

Optimal sequential fingerprinting: Wald vs. Tardos

Thijs Laarhoven

mail@thijs.com
http://www.thijs.com/

IH&MMSec 2015, Portland (OR), USA (June 18, 2015)

Problem: Illegal redistribution

User	C	эру	rigl	nte	d c	ont	ent	:									
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	
Boris	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	
Caroline	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	
Gábor	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	

Problem: Illegal redistribution

User	C	ору	rig	hte	d c	ont	ent	:									
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	
Boris	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	1	1	0	0	1	1	1	0	1	1	0	0	1	0	

User	C	ору	rig	hte	d c	ont	ent	t (f	ng	erp	rint	ed)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	

User	C	ору	rig	hte	d c	ont	ent	t (f	ng	erp	rint	ted)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	0	

TU/e

User	C	эру	rigl	hte	d c	ont	ent	t (f	ng	erp	rint	ted)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	0	

TU/e

User	C	эру	rigl	hte	d c	ont	ent	t (f	ng	erp	rint	ted)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0	0	

Problem: Collusion attacks

User	C	эру	/rig	hte	d c	ont	en	t (f	ng	erp	rint	ed)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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: Collusion attacks

User	C	ору	rig	nte	d c	ont	en	t (f	ing	erp	rint	ted)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	1	1	0	1	0	1	1	0	1	1	0	1	0	0	

Problem: Collusion attacks

User	C	ору	rig	hte	d c	ont	ent	t (f	ng	erp	rint	ted)				
Antonino	0	1	1	1	0	0	1	1	1	0	1	1	0	1	0	0	
Boris	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	
Caroline	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	
Gábor	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	
Сору	0	1	1	1	0	1	0	1	1	0	1	1	0	1	0	0	

User	C	эру	rig	hte	d c	ont	ent	t (f	ng	erp	rint	ted)				
Antonino	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Boris	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Caroline	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
David	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Eve	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Fred	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Gábor	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Henry	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Сору	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	

Solution: Collusion-resistant schemes

User	C	ору	rig	hte	d c	ont	ent	t (f	ing	erp	rint	ted)				
Antonino	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Boris	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Caroline	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
David	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Eve	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Fred	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Gábor	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Henry	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Сору	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	

1. An algorithm to construct collusion-resistant codes

User	C	ору	rig	hte	d c	ont	en	t (f	ing	erp	rint	ted)				
Antonino	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Boris	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Caroline	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
David	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Eve	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Fred	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Gábor	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Henry	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	
Сору	0	1	?	1	0	?	?	1	1	0	?	1	?	?	?	0	

- 1. An algorithm to construct collusion-resistant codes
- 2. An algorithm to trace pirate copies to colluders

User	Copyrighted content (fingerprinted)										
Antonino	?	? ?	?	? ?	?						
Boris	?	? ?	?	? ?	?						
Caroline	?	? ?	?	? ?	?						
David	?	? ?	?	? ?	?						
Eve	?	? ?	?	? ?	?						
Fred	?	? ?	?	? ?	?						
Gábor	?	? ?	?	? ?	?						
Henry	?	? ?	?	? ?	?						
Сору	?	? ?	?	? ?	?						

- 1. An algorithm to construct collusion-resistant codes
- 2. An algorithm to trace pirate copies to colluders



User	Copyrighted content (fingerprinted)	
Antonino		
Boris		
Caroline	. .	
David	V	
Eve		
Fred		
Gábor		
Henry		
Сору	у	

- 1. An algorithm to construct collusion-resistant codes
- 2. An algorithm to trace pirate copies to colluders

- 1. An algorithm to construct collusion-resistant codes
- 2. An algorithm to trace pirate copies to colluders



Tardos' scheme

1. An algorithm to construct collusion-resistant codes

2. An algorithm to trace pirate copies to colluders

- 1. An algorithm to construct collusion-resistant codes
 - 1a. For each segment *i*, generate $p_i \sim F$.
 - 1b. For each segment i, user j, choose $X_{j,i} = 1$ with prob. p_i .
- 2. An algorithm to trace pirate copies to colluders

- 1. An algorithm to construct collusion-resistant codes
 - 1a. For each segment i, generate $p_i \sim F$.
 - 1b. For each segment i, user j, choose $X_{i,i} = 1$ with prob. p_i .
- 2. An algorithm to trace pirate copies to colluders
 - 2a. For each segment i, user j, calculate $S_{j,i} = g(X_{j,i}, y_i, p_i)$.
 - 2b. For each user j, accuse user j iff $\sum_i S_{j,i}$ is "large".

p _i	p_1	<i>p</i> ₂	<i>p</i> ₃	<i>p</i> ₄	<i>p</i> ₅	 <i>p</i> ₁₂₀₀
Antonino	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	 $X_{1,1200}$
Boris	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	 $X_{2,1200}$
Caroline	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	 $X_{3,1200}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	 $X_{4,1200}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	 $X_{5,1200}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	 $X_{6,1200}$
Gábor	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	 $X_{7,1200}$
Henry	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	 X _{8,1200}
Сору	<i>y</i> ₁	<i>y</i> ₂	<i>y</i> 3	<i>y</i> ₄	<i>y</i> ₅	 <i>y</i> ₁₂₀₀

1a. For each segment *i*, generate $p_i \sim F$.

p _i	p_1	p_2	<i>p</i> ₃	<i>p</i> ₄	<i>p</i> ₅	 p_{1200}
Antonino	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	 $X_{1,1200}$
Boris	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	 $X_{2,1200}$
Caroline	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	 $X_{3,1200}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	 $X_{4,1200}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	 $X_{5,1200}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	 $X_{6,1200}$
Gábor	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	 $X_{7,1200}$
Henry	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	 X _{8,1200}
Сору	<i>y</i> 1	<i>y</i> 2	<i>y</i> 3	<i>y</i> 4	<i>y</i> ₅	 <i>y</i> 1200

1a. For each segment *i*, generate $p_i \sim F$.

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	X _{1,1}	X _{1,2}	X _{1,3}	X _{1,4}	X _{1,5}	 X _{1,1200}
Boris	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	 $X_{2,1200}$
Caroline	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	 $X_{3,1200}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	 $X_{4,1200}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	 $X_{5,1200}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	 $X_{6,1200}$
Gábor	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	 $X_{7,1200}$
Henry	$X_{8,1}$	<i>X</i> _{8,2}	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	 X _{8,1200}
Сору	<i>y</i> ₁	<i>y</i> ₂	<i>y</i> 3	<i>y</i> 4	<i>y</i> 5	 <i>y</i> 1200

Tardos' scheme

1b. For each segment i, user j, choose $X_{j,i} = 1$ with prob. p_i .

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	$X_{1,1}$	$X_{1,2}$	X _{1,3}	X _{1,4}	$X_{1,5}$	 X _{1,1200}
Boris	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	 $X_{2,1200}$
Caroline	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	 $X_{3,1200}$
David	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	 $X_{4,1200}$
Eve	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	 $X_{5,1200}$
Fred	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	 $X_{6,1200}$
Gábor	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	 $X_{7,1200}$
Henry	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	 X _{8,1200}
Сору	<i>y</i> 1	<i>y</i> ₂	<i>y</i> 3	<i>y</i> 4	<i>y</i> 5	 <i>У</i> 1200

1b. For each segment i, user j, choose $X_{j,i} = 1$ with prob. p_i .

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	0	0	1	1	1	 0
Boris	1	0	1	1	1	 1
Caroline	1	0	0	1	0	 0
David	0	0	1	1	1	 0
Eve	0	0	1	0	1	 0
Fred	1	0	1	0	1	 0
Gábor	0	0	1	0	1	 0
Henry	1	0	0	0	1	 0
Сору	<i>y</i> 1	<i>y</i> ₂	<i>y</i> 3	<i>y</i> 4	<i>y</i> 5	 <i>y</i> 1200

Tardos' scheme

The copy is distributed and detected by the tracer.

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	0	0	1	1	1	 0
Boris	1	0	1	1	1	 1
Caroline	1	0	0	1	0	 0
David	0	0	1	1	1	 0
Eve	0	0	1	0	1	 0
Fred	1	0	1	0	1	 0
Gábor	0	0	1	0	1	 0
Henry	1	0	0	0	1	 0
Сору	0	0	0	1	1	 0

 $Coalition = \{Caroline, Eve, Henry\}$

Tardos' scheme

2a. For each segment i, user j, calculate $S_{i,i} = g(X_{i,i}, y_i, p_i)$.

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	0	0	1	1	1	 0
Boris	1	0	1	1	1	 1
Caroline	1	0	0	1	0	 0
David	0	0	1	1	1	 0
Eve	0	0	1	0	1	 0
Fred	1	0	1	0	1	 0
Gábor	0	0	1	0	1	 0
Henry	1	0	0	0	1	 0
Сору	0	0	0	1	1	 0

 $\mathsf{Coalition} = \{\mathsf{Caroline}, \mathsf{Eve}, \mathsf{Henry}\}$

Tardos' scheme

2a. For each segment i, user j, calculate $S_{i,i} = g(X_{i,i}, y_i, p_i)$.

p _i	0.20	0.05	0.88	0.79	0.98	 0.18
Antonino	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5
Boris	-2.0	+0.2	-0.4	+0.5	+0.1	 -2.1
Caroline	-2.0	+0.2	+2.7	+0.5	-7.2	 +0.5
David	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5
Eve	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5
Fred	-2.0	+0.2	-0.4	-1.9	+0.1	 +0.5
Gábor	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5
Henry	-2.0	+0.2	+2.7	-1.9	+0.1	 +0.5
Сору	0	0	0	1	1	 0

 $\mathsf{Coalition} = \{\mathsf{Caroline}, \mathsf{Eve}, \mathsf{Henry}\}$

Tardos' scheme

2b. For each user j, accuse user j iff $\sum_{i} S_{j,i}$ is "large".

p _i	0.20	0.05	0.88	0.79	0.98	 0.18	$\sum_{i} S_{j,i}$
Antonino	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	0
Boris	-2.0	+0.2	-0.4	+0.5	+0.1	 -2.1	0
Caroline	-2.0	+0.2	+2.7	+0.5	-7.2	 +0.5	0
David	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	0
Eve	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	0
Fred	-2.0	+0.2	-0.4	-1.9	+0.1	 +0.5	0
Gábor	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	0
Henry	-2.0	+0.2	+2.7	-1.9	+0.1	 +0.5	0
Сору	0	0	0	1	1	 0	

 $Coalition = \{Caroline, Eve, Henry\}$

Tardos' scheme

2b. For each user j, accuse user j iff $\sum_{i} S_{j,i}$ is "large".

p _i	0.20	0.05	0.88	0.79	0.98	 0.18	$\sum_{i} S_{j,i}$
Antonino	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	+14
Boris	-2.0	+0.2	-0.4	+0.5	+0.1	 -2.1	-19
Caroline	-2.0	+0.2	+2.7	+0.5	-7.2	 +0.5	+291
David	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	+29
Eve	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	+292
Fred	-2.0	+0.2	-0.4	-1.9	+0.1	 +0.5	-53
Gábor	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	-42
Henry	-2.0	+0.2	+2.7	-1.9	+0.1	 +0.5	+269
Сору	0	0	0	1	1	 0	-

 $Coalition = \{Caroline, Eve, Henry\}$

Tardos' scheme

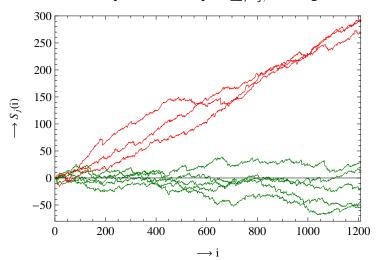
2b. For each user j, accuse user j iff $\sum_{i} S_{i,i}$ is "large".

					• • •		
p _i	0.20	0.05	0.88	0.79	0.98	 0.18	$\sum_{i} S_{j,i}$
Antonino	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	+14
Boris	-2.0	+0.2	-0.4	+0.5	+0.1	 -2.1	-19
Caroline	-2.0	+0.2	+2.7	+0.5	-7.2	 +0.5	+291
David	+0.5	+0.2	-0.4	+0.5	+0.1	 +0.5	+29
Eve	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	+292
Fred	-2.0	+0.2	-0.4	-1.9	+0.1	 +0.5	-53
Gábor	+0.5	+0.2	-0.4	-1.9	+0.1	 +0.5	-42
Henry	-2.0	+0.2	+2.7	-1.9	+0.1	 +0.5	+269
Сору	0	0	0	1	1	 0	

 $\begin{aligned} & \mathsf{Coalition} = \{\mathsf{Caroline}, \mathsf{Eve}, \mathsf{Henry}\} \\ & \mathsf{Accused} = \{\mathsf{Caroline}, \mathsf{Eve}, \mathsf{Henry}\} \end{aligned}$

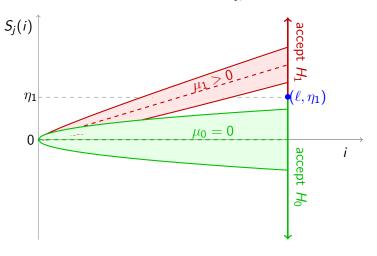
Tardos' scheme

2b. For each user j, accuse user j iff $\sum_{i} S_{i,i}$ is "large".



Tardos' scheme

2b. For each user j, accuse user j iff $\sum_{i} S_{j,i}$ is "large".

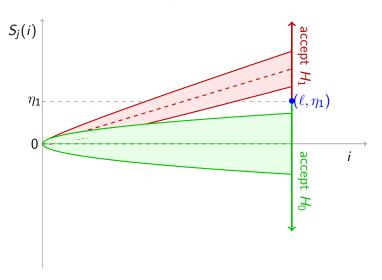




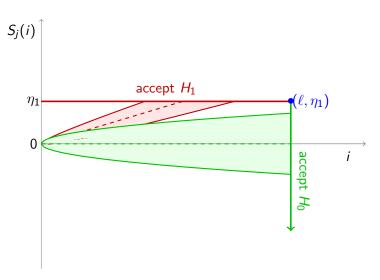
Tardos' scheme Non-adaptive solution

- Proposed by Tardos [STOC 2003]
- · Later related to hypothesis testing
- Neyman-Pearson lemma: this strategy is optimal
- Asymptotic code length: $\ell \sim 2c^2 \ln n$
- Situation very well understood

Tardos' scheme Non-adaptive solution



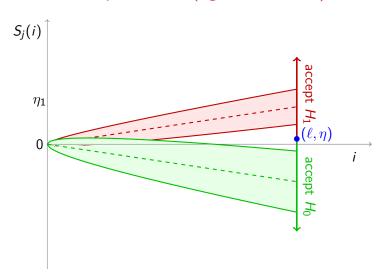
Tardos' scheme Sequential solution



TU/e

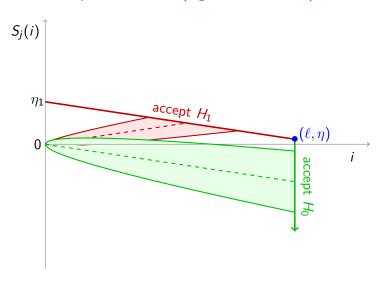
Tardos' scheme

Non-adaptive solution (log-likelihood scores)



Tardos' scheme

Sequential solution (log-likelihood scores)



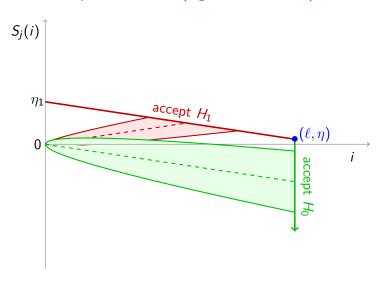


Tardos' scheme Sequential solution

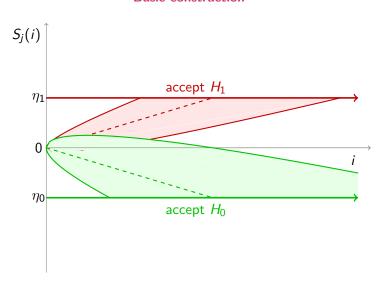
- Proposed by Laarhoven et al. [IEEE T-IT 2013]
- Efficient solution, but no optimality result
- Asymptotic code length: $\ell \sim 2c^2 \ln n$
- Situation not very well understood

Tardos' scheme

Sequential solution (log-likelihood scores)



Wald's scheme Basic construction

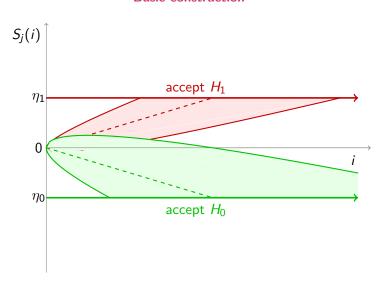




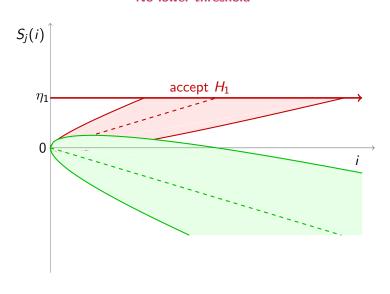
Wald's scheme Outline

- Proposed by Wald [Ann. Math. Stat. 1945]
- No guaranteed termination time
- Out of all sequential tests, Wald's minimizes $\mathbb{E}[T|H_{0,1}]$
- Optimal for arbitrary parameters
- Asymptotic code length: $\ell \sim 2c^2 \ln n$
- Studied since the 1940's, well understood

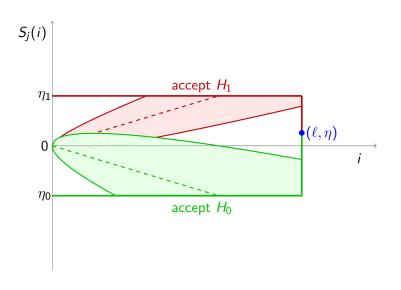
Wald's scheme Basic construction



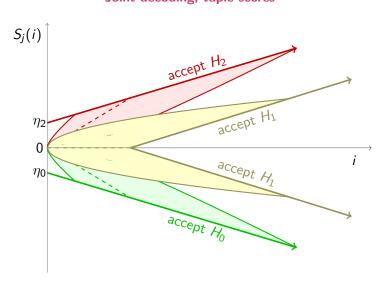
Wald's scheme No lower threshold



Wald's scheme Truncation at time ℓ

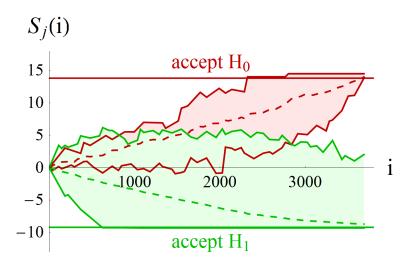


Wald's scheme Joint decoding, tuple scores



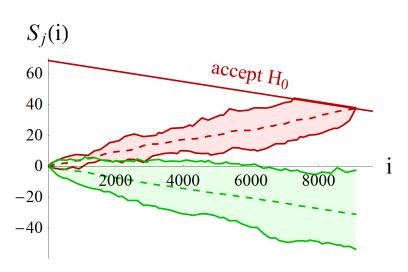
Comparison

Wald's scheme (interleaving attack)



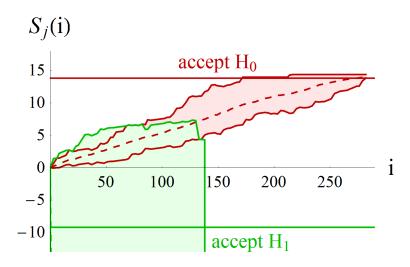
Comparison

Tardos' scheme (interleaving attack)



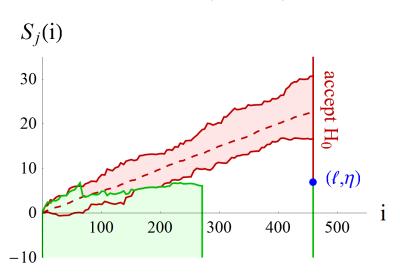
Comparison

Wald's scheme (all-1 attack)



Comparison

Tardos' scheme (all-1 attack)





Conclusions

- Proper way to handle sequential setting: use Wald's scheme
- Optimality guaranteed for arbitrary parameters
- Variants well studied in decades of research
- Easier to choose parameters than other schemes
- No guaranteed decision at time $\ell \Leftrightarrow \mathsf{No}$ false negatives

Non-adaptive decoding	Sequential decoding
Neyman-Pearson lemma	Wald's scheme

Questions?