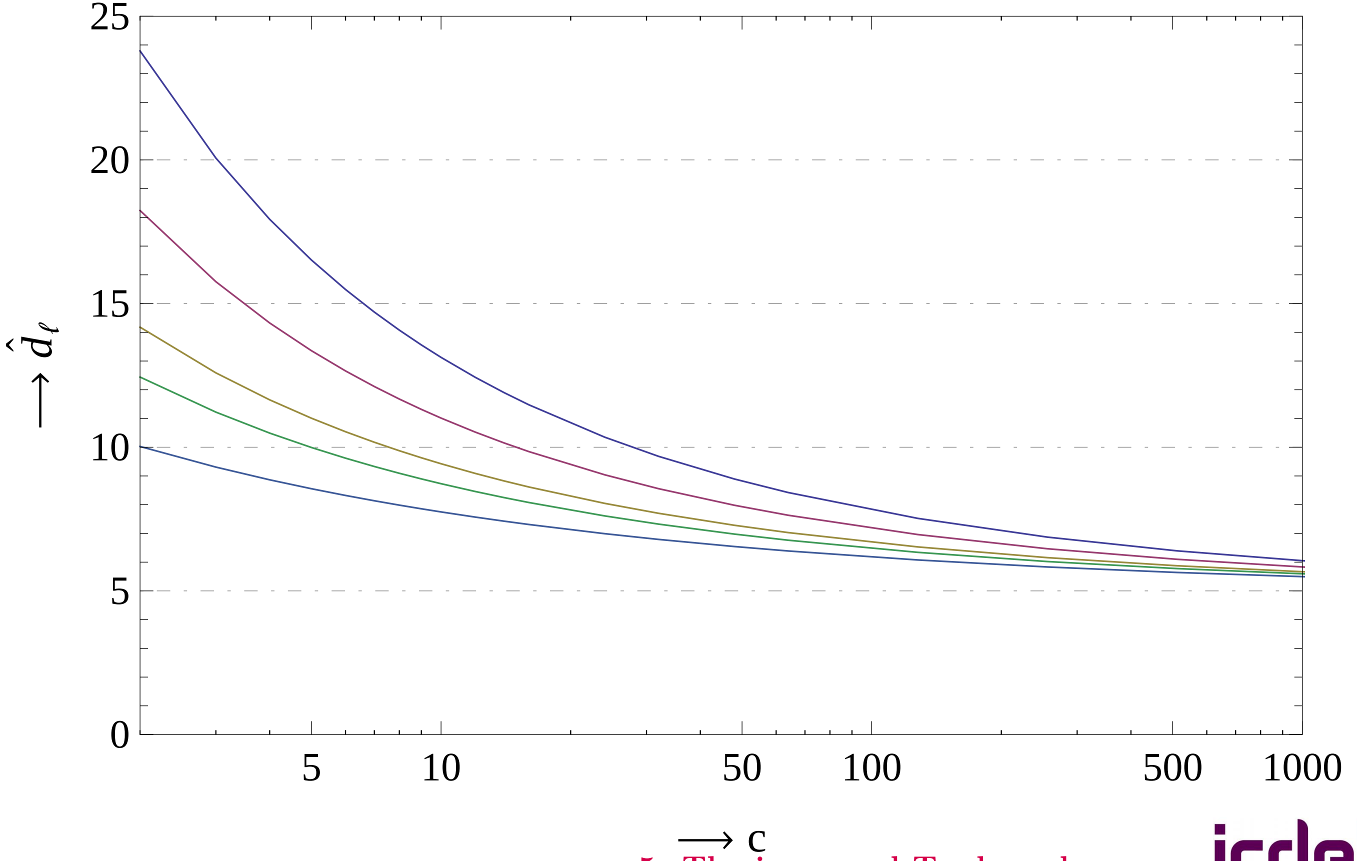
**Theorem (Laarhoven, ...)**

For large $c$ we can prove soundness and completeness with scheme parameters:

$$\ell \approx \frac{\pi^2}{2} c^2 \ln(n/\epsilon_1), \quad Z \approx \pi c \ln(n/\epsilon_1), \quad \delta \approx 0.$$

# The improved Tardos scheme: Results

Optimal codelength constant $d_\ell = \ell/(c^2 \ln(n/\epsilon_1))$, for $\epsilon_2 = \epsilon_1/n$ (top) and $\epsilon_2 \gg \epsilon_1/n$ (bottom).



# The improved Tardos scheme: Summary

Small $c$:

- Codelengths more than 3.5 times shorter than Blayer and Tassa.
- Codelengths more than 2 times shorter than Škorić et al.
- Codelengths slightly longer than Nuida et al.

Large $c$:

- Codelengths 4 times shorter than Blayer and Tassa.
- Codelengths 2 times shorter than Škorić et al.
- Codelengths 1.08 times shorter than Nuida et al.
- Codelengths asymptotically optimal for this construction.

# The dynamic Tardos scheme: Intro

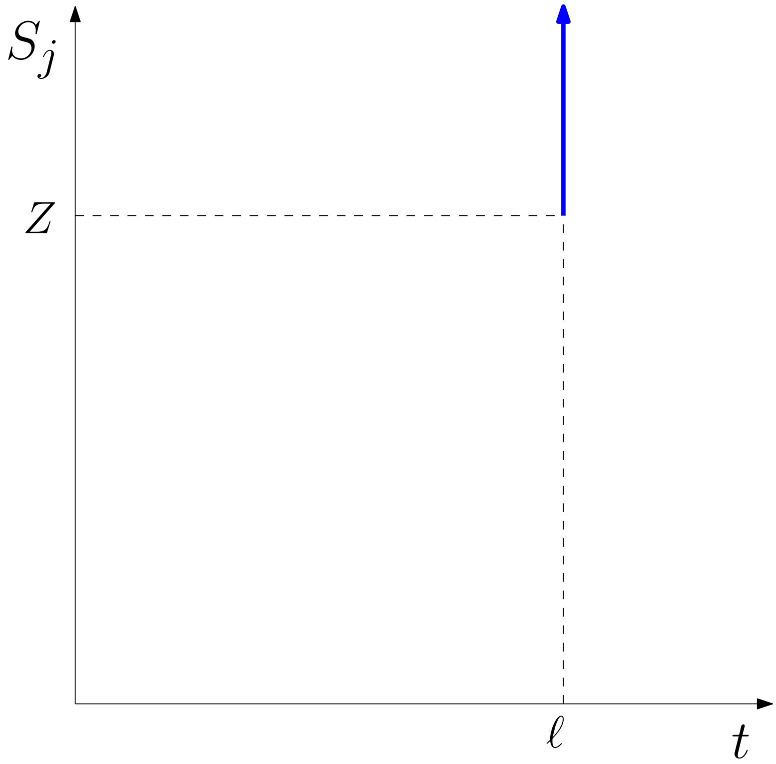
Recall: Dynamic schemes:

- Distribution of $i$th symbol may depend on $y_1, \ldots, y_{i-1}$.
- Ability to disconnect users at any time $i$.
- Possibility to catch *all* colluders.
- No good probabilistic dynamic schemes (until now...).

# The dynamic Tardos scheme: Intro

Recall: Static Tardos scheme:

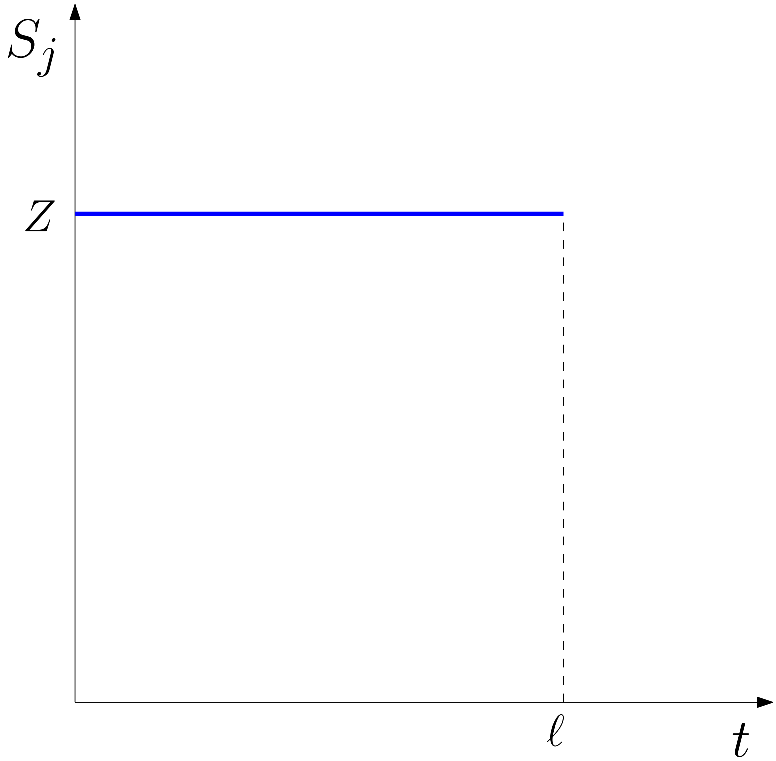
- Keep scores for each user.
- At time $\ell$, disconnect users with $S_j(\ell) = \sum_{i=1}^{\ell} S_{ji} > Z$



# The dynamic Tardos scheme: Intro

Dynamic Tardos scheme:

- Keep scores for each user.
- At each time $t$, disconnect users with $S_j(t) = \sum_{i=1}^{t} S_{ji} > Z$



# The dynamic Tardos scheme: Outline

Initialization:

- Take $\ell = \mathcal{O}(c^2 \ln(n/\epsilon_1))$.
- Take $\delta = \mathcal{O}(c^{-4/3})$.
- Take $Z = \mathcal{O}(c \ln(n/\epsilon_1))$.

Codeword generation:

- Generate $p_i \in [\delta, 1-\delta]$ from $f(p)$.
- Generate $X_{ji}$ using $\mathbb{P}[X_{ji} = 1] = p_i$.

Distribution/Accusation: For each $t = 1, \ldots, (\ell)$.

- Send $t$th symbols to active users
- Intercept $y_t$ (or terminate if no pirate output)
- Calculate $S_j(t) = \sum_{i=1}^{t} S_{ji}$.
- Disconnect user $j$ if $S_j(t) > Z$.

# The dynamic Tardos scheme: Details

Soundness:

- Error probability increases by a factor at most 2.

Completeness (here: catch all colluders):

- Error probability increases by a factor at most $2e^s$.

**Theorem (Laarhoven, ...)**
For $c \geq 2, \epsilon_2 \geq \epsilon_1/n$ and $n/\epsilon_1 \geq 10^9$ we can prove secureness with scheme parameters:

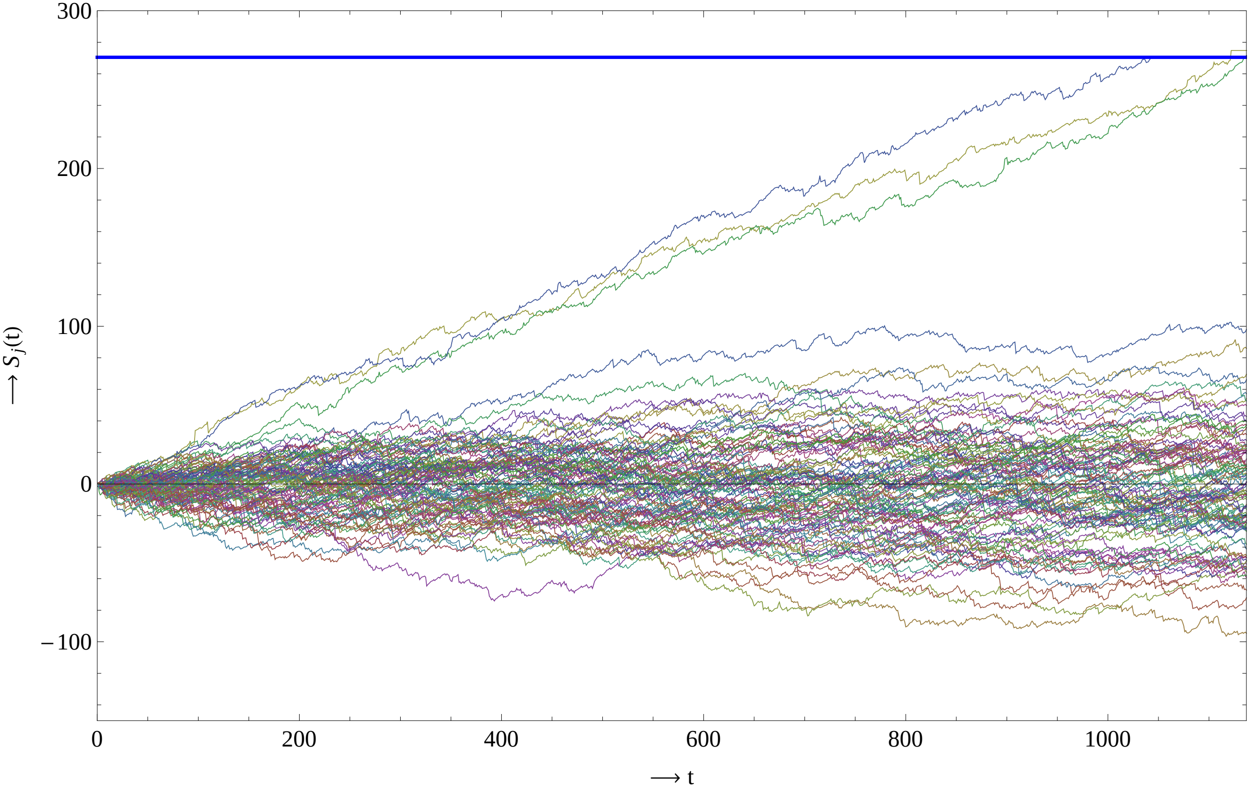
$$\ell = 25.11c^2 \ln(n/\epsilon_1), \quad Z = 8.39c \ln(n/\epsilon_1), \quad \delta = 1/(27.18c).$$

**Theorem (Laarhoven, ...)**
For $c \to \infty$ the optimal values again converge to:

$$\ell \approx \frac{\pi^2}{2} c^2 \ln(n/\epsilon_1), \quad Z \approx \pi c \ln(n/\epsilon_1), \quad \delta \approx 0.$$

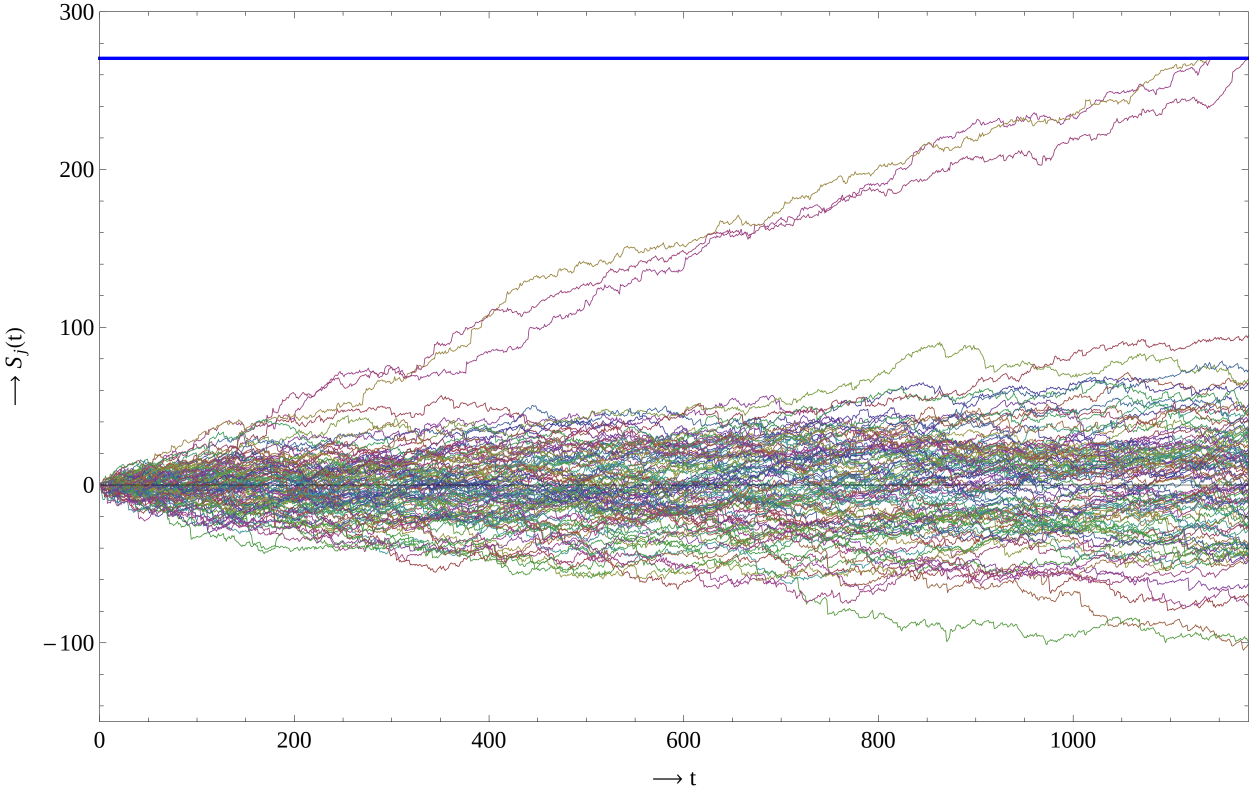
# The dynamic Tardos scheme: Example

Example: $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$ and $n = 100$. Parameters: $Z = 270.47$, $\delta = 0.0123$ and theoretically $\ell = 2285$. Strategy: Interleaving attack. Time needed: $t = 1137$.



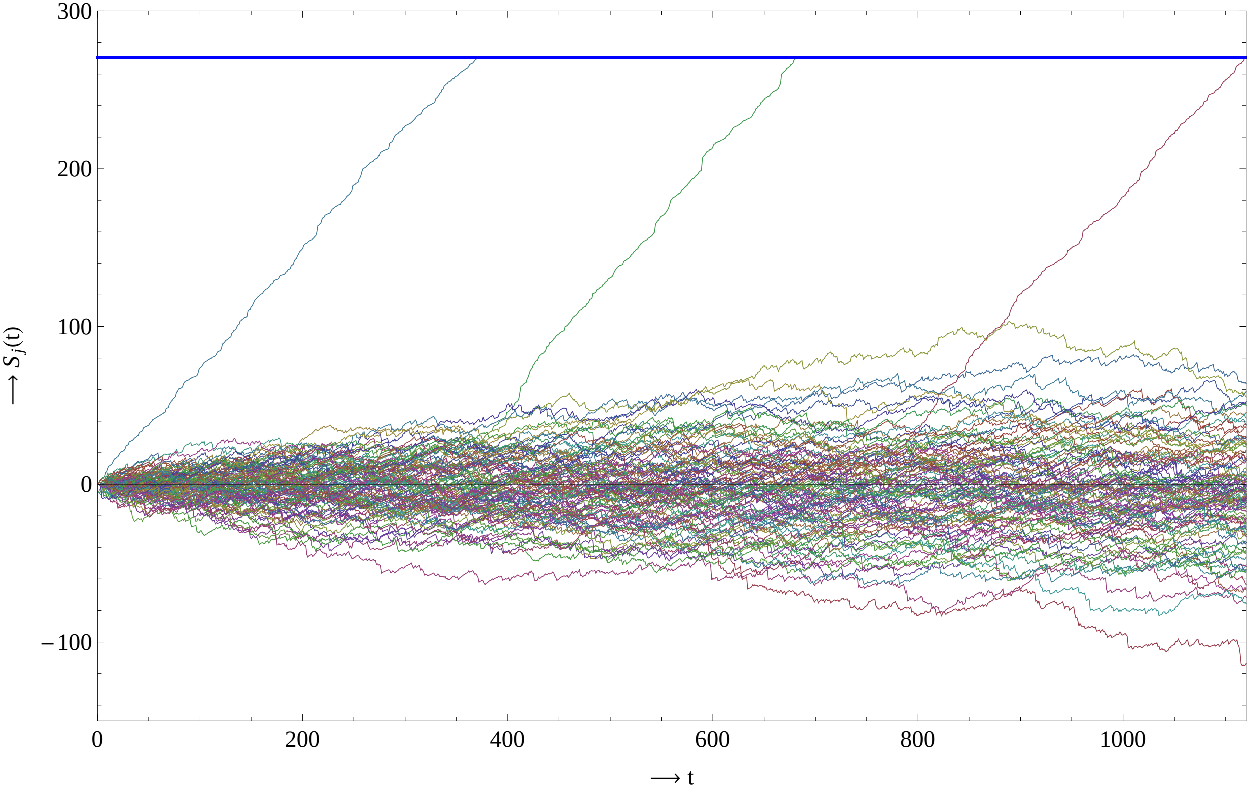
# The dynamic Tardos scheme: Example

Example: $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$ and $n = 100$. Parameters: $Z = 270.47$, $\delta = 0.0123$ and theoretically $\ell = 2285$. Strategy: Minority voting. Time needed: $t = 1180$.



# The dynamic Tardos scheme: Example

Example: $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$ and $n = 100$. Parameters: $Z = 270.47$, $\delta = 0.0123$ and theoretically $\ell = 2285$. Strategy: Scapegoat strategy. Time needed: $t = 1120$.



# The dynamic Tardos scheme: Summary

Comparison with static Tardos scheme:

- Now certainty about catching all colluders instead of at least one.
- Still with high probability no innocent users are accused.
- Value $\ell$ only (rough) upper bound on time needed; usually $t \ll \ell$.
- Small $c$: Slightly higher values of $\ell$.
- Large $c$: Asymptotically same codelengths.
- Code can still be generated in advance.
- Downside: Need to know $c$ in advance.

# The dynamic Tardos scheme: Summary

Comparison with static Tardos scheme:

- Now certainty about catching all colluders instead of at least one.
- Still with high probability no innocent users are accused.
- Value $\ell$ only (rough) upper bound on time needed; usually $t \ll \ell$.
- Small $c$: Slightly higher values of $\ell$.
- Large $c$: Asymptotically same codelengths.
- Code can still be generated in advance.
- **Downside: Need to know $c$ in advance.**

# The universal Tardos scheme: Intro

The Tardos scheme depends on $c$:

- Distribution $f$ depends on $\delta$ and hence on $c$.
- Scores do not depend on $c$.

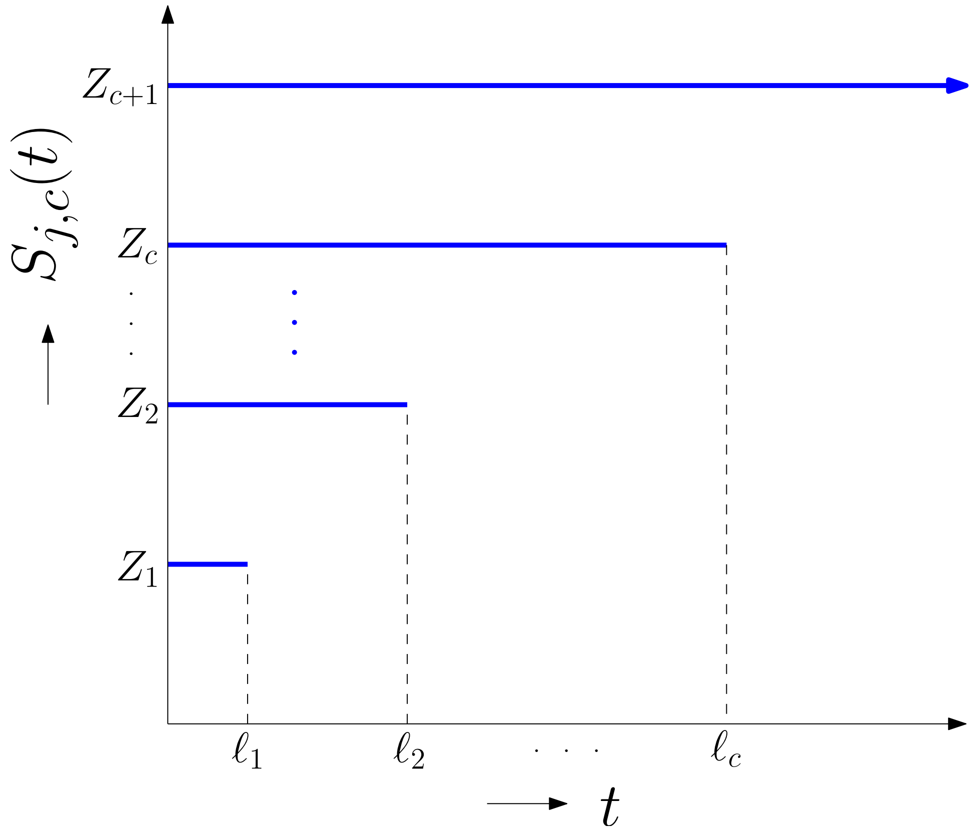
First idea: Generate $p_i$ and $X_{ji}$ using $u(p)$, and for scores for fixed $c$, simply disregard $p_i \notin [\delta_c, 1-\delta_c]$. The values that are in $[\delta_c, 1-\delta_c]$ are then distributed as $f_c(p)$ because $f_c(p) = K_c \cdot u(p)$.

$$u(p) = \frac{1}{\pi} \cdot \frac{1}{\sqrt{p(1-p)}}$$

Second idea: Run simultaneous dynamic Tardos schemes for each $c$, each using the same code $X_{j,i}$.

# The universal Tardos scheme: Intro

Second idea: Run simultaneous dynamic Tardos schemes for each $c$, each using the same code $X_{j,i}$.



# The universal Tardos scheme: Outline

Initialization:

- For each $c$, take $\ell_c = d_{\ell,c} c^2 \ln(n/\epsilon_{1,c})$.
- For each $c$, take $\delta_c = 1/(d_{\delta,c} c)$.
- For each $c$, take $Z_c = d_{z,c} c \ln(n/\epsilon_{1,c})$.
- For each $c$, initialize a counter $t_c = 0$.
- For each $c$ and $j$, initialize scores $S_{j,c}(0) = 0$.

Codeword generation: (independent of $c$)

- Generate $p_i \in [0, 1]$ from $u(p)$.
- Generate $X_{ji}$ using $\mathbb{P}[X_{ji} = 1] = p_i$.

# The universal Tardos scheme: Outline

Initialization:

- $\ell_c = d_{\ell,c} c^2 \ln(n/\epsilon_1)$, $\delta_c = 1/(d_{\delta,c} c)$, $Z_c = d_{z,c} c \ln(n/\epsilon_{1,c})$, $t_c = 0$, $S_{j,c}(0) = 0$.

Codeword generation: (independent of $c$)

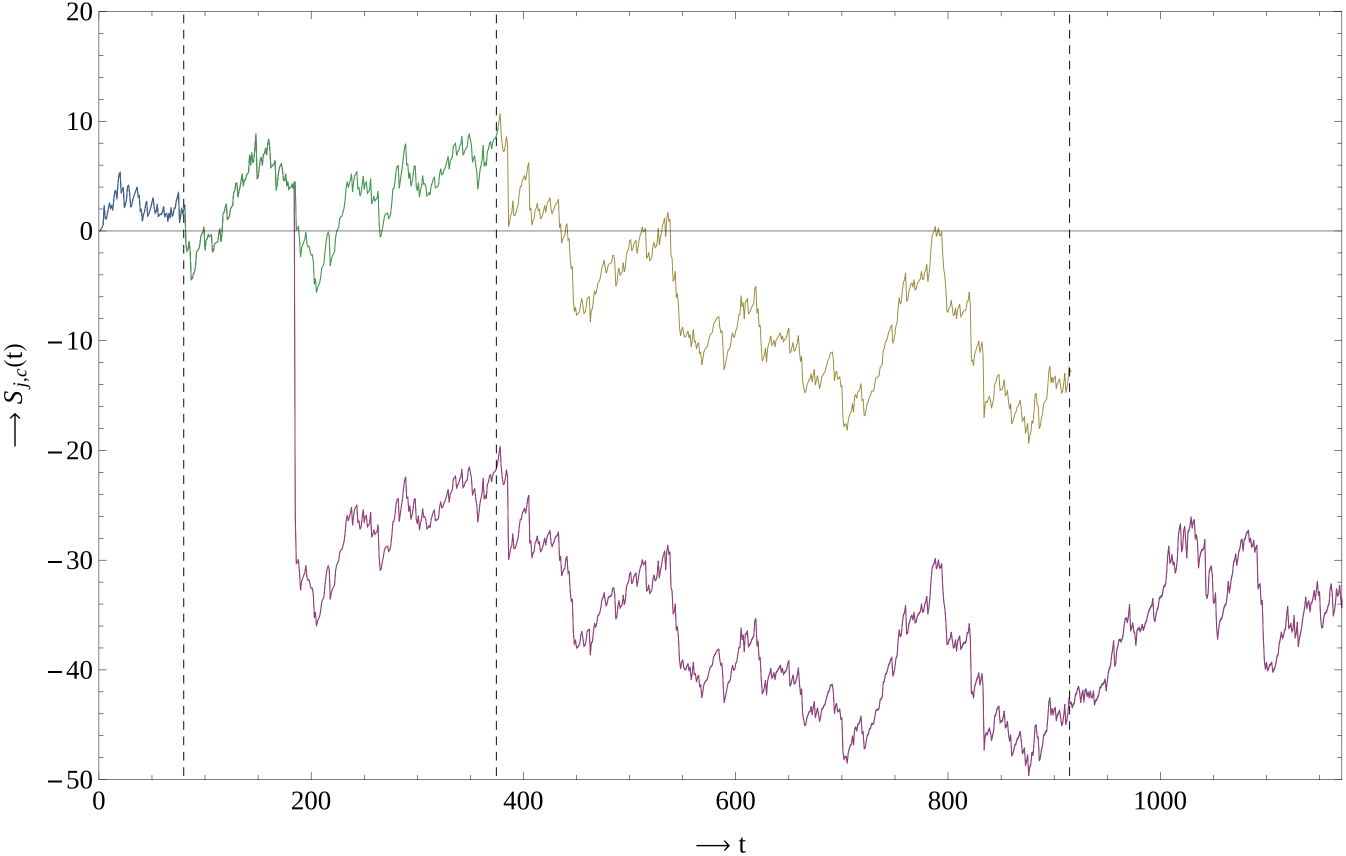
- $p_i \in [0, 1]$ from $u(p)$, $\mathbb{P}[X_{ji} = 1] = p_i$.

Distribution/Accusation: For each $t = 1, \ldots, (\ell)$.

- Send $t$th symbols to active users
- Intercept $y_t$ (or terminate if no pirate output)
- Calculate $S_{j,t}$ for $X_{j,t} = 0/1$.
- For each $c$ with $p_t \in [\delta_c, 1 - \delta_c]$:
  - ▷ Update $S_{j,c}(t) = S_{j,c}(t-1) + S_{j,t}$.
  - ▷ Update $t_c = t_c + 1$.
  - ▷ If $t_c \leq \ell_c$ and $S_{j,c}(t) > Z_c$ then disconnect user $j$.

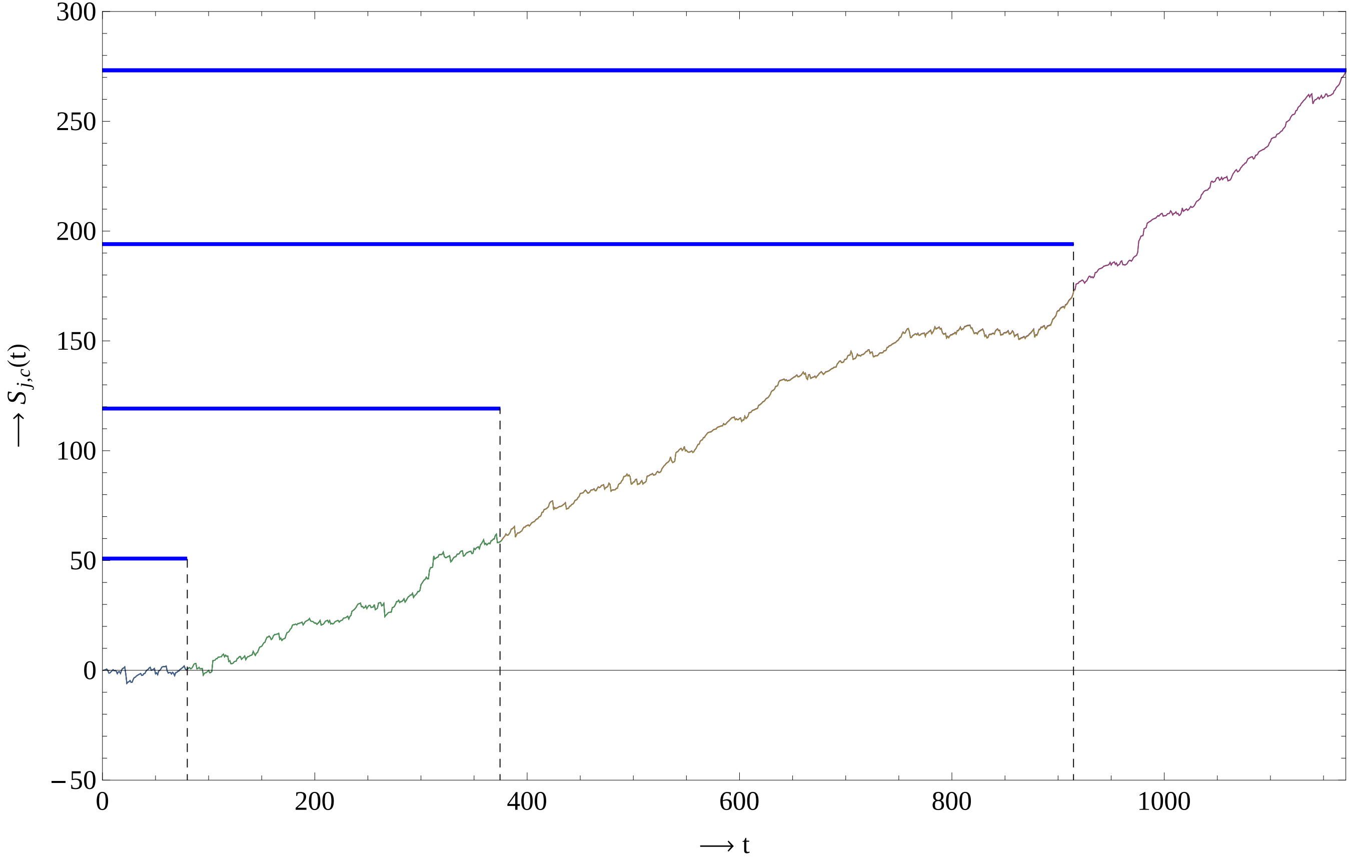
# The universal Tardos scheme: Example

Keeping multiple scores per user:



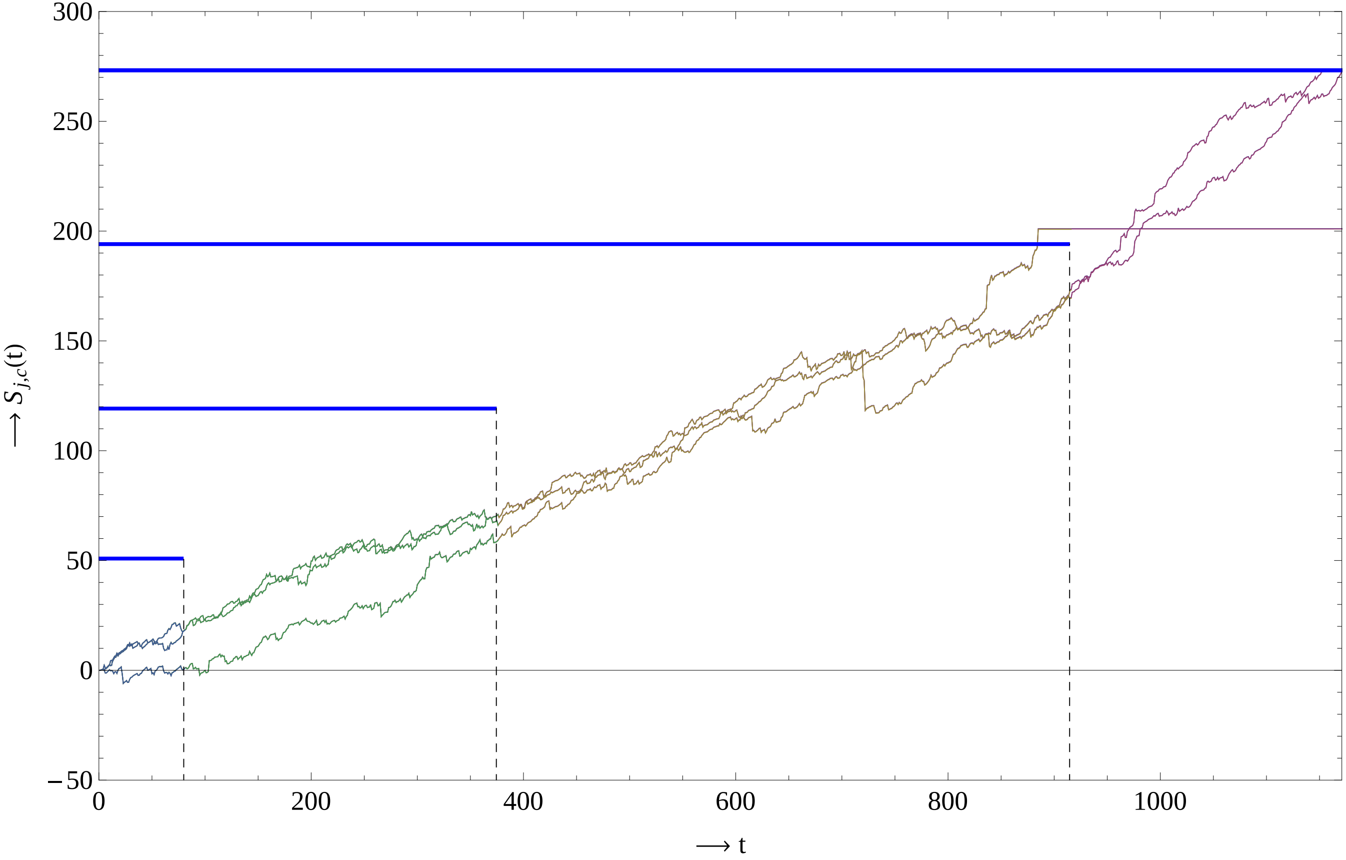
# The universal Tardos scheme: Example

Keeping multiple scores per user:



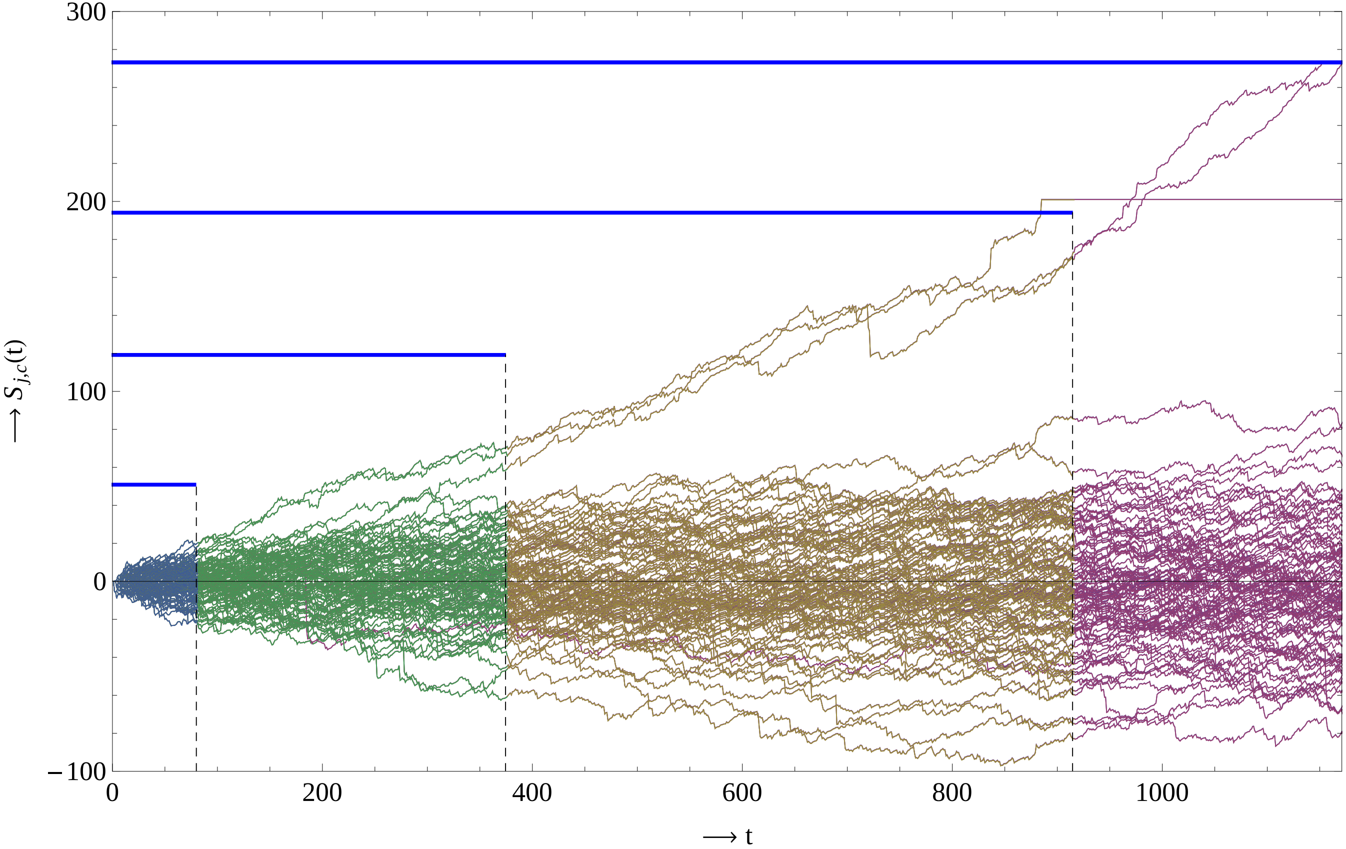
# The universal Tardos scheme: Example

Keeping multiple scores per user:



# The universal Tardos scheme: Example

Keeping multiple scores per user:



# The universal Tardos scheme: Details

Soundness:

- Errors stack: Total error probability $\sum_{c=1}^{\infty} \epsilon_{1,c}$.
- Use e.g. $\sum_{c=1}^{\infty} 1/c^2 = \pi^2/6$.
- Taking $\epsilon_{1,c} = 6\epsilon_1/(\pi^2 c^2)$ gives $\sum_{c=1}^{\infty} \epsilon_{1,c} \leq \epsilon_1$.

Completeness:

- Success probability at least as big as in regular dynamic scheme.

Time needed:

- On average $\ell_c/(1 - \frac{4}{\pi}\arcsin(\sqrt{1/(d_\delta c)})) = \mathcal{O}(c^2 \ln(n/\epsilon_1))$ time needed.
- Probability of needing more time decreases exponentially.

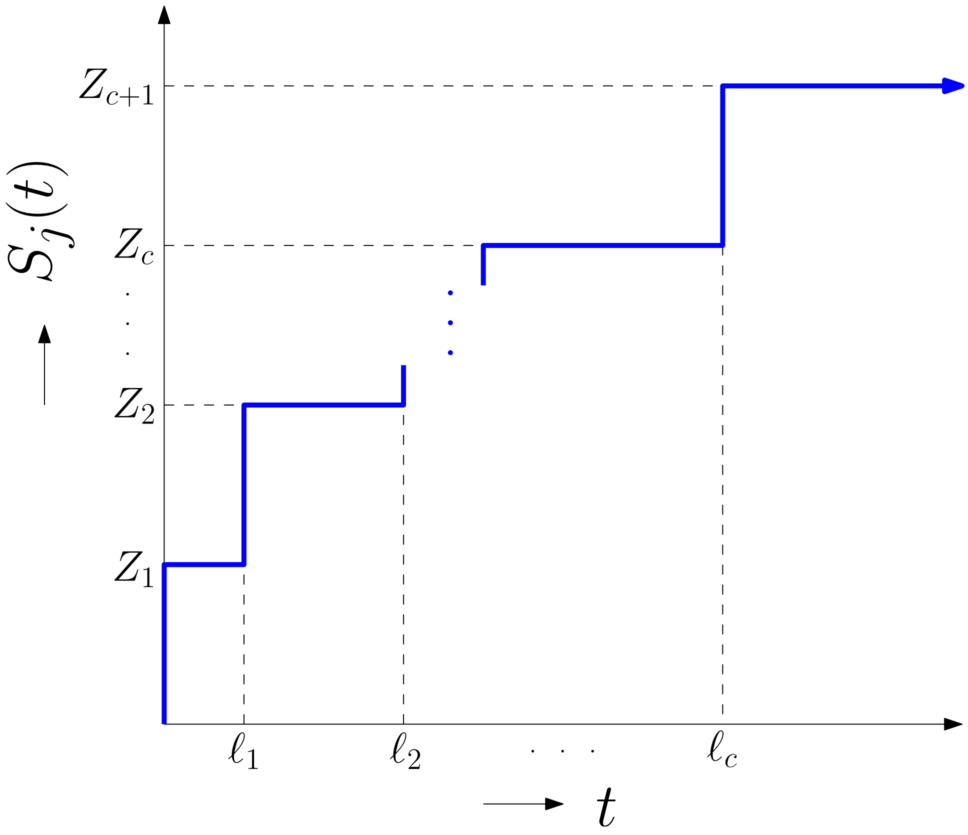
# The universal Tardos scheme: Summary

Comparison with dynamic Tardos scheme:

- Still high certainty about catching all colluders.
- Still with high probability no innocent users are ever accused.
- General algorithm: Can be applied for any coalition size.
- Code can still be generated in advance.
- Codelength/time slightly increases.
- Symbols always distributed using same $u(p)$.
- Only downside: Need to keep scores per user and per $c$.

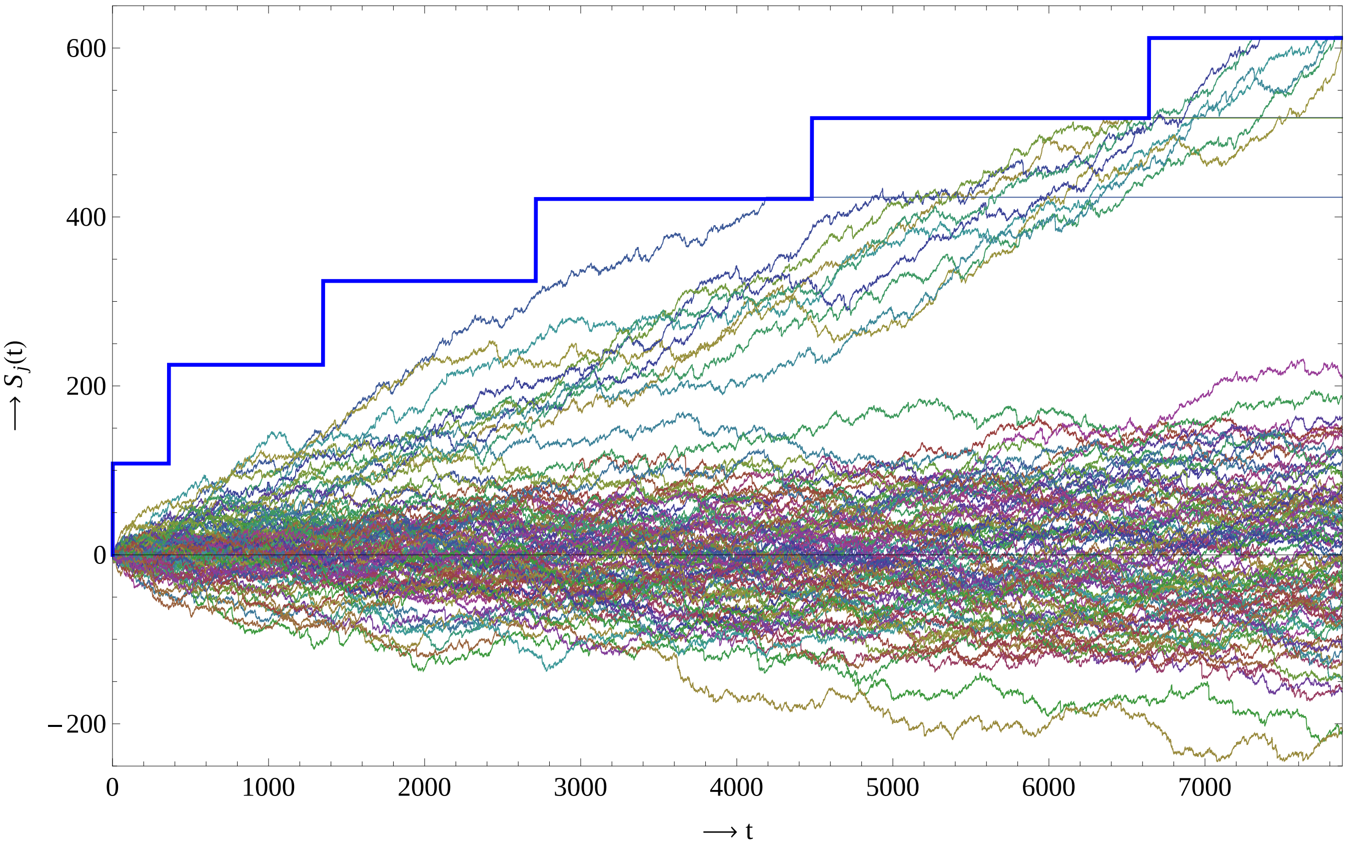
# The staircase Tardos scheme: Intro

Alternative to universal Tardos scheme: Staircase Tardos scheme:



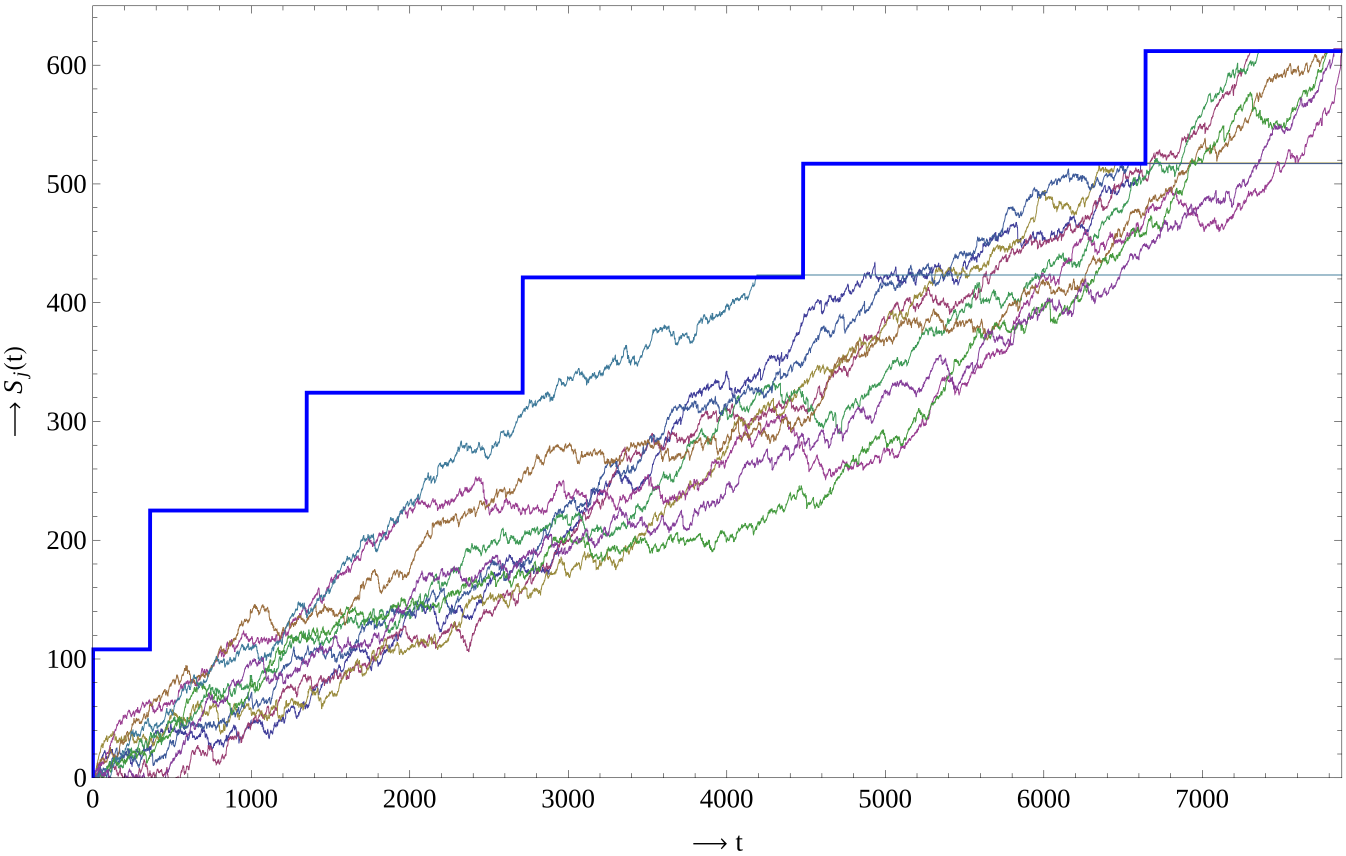
# The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme:



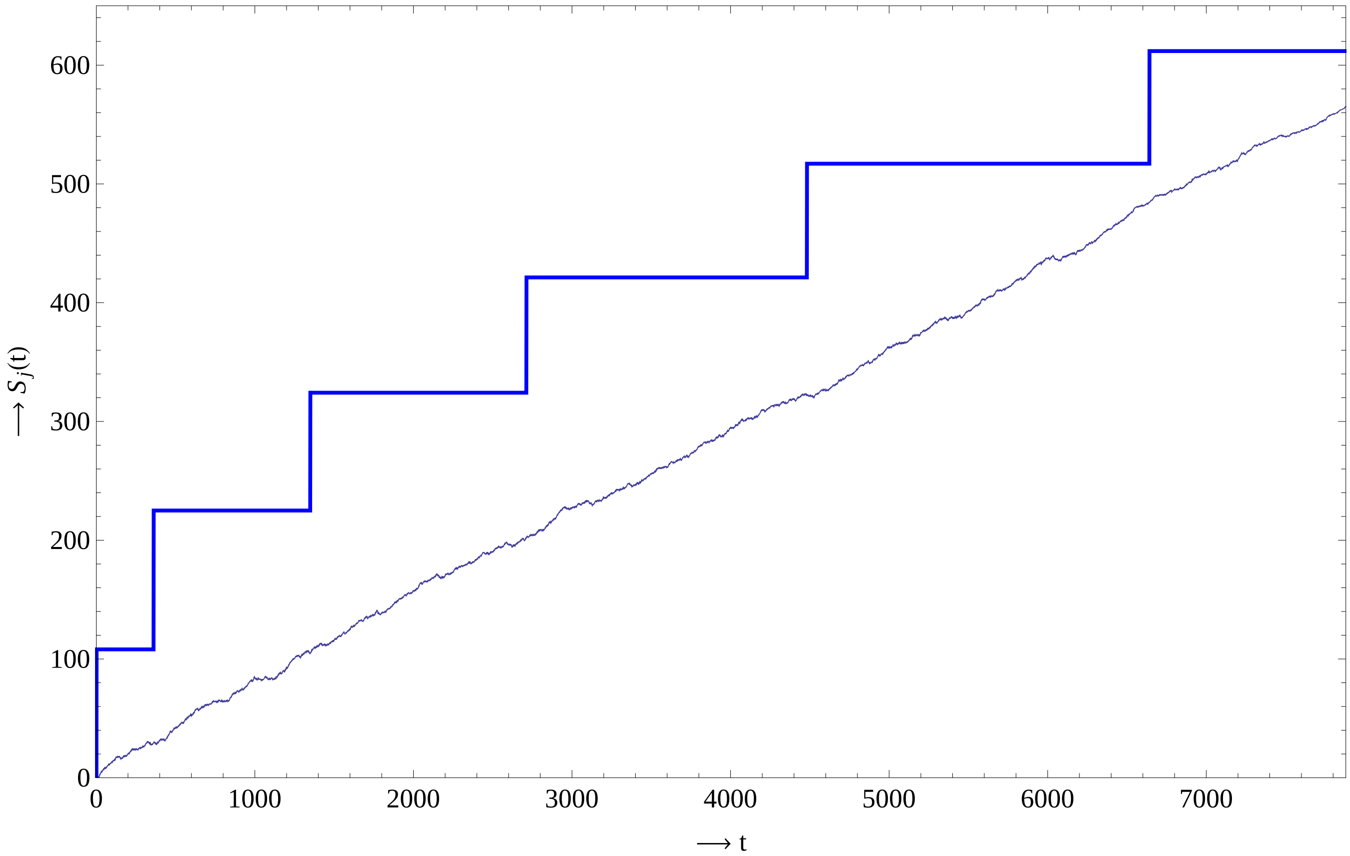
# The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme:



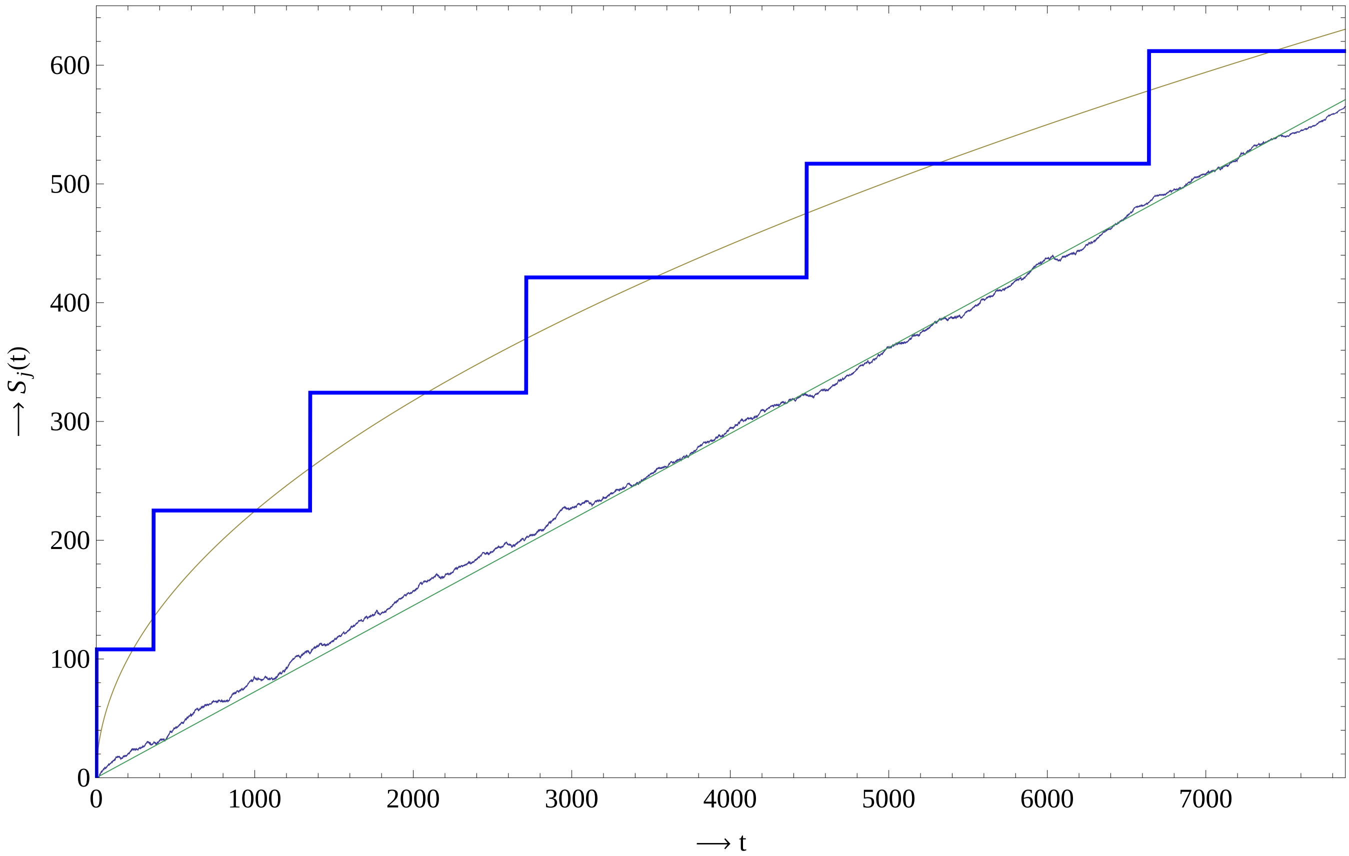
# The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme:



# The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme:



# The staircase Tardos scheme: Details

Soundness:

- Errors still stack: Total error probability $\sum_{c=1}^{\infty} \epsilon_{1,c}$.
- Taking $\epsilon_{1,c} = 6\epsilon_1/(\pi^2 c^2)$ again gives $\sum_{c=1}^{\infty} \epsilon_{1,c} \leq \epsilon_1$.

Completeness:

- Success probability still at least as big as in dynamic scheme.

Time needed fixed: After $\ell_c$ time, at least $1-\epsilon_2$ chance of having caught the whole coalition.

# The staircase Tardos scheme: Summary

Alternative to universal Tardos scheme: Staircase Tardos scheme:

- Update distribution of $f(p)$ after $\ell_1, \ell_2, \ldots$.
- Advantage: Keep only one score per user.
- Advantage: Always use all positions.
- Advantage: Slightly shorter (fixed) codelengths.
- Disadvantage: Distribution $f(p)$ depends on time $t$.
- Disadvantage: Less flexible for stopping/continuing tracing.

# Conclusion

First half of the project:

- Extensive literature study.
- Report: Detailed analysis of many known schemes.
- Gap in literature: Probabilistic dynamic schemes.

Second half of the project:

- New result (2): Dynamic Tardos scheme.
- Problem: Which Tardos scheme to use? Blayer and Tassa? Skoric?
- New result (1): Improved Tardos scheme.
- Problem: Dynamic Tardos scheme depends on $c$...
- New result (3): Universal Tardos scheme.
- New result (4): Staircase Tardos scheme.

After the project:

- Paper 1: Improved Tardos scheme.
- Paper 2: Dynamic Tardos schemes.

# Questions

Thank you for your attention! Any questions?