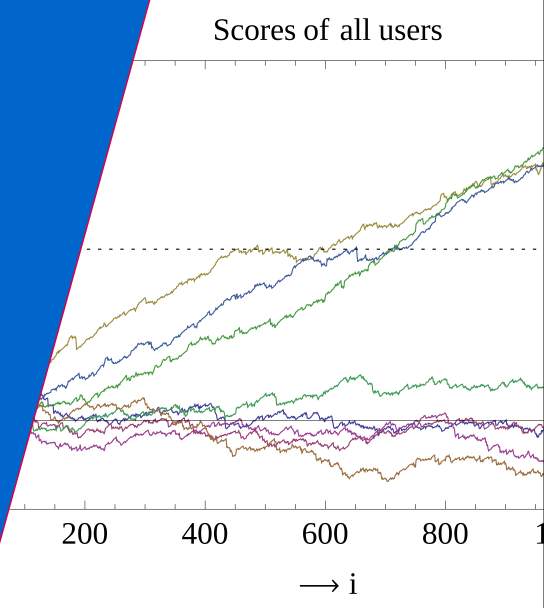
Collusion-resistant traitor tracing schemes

Final presentation of Thijs Laarhoven



Technische Universiteit Eindhoven University of Technology

July 13th, 2011

Contents

Technische Universiteit Eindhoven University of Technology

Introduction: Digital content

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	...
David	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	...
Henry	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	...

These days a lot of digital content is sold and distributed, e.g. movies, software.

This content can generally be represented by a long list of bits.

TU/e Technische Universiteit Eindhoven University of Technology

Introduction: Illegal redistribution

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	...
David	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	...
Henry	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	...
Copy	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	...

Problem: Digital content is easy to copy and distribute among others.

It is impossible for the distributor to find the guilty user.

Technische Universiteit Eindhoven University of Technology

Introduction: Embed watermarks

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	...
David	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	...
Henry	0	1	0	1	0	1	1	1	1	0	0	1	0	1	1	0	...

Solution: Embed watermarks in data so that copies can be traced back to users.

TU/e Technische Universiteit Eindhoven University of Technology

Introduction: Embed watermarks

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	...
David	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	...
Henry	0	1	0	1	0	1	1	1	1	0	0	1	0	1	1	0	...
Copy	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	0	...

Solution: Embed watermarks in data so that copies can be traced back to users.

Someone bought the content, copies it and distributes the copies.

Introduction: Embed watermarks

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	...
David	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	...
Henry	0	1	**0**	1	0	**1**	**1**	1	1	0	**0**	1	**0**	**1**	**1**	0	...
Copy	0	1	**0**	1	0	**1**	**0**	1	1	0	**1**	1	**1**	**0**	**0**	0	...

Solution: Embed watermarks in data so that copies can be traced back to users.

Someone bought the content, copies it and distributes the copies.

But the distributor can intercept a copy, and find the guilty user.

Introduction: Collusion-attacks

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	...
David	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	...
Henry	0	1	0	1	0	1	1	1	1	0	0	1	0	1	1	0	...

Problem: Users may collude and compare their content to find the watermark.

TU/e Technische Universiteit Eindhoven University of Technology

Introduction: Collusion-attacks

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	...
David	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	...
Henry	0	1	0	1	0	1	1	1	1	0	0	1	0	1	1	0	...

Problem: Users may collude and compare their content to find the watermark.

Introduction: Collusion-attacks

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	...
David	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	...
Henry	0	1	0	1	0	1	1	1	1	0	0	1	0	1	1	0	...
Copy	0	1	**1**	1	0	**1**	**0**	1	1	0	1	1	**0**	**1**	0	0	...

Problem: Users may collude and compare their content to find the watermark.

On detectable positions they choose a bit, the rest they simply copy.

Introduction: Collusion-attacks

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	...
David	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	...
Henry	0	1	**0**	1	0	**1**	**1**	1	1	0	**0**	1	**0**	**1**	**1**	0	...
Copy	0	1	**1**	1	0	**1**	**0**	1	1	0	**1**	1	**0**	**1**	**0**	0	...

Problem: Users may collude and compare their content to find the watermark.

On detectable positions they choose a bit, the rest they simply copy.

Now the distributor cannot find the guilty users.

Technische Universiteit Eindhoven University of Technology

Introduction: Our problem

Alice	1	0	1	1	0	1	0	...
Bob	1	1	0	1	1	1	1	...
Charlie	0	1	0	0	1	0	1	...
David	1	0	0	1	0	0	0	...
Eve	0	1	0	1	1	0	0	...
Fred	0	0	1	0	0	1	0	...
George	1	1	1	1	0	0	1	...
Henry	0	1	1	0	0	1	1	...
Copy	1	1	0	1	0	1	0	...

So we need **collusion-resistant traitor tracing schemes**, consisting of:

- Codeword generation: Assigning symbols to users.
- Tracing algorithm: Tracing copies back to guilty users.

We only focus on the embedded watermarks, not on the data itself.

Model: Abstraction

Alice	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	$X_{1,6}$	$\dots$	$X_{1,\ell}$
Bob	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	$X_{2,6}$	$\dots$	$X_{2,\ell}$
Charlie	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$	$\dots$	$X_{3,\ell}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	$X_{4,6}$	$\dots$	$X_{4,\ell}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	$X_{5,6}$	$\dots$	$X_{5,\ell}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	$X_{6,6}$	$\dots$	$X_{6,\ell}$
George	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	$X_{7,6}$	$\dots$	$X_{7,\ell}$
Henry	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$	$\dots$	$X_{8,\ell}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\dots$	y_ℓ

Notation: Users $j = 1, \dots, n$, positions $i = 1, \dots \ell$, code matrix $X = (X_{j,i})$.

Pirates: A coalition C of c pirates, generates $\vec{y}$ such that $y_i \in \{X_{j,i} : j \in C\}$.

Tracing algorithm: Maps output $\vec{y}$ to a set of accused users $C^* \stackrel{?}{=} C$.

Successful if $C^* \subseteq C$ and either $C^* \cap C \neq \emptyset$ or (ideally) $C \subseteq C^*$.

Model: Pirate strategies

On any position, pirates output one of their symbols.

- Scapegoat: Always take the symbol of the same pirate.
- Always bit 0: Output a 0 whenever possible.
- Majority voting: Output the most occurring bit.
- Minority voting: Output the least occurring bit.
- Interleaving attack: Select a random pirate and output his symbol.

Example:

$$\begin{aligned}
(X_{j,i} : j \in C) &= \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 1 \\ 1 & \mathbf{1} & 1 & 0 & \mathbf{1} & 0 & 0 \\ 1 & \mathbf{1} & 0 & 1 & \mathbf{1} & 1 & 0 \end{pmatrix} \\
\vec{y} &= \begin{pmatrix} * & \mathbf{1} & * & * & \mathbf{1} & * & * \end{pmatrix} \\
\text{Scapegoat: } \vec{y} &= \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 1 \end{pmatrix} \\
\text{Always bit 0: } \vec{y} &= \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 \end{pmatrix} \\
\text{Majority: } \vec{y} &= \begin{pmatrix} 1 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 \end{pmatrix}
\end{aligned}$$

Model: Static vs. dynamic

Static schemes: **Distribute all symbols at the start.**

- Codewords do not depend on pirate output.
- Catch at least one pirate.
- Applications: Video on demand, software.

Dynamic schemes: **Distribute symbols $X_{j,i}$ after receiving y_{i-1}.**

- Codewords may depend on previous pirate output.
- Users may be disconnected from the system before distributing new content.
- Catch all pirates.
- Applications: Live streams, pay-tv.

This presentation: Both types.

TU/e Technische Universiteit Eindhoven University of Technology

Model: Deterministic vs. probabilistic

Deterministic schemes: **No error in accusations.**

- Do not exist for $c \geq 2$ and binary alphabet: need bigger alphabet.

Probabilistic schemes: **Accusation errors bounded by $\epsilon_1, \epsilon_2 > 0$.**

- Accuse no innocent users with probability at least $1 - \epsilon_1$.
- Static: Catch at least one guilty user w.p. at least $1 - \epsilon_2$.
- Dynamic: Catch all users w.p. at least $1 - \epsilon_2$.

This presentation: Only probabilistic (binary) schemes.

TU/e Technische Universiteit Eindhoven University of Technology

Previous results: Probabilistic schemes

ℓ codelength, n total users, c pirates, ϵ_1 probability of accusing innocent users

	Codelength (small coalitions)	Codelength (large coalitions)
Static schemes	$\ell \geq \Omega(c^2 \ln(n/\epsilon_1))$	$\ell \geq 1.38c^2 \ln(n/\epsilon_1)$
- Boneh and Shaw	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$
- Tardos	$\ell = 100c^2 \ln(n/\epsilon_1)$	$\ell = 100c^2 \ln(n/\epsilon_1)$
- Vladimirova et al.	$\ell \approx 90c^2 \ln(n/\epsilon_1)$	$\ell \approx 39.48c^2 \ln(n/\epsilon_1)$
- Blayer and Tassa	$\ell = 85c^2 \ln(n/\epsilon_1)$	$\ell \approx 19.74c^2 \ln(n/\epsilon_1)$
- Škorić et al.	$\ell \approx 50c^2 \ln(n/\epsilon_1)$	$\ell \approx 9.87c^2 \ln(n/\epsilon_1)$
- Nuida et al.	$\ell \approx 5c^2 \ln(n/\epsilon_1)$	$\ell \approx 5.35c^2 \ln(n/\epsilon_1)$
Dynamic schemes	?	?
- Tassa	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$

Technische Universiteit Eindhoven University of Technology

New results: Tardos modifications

ℓ codelength, n total users, c pirates, ϵ_1 probability of accusing innocent users

	Codelength (small coalitions)	Codelength (large coalitions)
Static schemes	$\ell \geq \Omega(c^2 \ln(n/\epsilon_1))$	$\ell \geq 1.38c^2 \ln(n/\epsilon_1)$
- Boneh and Shaw	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$
- Tardos	$\ell = 100c^2 \ln(n/\epsilon_1)$	$\ell = 100c^2 \ln(n/\epsilon_1)$
- Vladimirova et al.	$\ell \approx 90c^2 \ln(n/\epsilon_1)$	$\ell \approx 39.48c^2 \ln(n/\epsilon_1)$
- Blayer and Tassa	$\ell = 85c^2 \ln(n/\epsilon_1)$	$\ell \approx 19.74c^2 \ln(n/\epsilon_1)$
- Škorić et al.	$\ell \approx 50c^2 \ln(n/\epsilon_1)$	$\ell \approx 9.87c^2 \ln(n/\epsilon_1)$
- Nuida et al.	$\ell \approx 5c^2 \ln(n/\epsilon_1)$	$\ell \approx 5.35c^2 \ln(n/\epsilon_1)$
- Optimal Tardos	$\ell \approx \mathbf{24}c^2 \ln(n/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(n/\epsilon_1)$
Dynamic schemes	?	?
- Tassa	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$
- Dynamic Tardos	$\ell \approx \mathbf{26}c^2 \ln(n/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(n/\epsilon_1)$
- Universal Tardos	$\ell \approx \mathbf{26}c^2 \ln(nc^2/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon_1)$
- Staircase Tardos	$\ell \approx \mathbf{26}c^2 \ln(nc^2/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon_1)$

New results: Tardos modifications

ℓ codelength, n total users, c pirates, ϵ_1 probability of accusing innocent users

	Codelength (small coalitions)	Codelength (large coalitions)
Static schemes	$\ell \geq \Omega(c^2 \ln(n/\epsilon_1))$	$\ell \geq 1.38c^2 \ln(n/\epsilon_1)$
- Boneh and Shaw	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$	$\ell \approx 32c^4 \ln(n/\epsilon_1) \ln(c/\epsilon_1)$
- Tardos	$\ell = 100c^2 \ln(n/\epsilon_1)$	$\ell = 100c^2 \ln(n/\epsilon_1)$
- Vladimirova et al.	$\ell \approx 90c^2 \ln(n/\epsilon_1)$	$\ell \approx 39.48c^2 \ln(n/\epsilon_1)$
- Blayer and Tassa	$\ell = 85c^2 \ln(n/\epsilon_1)$	$\ell \approx 19.74c^2 \ln(n/\epsilon_1)$
- Škorić et al.	$\ell \approx 50c^2 \ln(n/\epsilon_1)$	$\ell \approx 9.87c^2 \ln(n/\epsilon_1)$
- Nuida et al.	$\ell \approx 5c^2 \ln(n/\epsilon_1)$	$\ell \approx 5.35c^2 \ln(n/\epsilon_1)$
- Optimal Tardos	$\ell \approx \mathbf{24}c^2 \ln(n/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(n/\epsilon_1)$
Dynamic schemes	?	?
- Tassa	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$	$\ell = \mathcal{O}(c^4 \log(n) \ln(c/\epsilon_1))$
- Dynamic Tardos	$\ell \approx \mathbf{26}c^2 \ln(n/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(n/\epsilon_1)$
- Universal Tardos	$\ell \approx \mathbf{26}c^2 \ln(nc^2/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon_1)$
- Staircase Tardos	$\ell \approx \mathbf{26}c^2 \ln(nc^2/\epsilon_1)$	$\ell \approx \mathbf{4.93}c^2 \ln(nc^2/\epsilon_1)$

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Introduction

Codeword generation: **Randomized code**

- For each column i, first select a bias $p_i \sim f(p)$.
- Then, for each user j, select $X_{j,i} = 1$ with probability p_i.

Tracing algorithm: **Assign scores to users**

- Each user starts with a score $S_j(0) = 0$.
- For each position i and user j, calculate $S_{j,i}$ and update $S_j(i) = S_j(i-1) + S_{j,i}$.

$$S_{j,i} = \begin{cases} +\sqrt{(1-p_i)/p_i} & \text{if } X_{j,i} = 1, y_i = 1, \\ -\sqrt{(1-p_i)/p_i} & \text{if } X_{j,i} = 1, y_i = 0, \\ -\sqrt{p_i/(1-p_i)} & \text{if } X_{j,i} = 0, y_i = 1, \\ +\sqrt{p_i/(1-p_i)} & \text{if } X_{j,i} = 0, y_i = 0. \end{cases}$$

- Positive scores for matches (guilty), negative scores for differences (innocent).
- High contributions for unlikely matches/differences.
- Accuse a user j if $S_j(\ell) > Z$.

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Example

Parameters we choose:

- $n = 8$: In total there will be 8 users in the system.
- $c = 3$: The size of the coalition is 3.
- $\epsilon_1 = 0.01$: With 99% certainty no innocent users are accused.
- $\epsilon_2 = 0.01$: With 99% certainty at least one pirate is caught.

Parameters for the scheme that roll out:

- $\ell = 1208$: The codelength of the scheme is 1208.
- $Z = 146$: If a user's final score exceeds 146, he will be accused.
- $\delta = 0.0115$: The values p_i chosen later will be in the interval $[\delta, 1-\delta]$.
- $f(p) = 0.369/\sqrt{p(1-p)}$: The probability density function for generating p_i.
  - High probability of getting $p \approx 0$ or $p \approx 1$.
  - Constant 0.369 such that $\int_\delta^{1-\delta} f(p)dp = 1$.

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

For each i**, generate** $p_i \sim f(p)$ **and take** $X_{j,i} = 1$ **w.p.** p_i

	p_1	p_2	p_3	p_4	p_5	p_6	$\cdots$	p_{1208}
Alice	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	$X_{1,6}$	$\cdots$	$X_{1,1208}$
Bob	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	$X_{2,6}$	$\cdots$	$X_{2,1208}$
Charlie	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$	$\cdots$	$X_{3,1208}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	$X_{4,6}$	$\cdots$	$X_{4,1208}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	$X_{5,6}$	$\cdots$	$X_{5,1208}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	$X_{6,6}$	$\cdots$	$X_{6,1208}$
George	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	$X_{7,6}$	$\cdots$	$X_{7,1208}$
Henry	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$	$\cdots$	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\cdots$	y_{1208}

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each i, generate $p_i \sim f(p)$ and take $X_{j,i} = 1$ w.p. p_i

	0.20	p_2	p_3	p_4	p_5	p_6	$\cdots$	p_{1208}
Alice	0	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	$X_{1,6}$	$\cdots$	$X_{1,1208}$
Bob	1	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	$X_{2,6}$	$\cdots$	$X_{2,1208}$
Charlie	1	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$	$\cdots$	$X_{3,1208}$
David	0	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	$X_{4,6}$	$\cdots$	$X_{4,1208}$
Eve	0	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	$X_{5,6}$	$\cdots$	$X_{5,1208}$
Fred	1	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	$X_{6,6}$	$\cdots$	$X_{6,1208}$
George	0	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	$X_{7,6}$	$\cdots$	$X_{7,1208}$
Henry	0	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$	$\cdots$	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\cdots$	y_{1208}

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

For each i, generate $p_i \sim f(p)$ and take $X_{j,i} = 1$ w.p. p_i

	0.20	0.05	p_3	p_4	p_5	p_6	$\dots$	p_{1208}
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	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$	$\dots$	$X_{3,1208}$
David	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	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$	$\dots$	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\dots$	y_{1208}

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

For each i**, generate** $p_i \sim f(p)$ **and take** $X_{j,i} = 1$ **w.p.** p_i

	0.20	0.05	0.88	p_4	p_5	p_6	$\cdots$	p_{1208}
Alice	0	0	1	$X_{1,4}$	$X_{1,5}$	$X_{1,6}$	$\cdots$	$X_{1,1208}$
Bob	1	0	1	$X_{2,4}$	$X_{2,5}$	$X_{2,6}$	$\cdots$	$X_{2,1208}$
Charlie	1	0	0	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$	$\cdots$	$X_{3,1208}$
David	0	0	1	$X_{4,4}$	$X_{4,5}$	$X_{4,6}$	$\cdots$	$X_{4,1208}$
Eve	0	0	1	$X_{5,4}$	$X_{5,5}$	$X_{5,6}$	$\cdots$	$X_{5,1208}$
Fred	1	0	1	$X_{6,4}$	$X_{6,5}$	$X_{6,6}$	$\cdots$	$X_{6,1208}$
George	0	0	1	$X_{7,4}$	$X_{7,5}$	$X_{7,6}$	$\cdots$	$X_{7,1208}$
Henry	0	0	0	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$	$\cdots$	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\cdots$	y_{1208}

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each i**, generate** $p_i \sim f(p)$ **and take** $X_{j,i} = 1$ **w.p.** p_i

	0.20	0.05	0.88	0.79	p_5	p_6	$\dots$	p_{1208}
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	$X_{3,5}$	$X_{3,6}$	$\dots$	$X_{3,1208}$
David	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	$X_{8,5}$	$X_{8,6}$	$\dots$	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	$\dots$	y_{1208}

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each i**, generate** $p_i \sim f(p)$ **and take** $X_{j,i} = 1$ **w.p.** p_i

	0.20	0.05	0.88	0.79	0.98	p_6	...	p_{1208}
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	$X_{3,6}$	...	$X_{3,1208}$
David	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	$X_{8,6}$	...	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each i, generate $p_i \sim f(p)$ and take $X_{j,i} = 1$ w.p. p_i

	0.20	0.05	0.88	0.79	0.98	0.09	...	p_{1208}
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	...	$X_{3,1208}$
David	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	1	...	$X_{8,1208}$
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each i**, generate** $p_i \sim f(p)$ **and take** $X_{j,i} = 1$ **w.p.** p_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	...	1
Charlie	1	0	0	1	0	1	...	0
David	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	1	...	0
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

The Tardos scheme: Codewords

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

The code is complete, and is embedded in the content.

	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	...	1
Charlie	1	0	0	1	0	1	...	0
David	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	1	...	0
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

The Tardos scheme: Coalition

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

Pirates buy their copies, ...

	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	...	1
Charlie	1	0	0	1	0	1	...	0
David	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	1	...	0
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

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

The Tardos scheme: Coalition

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

Pirates buy their copies, compare them ...

	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	...	1
Charlie	**1**	0	**0**	**1**	**0**	**1**	...	0
David	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**	**1**	...	0
Copy	y_1	y_2	y_3	y_4	y_5	y_6	...	y_{1208}

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Coalition

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

Pirates buy their copies, compare them and generate some $\vec{y}$

	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	...	1
Charlie	**1**	0	**0**	**1**	**0**	**1**	...	0
David	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**	**1**	...	0
Copy	**0**	0	**0**	**1**	**1**	**0**	...	0

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Coalition

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

The copy is put online, and the distributor intercepts $\vec{y}$

	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	...	1
Charlie	1	0	0	1	0	1	...	0
David	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	1	...	0
Copy	0	0	0	1	1	0	...	0

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i**, he calculates** $S_{j,i}$ **and** $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(0)$
Alice	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	...	$S_{1,1208}$	0
Bob	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	...	$S_{2,1208}$	0
Charlie	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	...	$S_{3,1208}$	0
David	$S_{4,1}$	$S_{4,2}$	$S_{4,3}$	$S_{4,4}$	$S_{4,5}$	$S_{4,6}$	...	$S_{4,1208}$	0
Eve	$S_{5,1}$	$S_{5,2}$	$S_{5,3}$	$S_{5,4}$	$S_{5,5}$	$S_{5,6}$	...	$S_{5,1208}$	0
Fred	$S_{6,1}$	$S_{6,2}$	$S_{6,3}$	$S_{6,4}$	$S_{6,5}$	$S_{6,6}$	...	$S_{6,1208}$	0
George	$S_{7,1}$	$S_{7,2}$	$S_{7,3}$	$S_{7,4}$	$S_{7,5}$	$S_{7,6}$	...	$S_{7,1208}$	0
Henry	$S_{8,1}$	$S_{8,2}$	$S_{8,3}$	$S_{8,4}$	$S_{8,5}$	$S_{8,6}$	...	$S_{8,1208}$	0
Copy	0	0	0	1	1	0	...	0	

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

For each j, i, he calculates $S_{j,i}$ and $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(1)$
Alice	$+0.5$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	...	$S_{1,1208}$	$+0.5$
Bob	-2.0	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	...	$S_{2,1208}$	-2.0
Charlie	-2.0	$S_{3,2}$	$S_{3,3}$	$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	...	$S_{3,1208}$	-2.0
David	$+0.5$	$S_{4,2}$	$S_{4,3}$	$S_{4,4}$	$S_{4,5}$	$S_{4,6}$	...	$S_{4,1208}$	$+0.5$
Eve	$+0.5$	$S_{5,2}$	$S_{5,3}$	$S_{5,4}$	$S_{5,5}$	$S_{5,6}$	...	$S_{5,1208}$	$+0.5$
Fred	-2.0	$S_{6,2}$	$S_{6,3}$	$S_{6,4}$	$S_{6,5}$	$S_{6,6}$	...	$S_{6,1208}$	-2.0
George	$+0.5$	$S_{7,2}$	$S_{7,3}$	$S_{7,4}$	$S_{7,5}$	$S_{7,6}$	...	$S_{7,1208}$	$+0.5$
Henry	$+0.5$	$S_{8,2}$	$S_{8,3}$	$S_{8,4}$	$S_{8,5}$	$S_{8,6}$	...	$S_{8,1208}$	$+0.5$
Copy	0	0	0	1	1	0	...	0	

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

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i, **he calculates** $S_{j,i}$ **and** $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(2)$
Alice	+0.5	+0.2	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	...	$S_{1,1208}$	+0.7
Bob	−2.0	+0.2	$S_{2,3}$	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	...	$S_{2,1208}$	−1.8
Charlie	−2.0	+0.2	$S_{3,3}$	$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	...	$S_{3,1208}$	−1.8
David	+0.5	+0.2	$S_{4,3}$	$S_{4,4}$	$S_{4,5}$	$S_{4,6}$	...	$S_{4,1208}$	+0.7
Eve	+0.5	+0.2	$S_{5,3}$	$S_{5,4}$	$S_{5,5}$	$S_{5,6}$	...	$S_{5,1208}$	+0.7
Fred	−2.0	+0.2	$S_{6,3}$	$S_{6,4}$	$S_{6,5}$	$S_{6,6}$	...	$S_{6,1208}$	−1.8
George	+0.5	+0.2	$S_{7,3}$	$S_{7,4}$	$S_{7,5}$	$S_{7,6}$	...	$S_{7,1208}$	+0.7
Henry	+0.5	+0.2	$S_{8,3}$	$S_{8,4}$	$S_{8,5}$	$S_{8,6}$	...	$S_{8,1208}$	+0.7
Copy	0	0	0	1	1	0	...	0	

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i, **he calculates** $S_{j,i}$ **and** $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(3)$
Alice	+0.5	+0.2	−0.4	$S_{1,4}$	$S_{1,5}$	$S_{1,6}$	...	$S_{1,1208}$	+0.4
Bob	−2.0	+0.2	−0.4	$S_{2,4}$	$S_{2,5}$	$S_{2,6}$	...	$S_{2,1208}$	−2.1
Charlie	−2.0	+0.2	+2.7	$S_{3,4}$	$S_{3,5}$	$S_{3,6}$	...	$S_{3,1208}$	+1.0
David	+0.5	+0.2	−0.4	$S_{4,4}$	$S_{4,5}$	$S_{4,6}$	...	$S_{4,1208}$	+0.4
Eve	+0.5	+0.2	−0.4	$S_{5,4}$	$S_{5,5}$	$S_{5,6}$	...	$S_{5,1208}$	+0.4
Fred	−2.0	+0.2	−0.4	$S_{6,4}$	$S_{6,5}$	$S_{6,6}$	...	$S_{6,1208}$	−2.1
George	+0.5	+0.2	−0.4	$S_{7,4}$	$S_{7,5}$	$S_{7,6}$	...	$S_{7,1208}$	+0.4
Henry	+0.5	+0.2	+2.7	$S_{8,4}$	$S_{8,5}$	$S_{8,6}$	...	$S_{8,1208}$	+3.5
Copy	0	0	0	1	1	0	...	0	

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

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

For each j, i, **he calculates** $S_{j,i}$ **and** $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(4)$
Alice	+0.5	+0.2	−0.4	+0.5	$S_{1,5}$	$S_{1,6}$	...	$S_{1,1208}$	+0.9
Bob	−2.0	+0.2	−0.4	+0.5	$S_{2,5}$	$S_{2,6}$	...	$S_{2,1208}$	−1.6
Charlie	−2.0	+0.2	+2.7	+0.5	$S_{3,5}$	$S_{3,6}$	...	$S_{3,1208}$	+1.5
David	+0.5	+0.2	−0.4	+0.5	$S_{4,5}$	$S_{4,6}$	...	$S_{4,1208}$	+0.9
Eve	+0.5	+0.2	−0.4	−1.9	$S_{5,5}$	$S_{5,6}$	...	$S_{5,1208}$	−1.6
Fred	−2.0	+0.2	−0.4	−1.9	$S_{6,5}$	$S_{6,6}$	...	$S_{6,1208}$	−4.1
George	+0.5	+0.2	−0.4	−1.9	$S_{7,5}$	$S_{7,6}$	...	$S_{7,1208}$	−1.6
Henry	+0.5	+0.2	+2.7	+0.5	$S_{8,5}$	$S_{8,6}$	...	$S_{8,1208}$	+4.0
Copy	0	0	0	1	1	0	...	0	

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

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i, he calculates $S_{j,i}$ and $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(5)$
Alice	$+0.5$	$+0.2$	-0.4	$+0.5$	$+0.1$	$S_{1,6}$	...	$S_{1,1208}$	$+1.0$
Bob	-2.0	$+0.2$	-0.4	$+0.5$	$+0.1$	$S_{2,6}$	...	$S_{2,1208}$	-1.5
Charlie	-2.0	$+0.2$	$+2.7$	$+0.5$	-7.2	$S_{3,6}$	...	$S_{3,1208}$	-5.7
David	$+0.5$	$+0.2$	-0.4	$+0.5$	$+0.1$	$S_{4,6}$	...	$S_{4,1208}$	$+1.0$
Eve	$+0.5$	$+0.2$	-0.4	-1.9	$+0.1$	$S_{5,6}$	...	$S_{5,1208}$	-1.4
Fred	-2.0	$+0.2$	-0.4	-1.9	$+0.1$	$S_{6,6}$	...	$S_{6,1208}$	-3.9
George	$+0.5$	$+0.2$	-0.4	-1.9	$+0.1$	$S_{7,6}$	...	$S_{7,1208}$	-1.4
Henry	$+0.5$	$+0.2$	$+2.7$	$+0.5$	$+0.1$	$S_{8,6}$	...	$S_{8,1208}$	$+4.1$
Copy	0	0	0	1	1	0	...	0	

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

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i, he calculates $S_{j,i}$ and $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(6)$
Alice	+0.5	+0.2	−0.4	+0.5	+0.1	+0.3	...	$S_{1,1208}$	+1.3
Bob	−2.0	+0.2	−0.4	+0.5	+0.1	+0.3	...	$S_{2,1208}$	−1.2
Charlie	−2.0	+0.2	+2.7	+0.5	−7.2	−3.3	...	$S_{3,1208}$	−9.0
David	+0.5	+0.2	−0.4	+0.5	+0.1	+0.3	...	$S_{4,1208}$	+1.3
Eve	+0.5	+0.2	−0.4	−1.9	+0.1	+0.3	...	$S_{5,1208}$	−1.1
Fred	−2.0	+0.2	−0.4	−1.9	+0.1	−3.3	...	$S_{6,1208}$	−7.2
George	+0.5	+0.2	−0.4	−1.9	+0.1	+0.3	...	$S_{7,1208}$	−1.1
Henry	+0.5	+0.2	+2.7	+0.5	+0.1	−3.3	...	$S_{8,1208}$	+0.8
Copy	0	0	0	1	1	0	...	0	

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

The Tardos scheme: Scores

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

For each j, i, he calculates $S_{j,i}$ and $S_j(i) = S_j(i-1) + S_{j,i}$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(1208)$
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	...	−2.1	−19
Charlie	−2.0	+0.2	+2.7	+0.5	−7.2	−3.3	...	+0.5	+291
David	+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	−3.3	...	+0.5	+269
Copy	0	0	0	1	1	0	...	0	

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

The Tardos scheme: Accusation

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

Finally the distributor accuses all users j with $S_j(\ell) > Z$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(1208)$
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	...	−2.1	−19
Charlie	−2.0	+0.2	+2.7	+0.5	−7.2	−3.3	...	+0.5	+291
David	+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	−3.3	...	+0.5	+269
Copy	0	0	0	1	1	0	...	0	

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

TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Accusation

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

Finally the distributor accuses all users j with $S_j(\ell) > Z$

	0.20	0.05	0.88	0.79	0.98	0.09	...	0.18	$S_j(1208)$
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	...	−2.1	−19
Charlie	−2.0	+0.2	+2.7	+0.5	−7.2	−3.3	...	+0.5	+291
David	+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	−3.3	...	+0.5	+269
Copy	0	0	0	1	1	0	...	0	

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

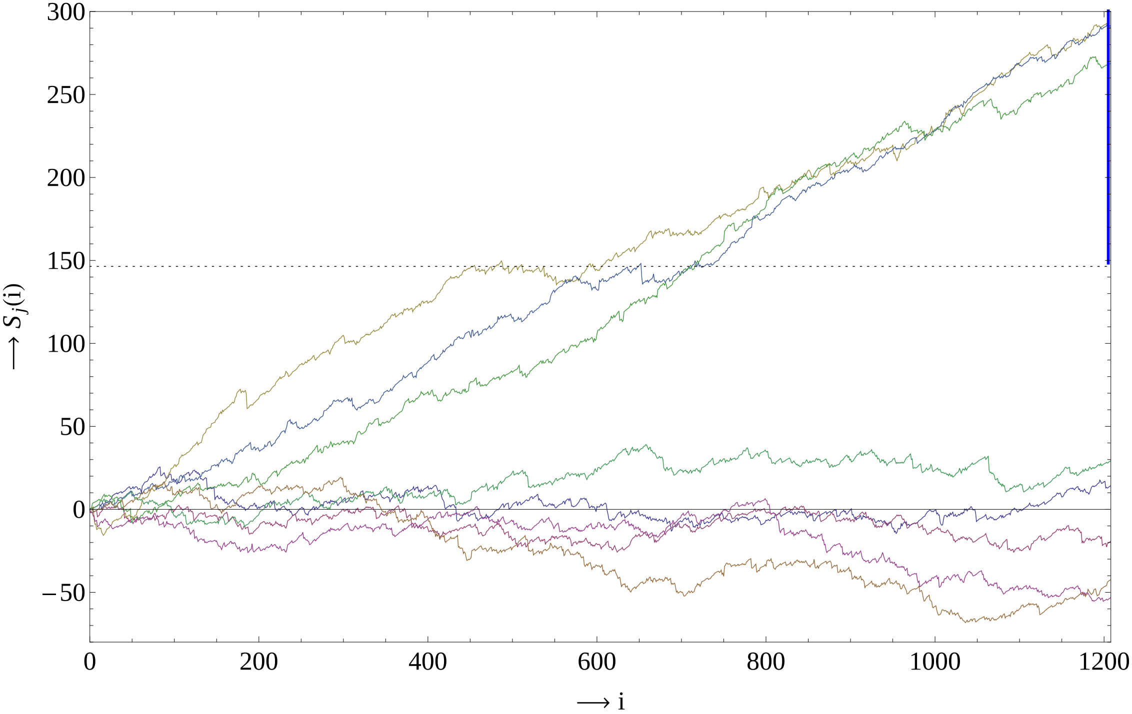
$$C^* = \{\text{Charlie, Eve, Henry}\}$$

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Accusation

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1-\delta]$.

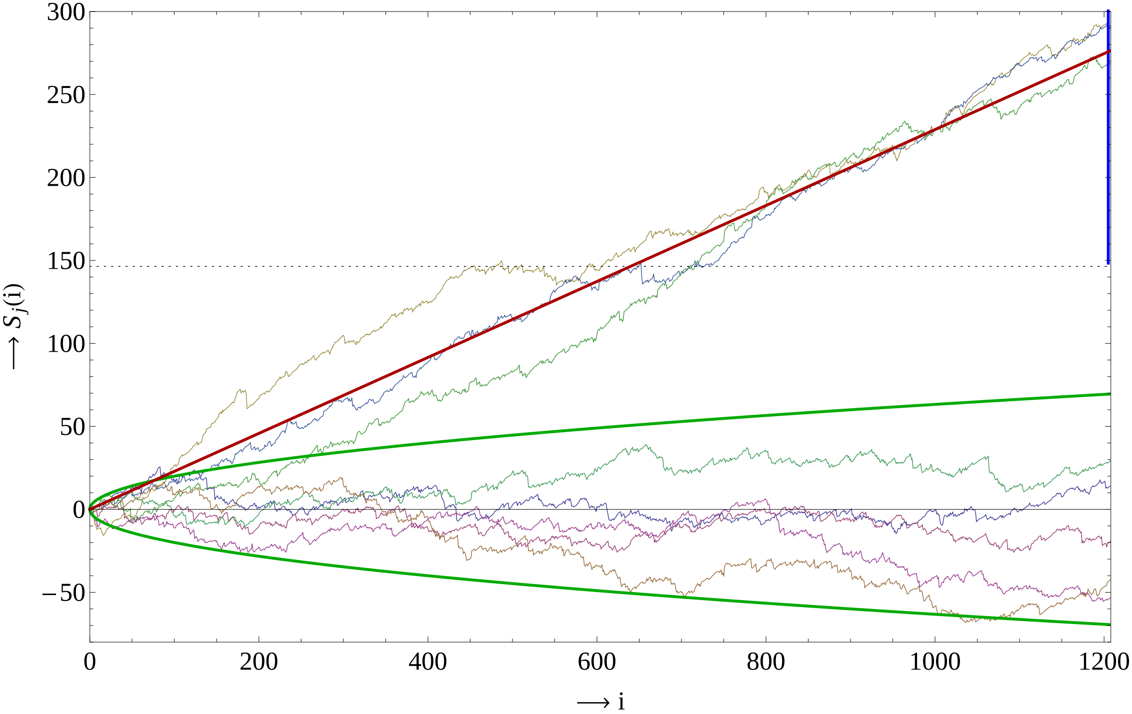
Finally the distributor accuses all users j with $S_j(\ell) > Z$



The Tardos scheme: Accusation

Let $n = 8$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.01$, $\ell = 1208$, $Z = 146$, $\delta = 0.0115$, $p_i \in [\delta, 1 - \delta]$.

Finally the distributor accuses all users j with $S_j(\ell) > Z$



TU/e Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Why does it work?

Why are no innocent users accused?

- All codewords are independent, so it is impossible to frame anyone.
- Scores for innocent users behave like random walks with zero drift.
- Proof: The probability that $S_j(\ell) > Z$ is sufficiently small.

Why are guilty users accused?

- If all pirates see the same symbol, then $S_C(i) = \sum_{j \in C} S_j(i)$ increases a lot.
- On other positions, pirates cannot significantly decrease $S_C(i)$.
- The total score $S_C(i)$ behaves like a random walk with $\tilde{\mu} \approx \frac{2}{\pi}$ drift.
- If $S_C(\ell) > cZ$ then at least one user is accused.
- Proof: The probability that $S_C(\ell) \leq cZ$ is sufficiently small.

Note: Never guarantee of catching multiple colluders!

Technische Universiteit Eindhoven University of Technology

The Tardos scheme: Why does it work?

Why are no innocent users accused?

- All codewords are independent, so it is impossible to frame anyone.
- Scores for innocent users behave like random walks with zero drift.
- Proof: The probability that $S_j(\ell) > Z$ is sufficiently small.

Why are guilty users accused?

- If all pirates see the same symbol, then $S_C(i) = \sum_{j \in C} S_j(i)$ increases a lot.
- On other positions, pirates cannot significantly decrease $S_C(i)$.
- The total score $S_C(i)$ behaves like a random walk with $\tilde{\mu} \approx \frac{2}{\pi}$ drift.
- If $S_C(\ell) > cZ$ then at least one user is accused.
- Proof: The probability that $S_C(\ell) \leq cZ$ is sufficiently small.

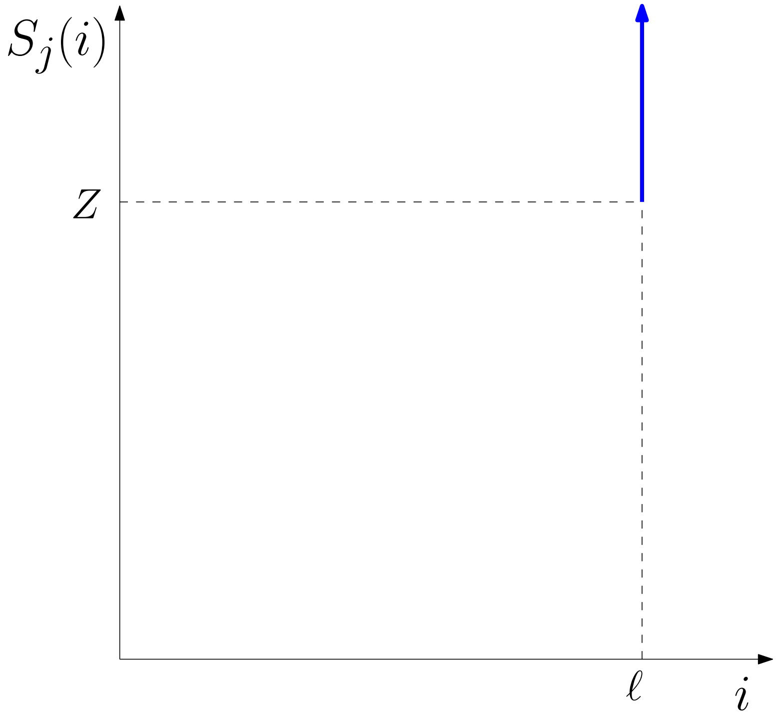
Note: Never guarantee of catching multiple colluders!

Technische Universiteit Eindhoven University of Technology

The dynamic Tardos scheme: Intro

Recall: Static Tardos scheme:

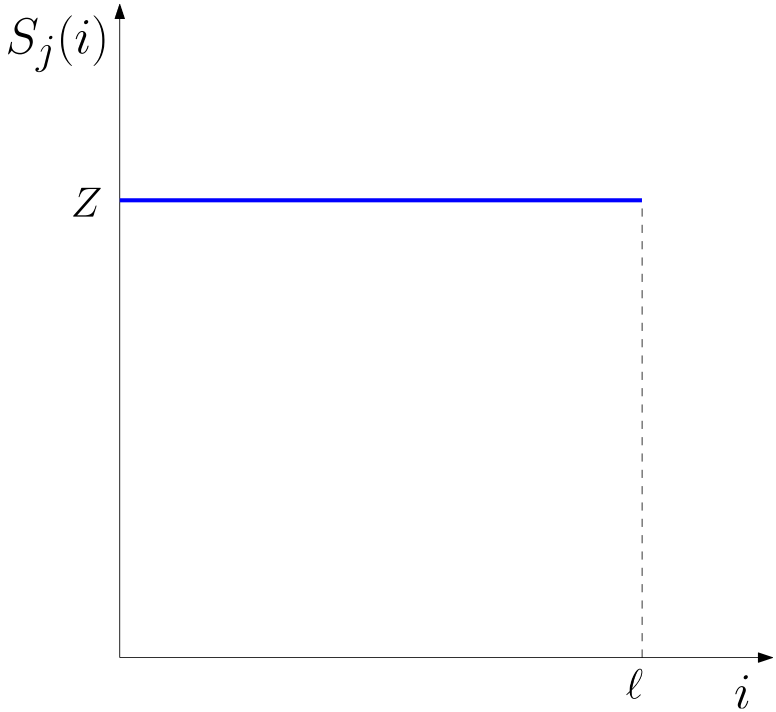
- At time ℓ, accuse users with $S_j(\ell) > Z$
- Catch at least one pirate at time ℓ with high probability



The dynamic Tardos scheme: Intro

New idea: Dynamic Tardos scheme:

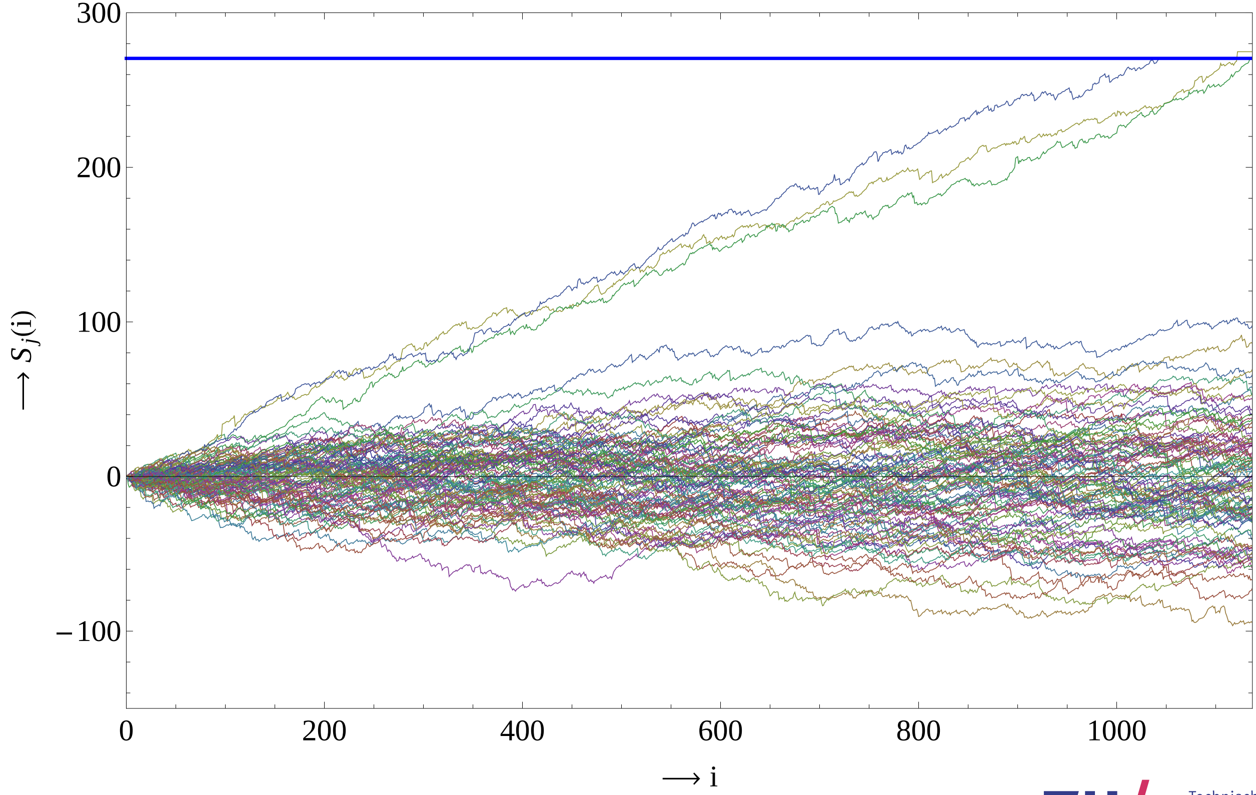
- At each time i, disconnect users with $S_j(i) > Z$
- Catch *all* pirates before time ℓ with high probability



The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

Strategy: Interleaving attack. Time needed: $t = 1137$.

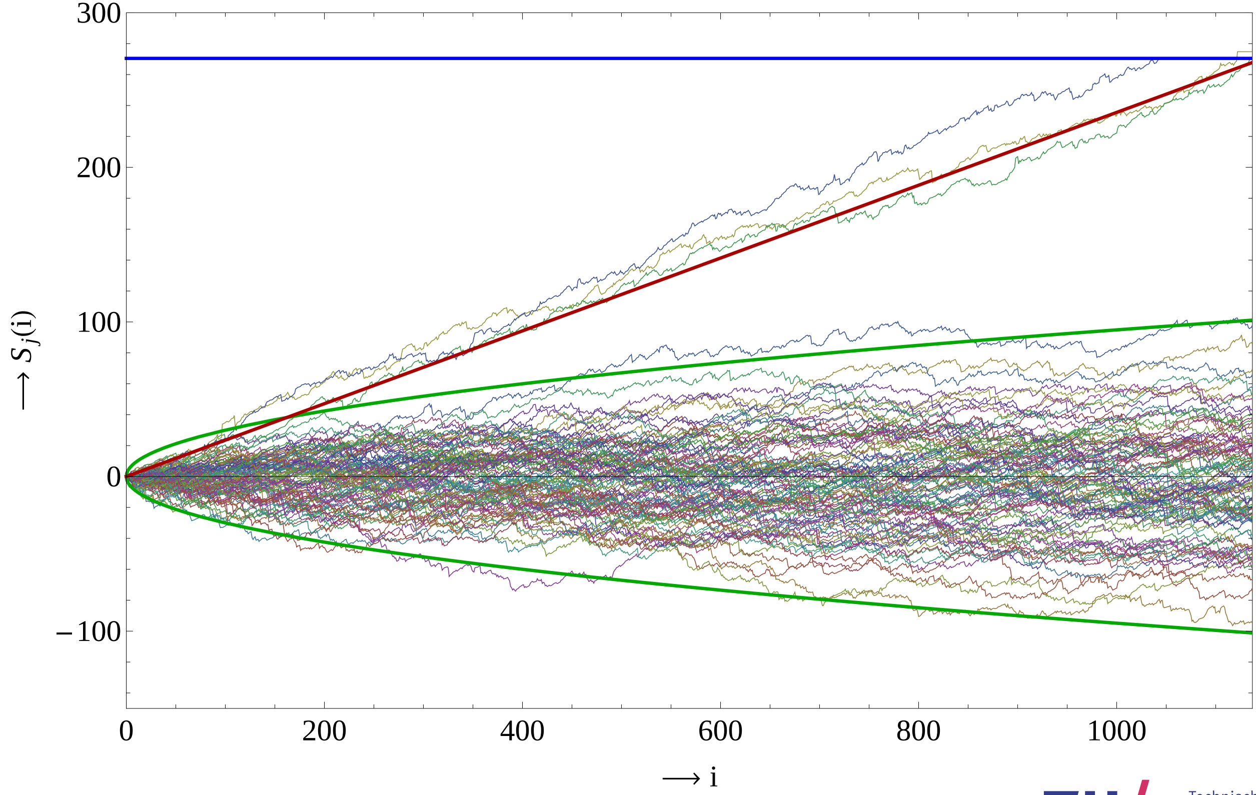


Technische Universiteit Eindhoven University of Technology

The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

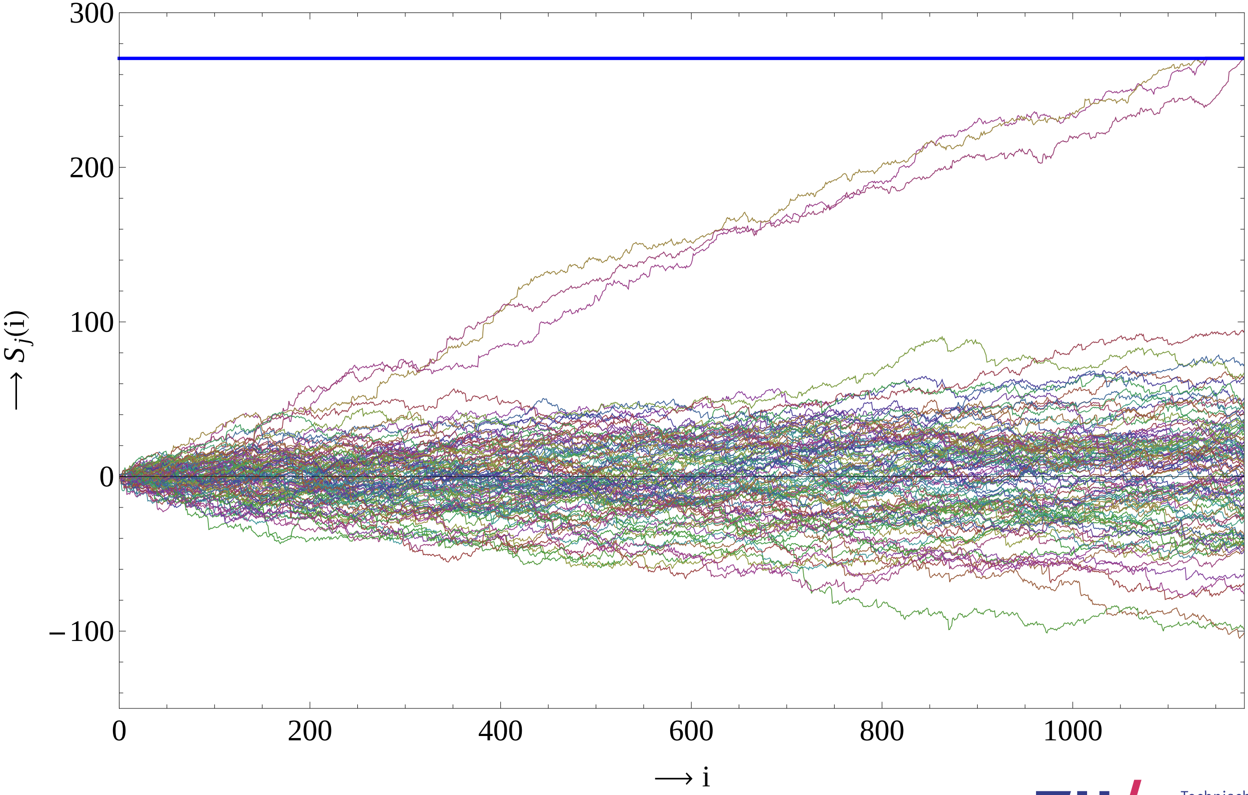
Strategy: Interleaving attack. Time needed: $t = 1137$.



The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

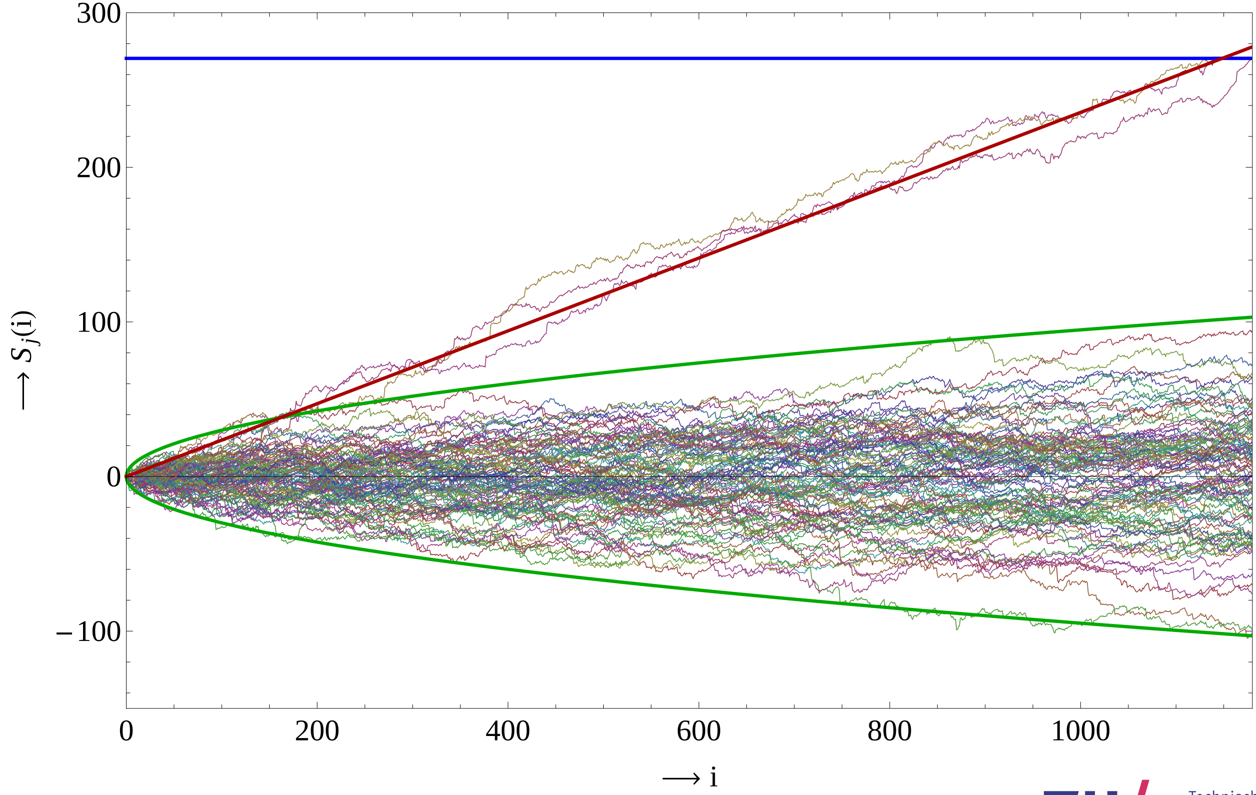
Strategy: Minority voting. Time needed: $t = 1180$.



The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

Strategy: Minority voting. Time needed: $t = 1180$.

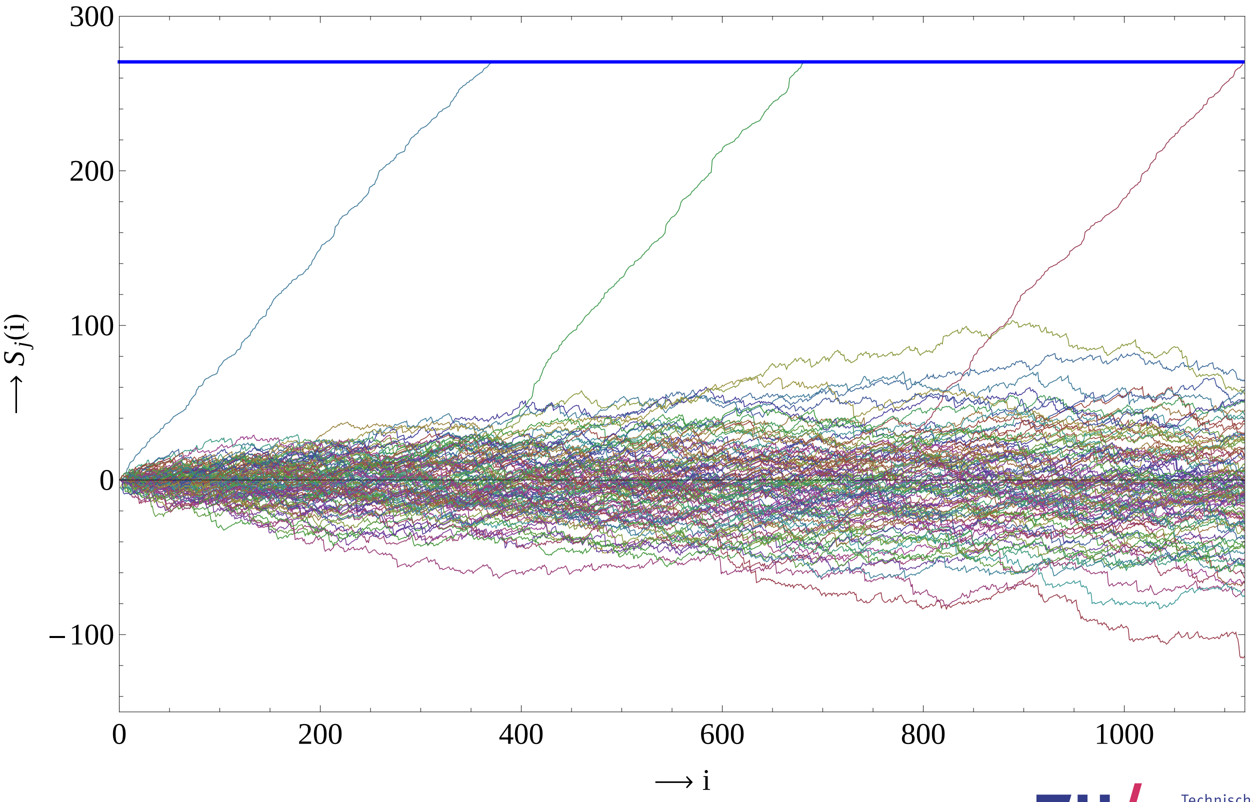


TU/e Technische Universiteit Eindhoven University of Technology

The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

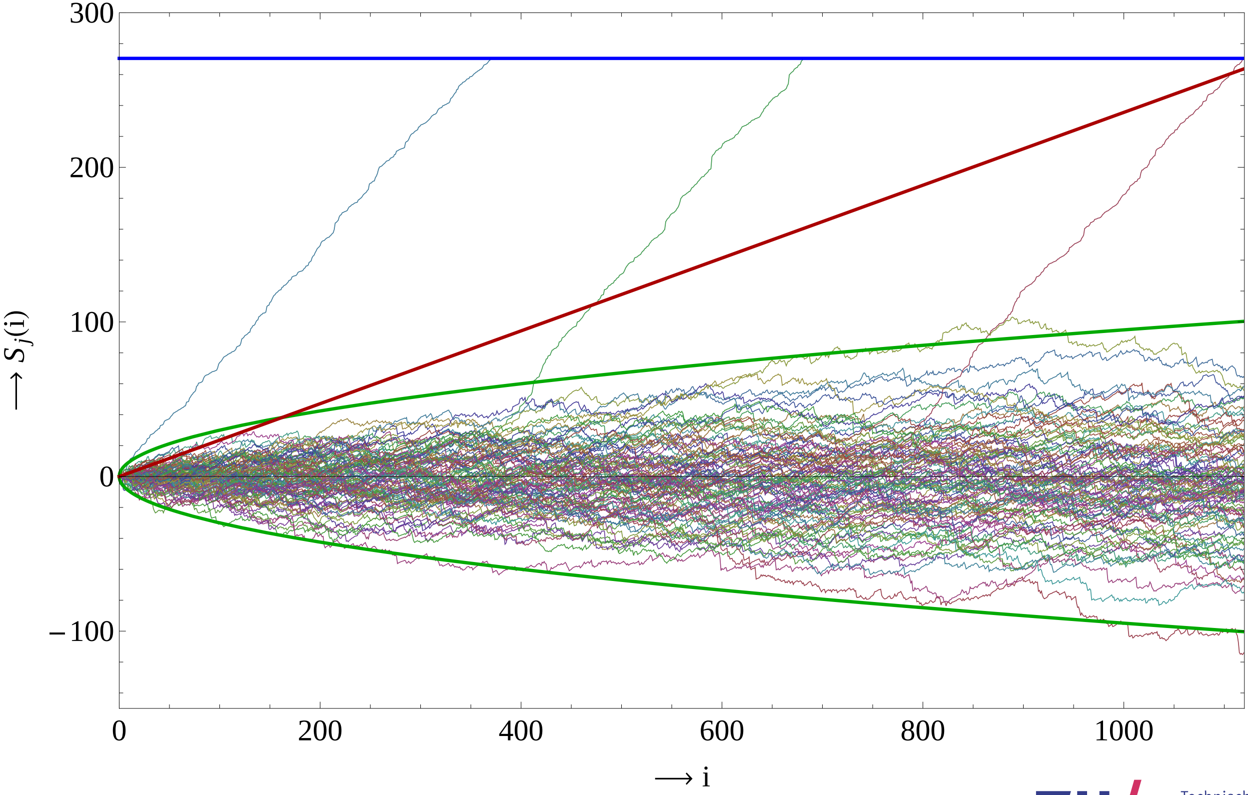
Strategy: Scapegoat strategy. Time needed: $t = 1120$.



The dynamic Tardos scheme: Example

Let $n = 100$, $c = 3$, $\epsilon_1 = \epsilon_2 = 0.001$, $\ell = 2285$, $Z = 270$, $\delta = 0.0123$, $p_i \in [\delta, 1-\delta]$.

Strategy: Scapegoat strategy. Time needed: $t = 1120$.



TU/e Technische Universiteit Eindhoven University of Technology

The dynamic Tardos scheme: Summary

Comparison with static Tardos scheme:

- Now certainty about catching all colluders!
- Slightly higher error probabilities/longer codelengths.
- Value ℓ only (rough) upper bound on time needed; usually $t \ll \ell$.
- Code can still be generated in advance.
- Downside: Need to know c in advance.

Technische Universiteit Eindhoven University of Technology

The dynamic Tardos scheme: Summary

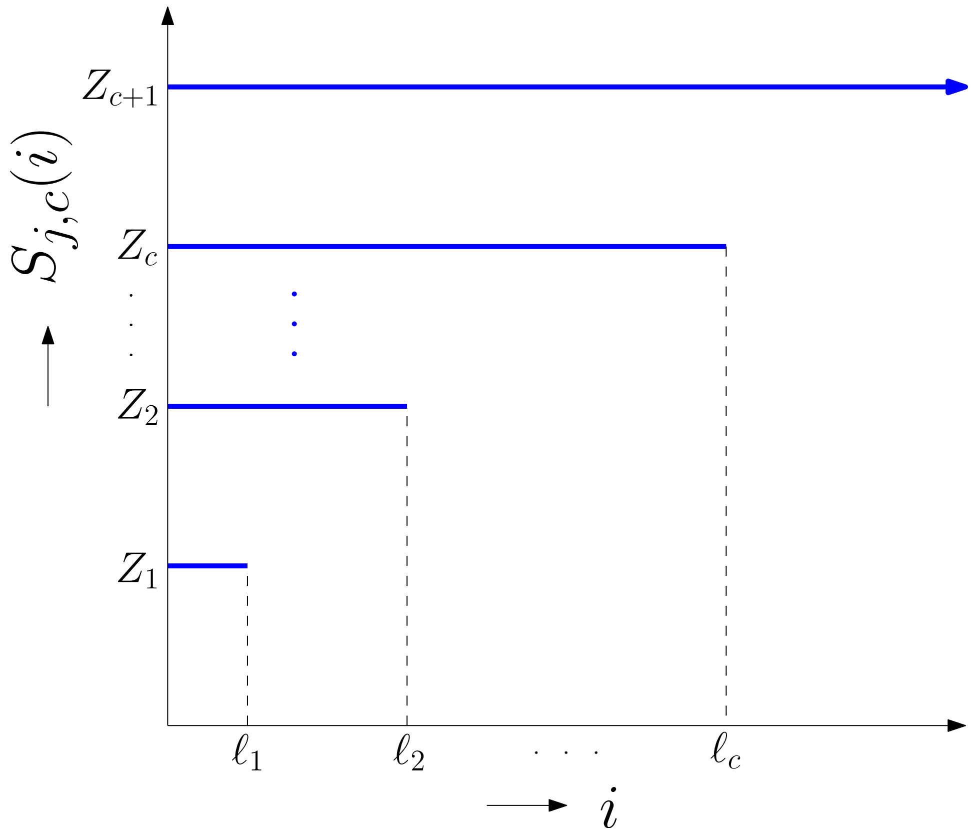
Comparison with static Tardos scheme:

- Now certainty about catching all colluders!
- Slightly higher error probabilities/longer codelengths.
- Value ℓ only (rough) upper bound on time needed; usually $t \ll \ell$.
- Code can still be generated in advance.
- **Downside: Need to know c in advance.**

TU/e Technische Universiteit Eindhoven University of Technology

The universal Tardos scheme: Intro

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



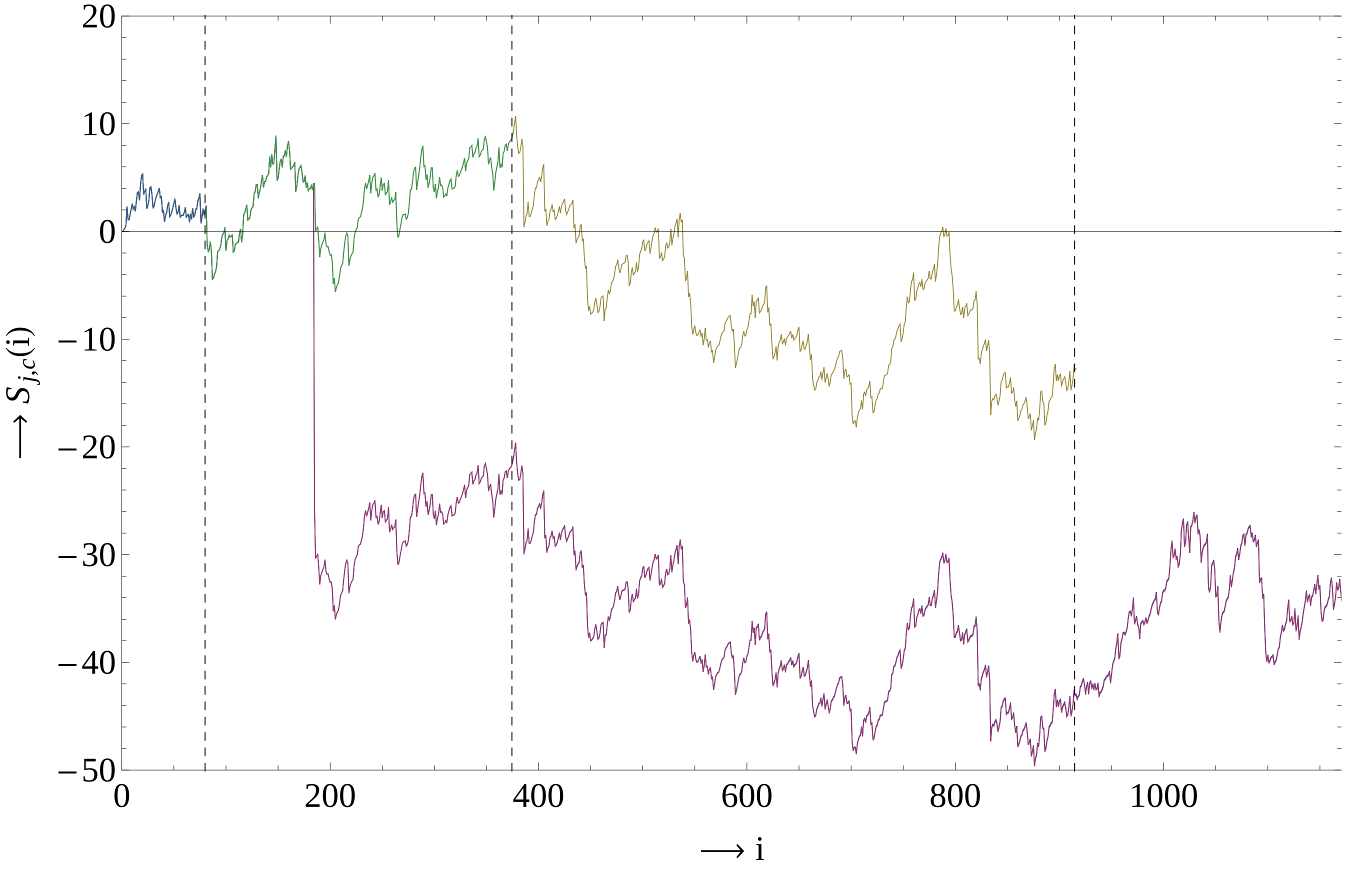
The universal Tardos scheme: Intro

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

- Symbols used for several values of c simultaneously.
- Some problems with making a c-universal code, but can be solved.
- Different score functions for different values of c
  - Keep scores for each user and each value of c: $S_{j,c}(i)$
- Codelength reduced from $\sum_c \ell_c = \mathcal{O}(c^3 \ln(n/\epsilon_1))$ to $\ell_c = \mathcal{O}(c^2 \ln(n/\epsilon_1))$.

The universal Tardos scheme: Example

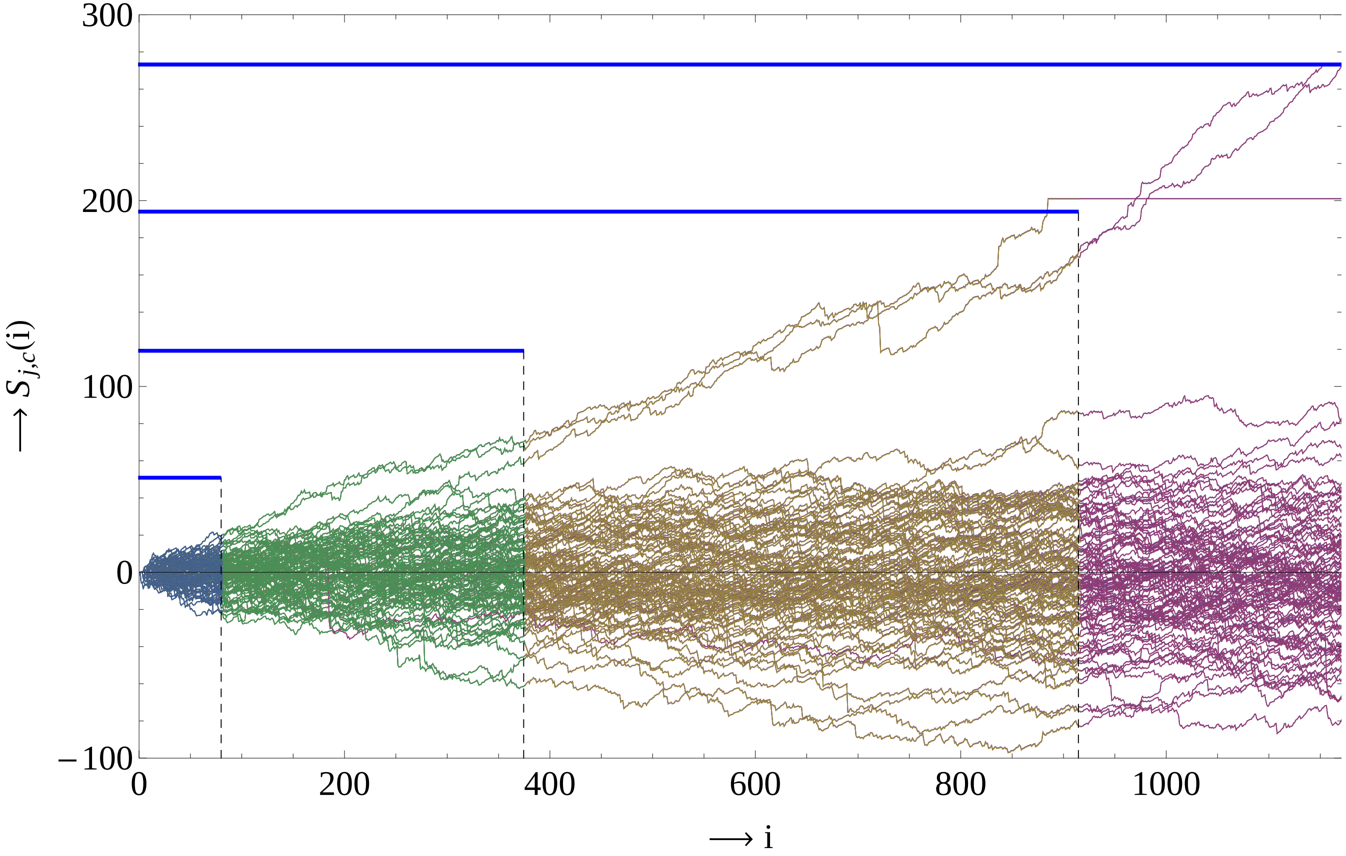
Keeping multiple scores per user: Mostly same and overlap, rarely different.



TU/e Technische Universiteit Eindhoven University of Technology

The universal Tardos scheme: Example

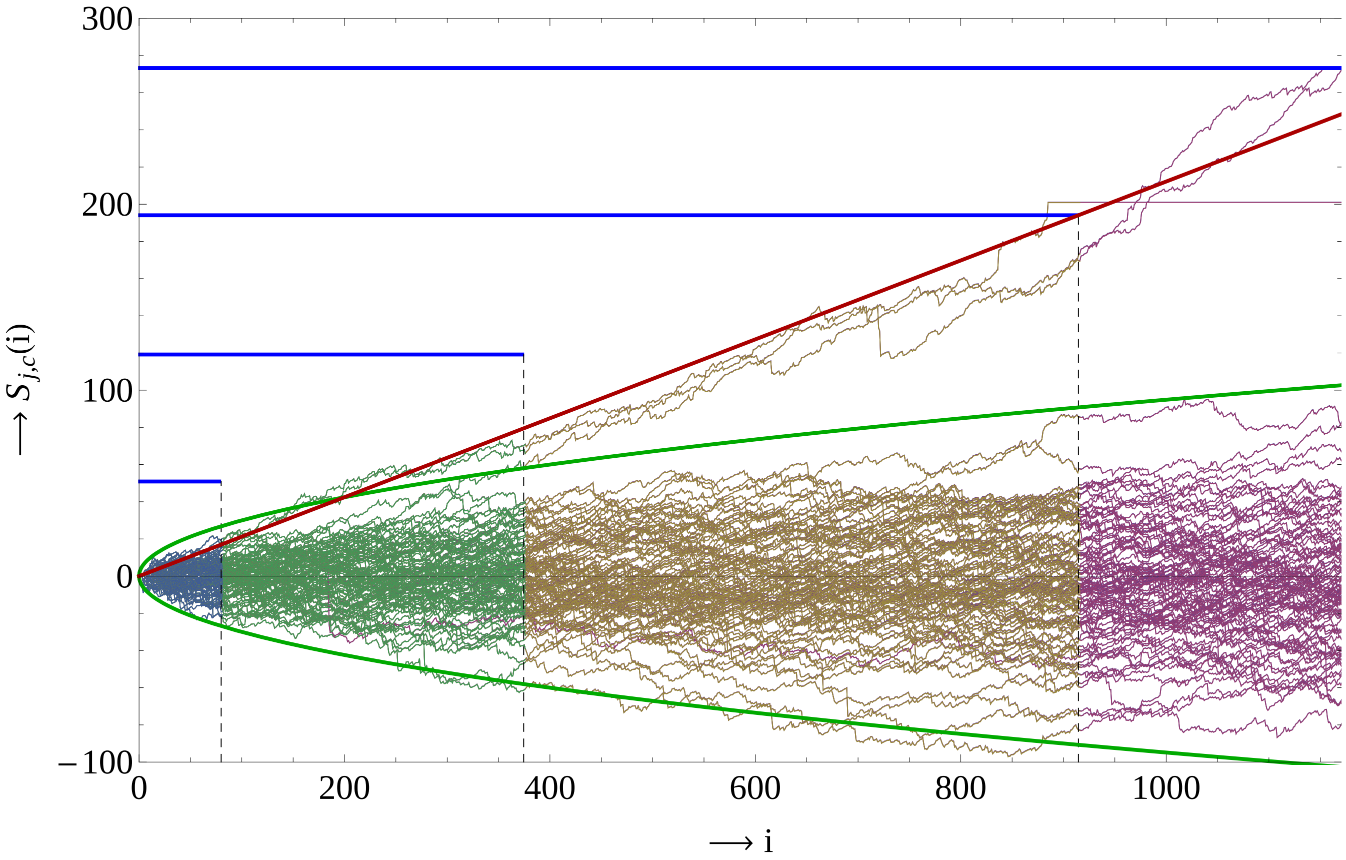
All scores of all users:



Technische Universiteit Eindhoven University of Technology

The universal Tardos scheme: Example

All scores of all users:



The universal Tardos scheme: Summary

Comparison with dynamic Tardos scheme: **No input c required**

- General algorithm: Can be applied for any coalition size.
- Code can still be generated in advance.
- Only downside: Need to keep scores per user and per c.

Comparison with the Tassa scheme: **Huge improvement**

- Shorter codelengths.
- Simpler code generation, accusation algorithm.
- Code can be generated in advance.
- More flexibility, in several ways.

Technische Universiteit Eindhoven University of Technology

The universal Tardos scheme: Summary

Comparison with dynamic Tardos scheme: **No input c required**

- General algorithm: Can be applied for any coalition size.
- Code can still be generated in advance.
- **Only downside: Need to keep scores per user and per c.**

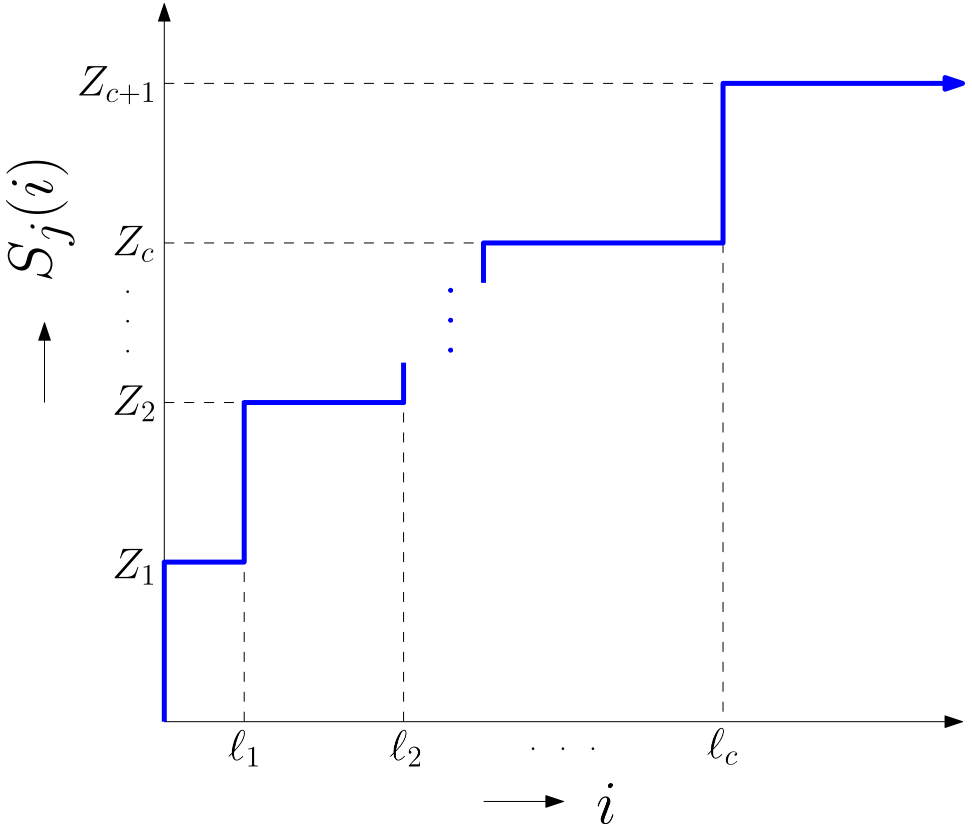
Comparison with the Tassa scheme: **Huge improvement**

- Shorter codelengths.
- Simpler code generation, accusation algorithm.
- Code can be generated in advance.
- More flexibility, in several ways.

Technische Universiteit Eindhoven University of Technology

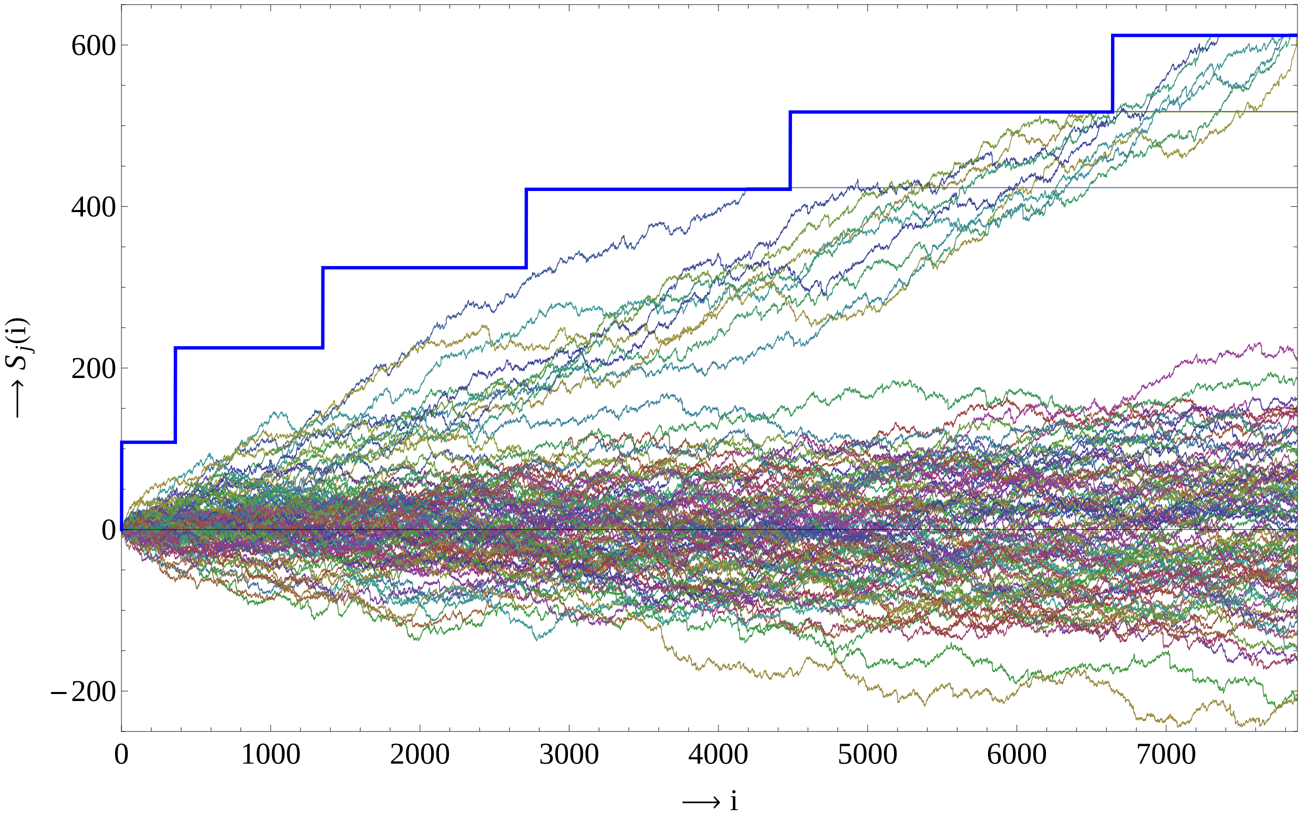
The staircase Tardos scheme: Intro

Alternative to universal Tardos scheme: Staircase Tardos scheme.



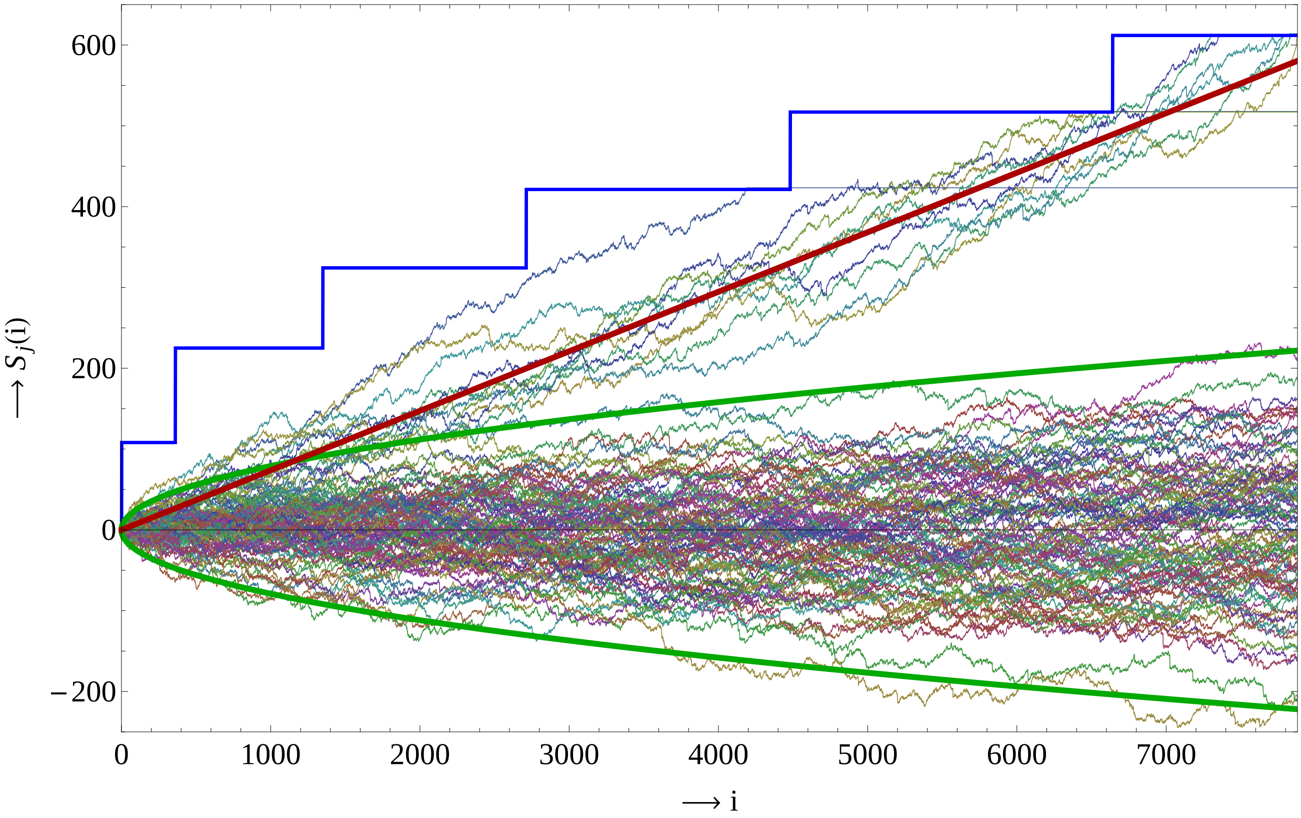
The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme.



The staircase Tardos scheme: Example

Alternative to universal Tardos scheme: Staircase Tardos scheme.



TU/e Technische Universiteit Eindhoven University of Technology

The staircase Tardos scheme: Summary

Comparison with universal Tardos scheme:

- Advantage: Keep only one score per user.
- Advantage: Slightly shorter codelengths.
- Disadvantage: Distribution $f(p)$ now depends on position i.
- Disadvantage: Less flexible.

TU/e Technische Universiteit Eindhoven University of Technology

Conclusion

Past work:

- October-December 2010: Literature study.
- January 2011: Invention of the dynamic Tardos scheme.
- March 2011: Invention of the universal Tardos scheme.
- April 2011: Improved results on the static Tardos scheme.
- May 2011: Invention of the staircase Tardos scheme.

Results:

- A report containing all of these results.
- A paper about the improved static Tardos scheme.
- An Irdeto patent on the dynamic Tardos schemes.
- Later: A paper about the dynamic Tardos schemes.

Questions

Thank you for your attention! Any questions?