# From Collusion-Resistant Traitor Tracing to Efficient Probabilistic Group Testing

Thijs Laarhoven

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

Eindhoven, The Netherlands
(December 9, 2013)

# Outline

Collusion-resistant traitor tracing
- Introduction
- Score-based construction
- Fighting against specific attacks
- Results

Efficient probabilistic group testing
- Introduction
- A traitor-tracing based solution
- Results

Conclusion

# Collusion-resistant traitor tracing

## Illegal redistribution

| User | Copyrighted content | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |

# Collusion-resistant traitor tracing

## Illegal redistribution

| User | Copyrighted content | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | ... |

# Collusion-resistant traitor tracing

## Embedding fingerprints

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |

# Collusion-resistant traitor tracing

## Embedding fingerprints

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

TU/e

# Collusion-resistant traitor tracing

## Embedding fingerprints

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | **0** | 1 | 0 | **1** | **0** | 1 | 1 | 0 | **1** | 1 | **1** | **0** | **0** | 0 | ... |

TU/e

# Collusion-resistant traitor tracing

## Embedding fingerprints

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | **0** | 1 | 0 | **1** | **0** | 1 | 1 | 0 | **1** | 1 | **1** | **0** | **0** | 0 | ... |

# Collusion-resistant traitor tracing

## Collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |

# Collusion-resistant traitor tracing

## Collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | ... |

TU/e

# Collusion-resistant traitor tracing

## Collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | **1** | 1 | 0 | **1** | **0** | 1 | 1 | 0 | **1** | 1 | **0** | **1** | **0** | 0 | ... |

TU/e

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | ? | 1 | 0 | ? | ? | 1 | 1 | 0 | ? | 1 | ? | ? | ? | 0 | ... |

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 0 | 1 | ? | 1 | 0 | ? | ? | 1 | 1 | 0 | ? | 1 | ? | ? | ? | 0 | ... |

1. An algorithm to construct collusion-resistant codes

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | ... |
| Copy | 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

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

| User | Copyrighted content (fingerprinted) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Antonino | ? | ? | ? | ? | ? | ? | ? | ... |
| Boris | ? | ? | ? | ? | ? | ? | ? | ... |
| Caroline | ? | ? | ? | ? | ? | ? | ? | ... |
| David | ? | ? | ? | ? | ? | ? | ? | ... |
| Eve | ? | ? | ? | ? | ? | ? | ? | ... |
| Fred | ? | ? | ? | ? | ? | ? | ? | ... |
| Gábor | ? | ? | ? | ? | ? | ? | ? | ... |
| Henry | ? | ? | ? | ? | ? | ? | ? | ... |
| Copy | ? | ? | ? | ? | ? | ? | ? | ... |

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

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

| User | Copyrighted content (fingerprinted) | |
|---|---|---|
| Antonino | | ... |
| Boris | | ... |
| Caroline | | ... |
| David | $X \in \{0,1\}^{n \times \ell}$ | ... |
| Eve | | ... |
| Fred | | ... |
| Gábor | | ... |
| Henry | | ... |
| Copy | $y \in \{0,1\}^{\ell}$ | ... |

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

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

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

# Collusion-resistant traitor tracing

## Schemes resistant against collusion attacks

1. An algorithm to construct collusion-resistant codes

2. An algorithm to trace pirate copies to colluders

# Score-based construction

## Overview

1. An algorithm to construct collusion-resistant codes

2. An algorithm to trace pirate copies to colluders

# Score-based construction

## Overview

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

# Score-based construction

## Overview

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
   - 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".

TU/e

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

$\ell = 100c^2 \ln n$ [Tar'03]

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

$\ell \sim 4\pi^2 c^2 \ln n$ [S+'06]

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

$\ell \sim 2\pi^2 c^2 \ln n$ [BT'08]

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

$$\ell \sim \pi^2 c^2 \ln n \quad \text{[S+'08]}$$

# Score-based construction

### Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

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

$$\ell \sim \tfrac{1}{2}\pi^2 c^2 \ln n \quad \text{[LdW'13]}$$

# Score-based construction

## Arbitrary attacks

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
   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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)/p_i & (X_{j,i}, y_i) = (1,1) \end{cases}$$

# Score-based construction

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)/p_i & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$\ell \sim 2c^2 \ln n$ [OSD'13]

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | $X_{1,1}$ | $X_{1,2}$ | $X_{1,3}$ | $X_{1,4}$ | $X_{1,5}$ | $\dots$ | $X_{1,\ell}$ |
| Boris | $X_{2,1}$ | $X_{2,2}$ | $X_{2,3}$ | $X_{2,4}$ | $X_{2,5}$ | $\dots$ | $X_{2,\ell}$ |
| Caroline | $X_{3,1}$ | $X_{3,2}$ | $X_{3,3}$ | $X_{3,4}$ | $X_{3,5}$ | $\dots$ | $X_{3,\ell}$ |
| David | $X_{4,1}$ | $X_{4,2}$ | $X_{4,3}$ | $X_{4,4}$ | $X_{4,5}$ | $\dots$ | $X_{4,\ell}$ |
| Eve | $X_{5,1}$ | $X_{5,2}$ | $X_{5,3}$ | $X_{5,4}$ | $X_{5,5}$ | $\dots$ | $X_{5,\ell}$ |
| Fred | $X_{6,1}$ | $X_{6,2}$ | $X_{6,3}$ | $X_{6,4}$ | $X_{6,5}$ | $\dots$ | $X_{6,\ell}$ |
| Gábor | $X_{7,1}$ | $X_{7,2}$ | $X_{7,3}$ | $X_{7,4}$ | $X_{7,5}$ | $\dots$ | $X_{7,\ell}$ |
| Henry | $X_{8,1}$ | $X_{8,2}$ | $X_{8,3}$ | $X_{8,4}$ | $X_{8,5}$ | $\dots$ | $X_{8,\ell}$ |
| Copy | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | $\dots$ | $y_\ell$ |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |
| Copy | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | ... | $y_\ell$ |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | 1 | 0 | 0 | 1 | 0 | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | 0 | 0 | 1 | 0 | 1 | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | 1 | 0 | 0 | 0 | 1 | ... | 0 |
| Copy | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | ... | $y_\ell$ |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | $y_1$ | $y_2$ | $y_3$ | $y_4$ | $y_5$ | ... | $y_\ell$ |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |

TU/e

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |
| All-1 | 1 | 0 | 1 | 1 | 1 | ... | 0 |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |
| All-1 | 1 | 0 | 1 | 1 | 1 | ... | 0 |
| Minority | 0 | 0 | 1 | 1 | 0 | ... | 0 |

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |
| All-1 | 1 | 0 | 1 | 1 | 1 | ... | 0 |
| Minority | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Majority | 1 | 0 | 0 | 0 | 1 | ... | 0 |

TU/e

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |
| All-1 | 1 | 0 | 1 | 1 | 1 | ... | 0 |
| Minority | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Majority | 1 | 0 | 0 | 0 | 1 | ... | 0 |
| Coin-flip | 1 | 0 | 1 | 0 | 0 | ... | 0 |

TU/e

# Fighting against specific attacks

## What can pirates do?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Antonino | . | . | . | . | . | ... | . |
| Boris | . | . | . | . | . | ... | . |
| Caroline | **1** | 0 | **0** | **1** | **0** | ... | 0 |
| David | . | . | . | . | . | ... | . |
| Eve | **0** | 0 | **1** | **0** | **1** | ... | 0 |
| Fred | . | . | . | . | . | ... | . |
| Gábor | . | . | . | . | . | ... | . |
| Henry | **1** | 0 | **0** | **0** | **1** | ... | 0 |
| Copy | 0/1 | 0 | 0/1 | 0/1 | 0/1 | ... | 0 |
| All-1 | 1 | 0 | 1 | 1 | 1 | ... | 0 |
| Minority | 0 | 0 | 1 | 1 | 0 | ... | 0 |
| Majority | 1 | 0 | 0 | 0 | 1 | ... | 0 |
| Coin-flip | 1 | 0 | 1 | 0 | 0 | ... | 0 |
| Interleaving | 0 | 0 | 0 | 0 | 1 | ... | 0 |

TU/e

# Fighting against specific attacks

## Arbitrary attacks

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)/p_i & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c^2 \ln n \quad \text{[OSD'13]}$$

# Fighting against specific attacks

## The interleaving attack

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)/p_i & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c^2 \ln n \quad \text{[OSD'13]}$$

# Fighting against specific attacks

## The interleaving attack

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
   - 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".

$$F(p_i) = 1\left\{p_i \geq p = \frac{1}{2}\right\}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +1 & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +1 & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c^2 \ln n$$

TU/e

# Fighting against specific attacks

## The all-1 attack

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -p_i(1-p_i)^{c-1}/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)^c/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim O(c^{1.5} \ln n) \quad \text{[OSD'13]}$$

# Fighting against specific attacks

## The all-1 attack

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
   - 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".

$$F(p_i) = 1\left\{p_i \geq p \approx \frac{1}{c}\right\}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -p_i(1-p_i)^{c-1}/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)^c/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c \ln n$$

# Fighting against specific attacks

## The minority voting attack

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
   - 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”.

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} + \dots & (X_{j,i}, y_i) = (0,0) \\ - \dots & (X_{j,i}, y_i) = (0,1) \\ - \dots & (X_{j,i}, y_i) = (1,0) \\ + \dots & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim O(c^{1.5} \ln n) \quad \text{[OSD'13]}$$

TU/e

# Fighting against specific attacks

## The minority voting attack

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
   - 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".

$$F(p_i) = 1\left\{p_i \geq p \approx \frac{1}{c}\right\}$$

$$g(X_{j,i}, y_i, p_i) \approx \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -p_i(1-p_i)^{c-1}/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)^c/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c \ln n$$

# Fighting against specific attacks

## The majority voting attack

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} + \dots & (X_{j,i}, y_i) = (0,0) \\ - \dots & (X_{j,i}, y_i) = (0,1) \\ - \dots & (X_{j,i}, y_i) = (1,0) \\ + \dots & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim O(c^{1.5} \ln n) \quad \text{[OSD'13]}$$

# Fighting against specific attacks

## The majority voting attack

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
   - 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".

$$F(p_i) = 1\left\{p_i \geq p = \frac{1}{2}\right\}$$

$$g(X_{j,i}, y_i, p_i) \approx \begin{cases} +1 & (X_{j,i}, y_i) = (0,0) \\ -1 & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +1 & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim \pi c \ln n$$

# Fighting against specific attacks

## The coin-flip attack

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
   - 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".

$$F(p_i) = \frac{2}{\pi} \arcsin \sqrt{p_i}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1 - p_i^c + (1 - p_i)^c) & (X_{j,i}, y_i) = (0,0) \\ -p_i/(1 + p_i^c - (1 - p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -(1 - p_i)/(1 - p_i^c + (1 - p_i)^c) & (X_{j,i}, y_i) = (1,0) \\ +(1 - p_i)/(1 + p_i^c - (1 - p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim O(c^{1.5} \ln n) \quad \text{[OSD'13]}$$

# Fighting against specific attacks

## The coin-flip attack

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
   - 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".

$$F(p_i) = 1\left\{p_i \geq p \approx \frac{1}{c}\right\}$$

$$g(X_{j,i}, y_i, p_i) \approx \begin{cases} +p_i/(1 - p_i^c + (1-p_i)^c) & (X_{j,i}, y_i) = (0,0) \\ -p_i/(1 + p_i^c - (1-p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -(1-p_i)/(1 - p_i^c + (1-p_i)^c) & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)/(1 + p_i^c - (1-p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 4c \ln n$$

# Results

## The Tardos scheme

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Arbitrary attacks | $100c^2$ | [Tar'03] | $\Omega(c^2)$ | [Tar'03] |
| Interleaving attack | $100c^2$ | [Tar'03] | $\Omega(c)$ | |
| All-1 attack | $100c^2$ | [Tar'03] | $\Omega(c)$ | |
| Minority voting | $100c^2$ | [Tar'03] | $\Omega(c)$ | |
| Majority voting | $100c^2$ | [Tar'03] | $\Omega(c)$ | |
| Coin-flip attack | $100c^2$ | [Tar'03] | $\Omega(c)$ | |

# Results

## Improvements of the Tardos scheme

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Arbitrary attacks | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| Interleaving attack | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| All-1 attack | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |
| Minority voting | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |
| Majority voting | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |
| Coin-flip attack | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |

# Results

## Results from group testing

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Arbitrary attacks | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| Interleaving attack | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| All-1 attack | $ec$ | [C+'11] | $\log_2(e)c$ | [Seb'85] |
| Minority voting | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |
| Majority voting | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |
| Coin-flip attack | $O(c^{1.5})$ | [OSD'13] | $\Omega(c)$ | |

TU/e

# Results

## Contributions

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Arbitrary attacks | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| Interleaving attack | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |
| All-1 attack | $2c$ | [Laa'13] | $\log_2(e)c$ | [Seb'85] |
| Minority voting | $2c$ | [Laa'13] | $\Omega(c)$ | |
| Majority voting | $\pi c$ | [Laa'13] | $\Omega(c)$ | |
| Coin-flip attack | $4c$ | [Laa'13] | $\Omega(c)$ | |

# Efficient probabilistic group testing

## Problem: Blood testing

| |
|---|
| Antonino |
| Boris |
| Caroline |
| David |
| Eve |
| Fred |
| Gábor |
| Henry |

# Efficient probabilistic group testing

## Problem: Blood testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Boris | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Caroline | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | | | | |
| David | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | | | | |
| Eve | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | | | | |
| Fred | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | | | | |
| Gábor | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | | | | |
| Henry | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | | | | |

# Efficient probabilistic group testing

## Problem: Blood testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Boris | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Caroline | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | | | | |
| David | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | | | | |
| Eve | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | | | | |
| Fred | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | | | | |
| Gábor | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | | | | |
| Henry | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | | | | |
| Results | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | | | | |

# Efficient probabilistic group testing

## Problem: Blood testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Boris | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | | | | |
| Caroline | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | | | | |
| David | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | | | | |
| Eve | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | | | | |
| Fred | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | | | | |
| Gábor | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | | | | |
| Henry | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | | | | |
| Results | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | | | | |

# Efficient probabilistic group testing

## Solution: Using pools

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | | | | | | | | | | | | |

# Efficient probabilistic group testing

## Solution: Using pools

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | 0 | 1 | 0 | | | | | | | | | |

# Efficient probabilistic group testing

## Solution: Using pools

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | 0 | 1 | 0 | | | | | | | | | |

# Efficient probabilistic group testing

## Problem: Multiple infected

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | | | | | | | | | | | | |

# Efficient probabilistic group testing

## Problem: Multiple infected

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | | | | | | | | | | | | |

# Efficient probabilistic group testing

## Problem: Multiple infected

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | 0 | 0 | 0 | | | | | | | | | |
| Boris | 0 | 0 | 1 | | | | | | | | | |
| Caroline | 0 | 1 | 0 | | | | | | | | | |
| David | 0 | 1 | 1 | | | | | | | | | |
| Eve | 1 | 0 | 0 | | | | | | | | | |
| Fred | 1 | 0 | 1 | | | | | | | | | |
| Gábor | 1 | 1 | 0 | | | | | | | | | |
| Henry | 1 | 1 | 1 | | | | | | | | | |
| Results | 1 | 1 | 1 | | | | | | | | | |

# Efficient probabilistic group testing

## Solution: Group testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Boris | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Caroline | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| David | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Eve | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Fred | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Gábor | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Henry | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Results | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |

# Efficient probabilistic group testing

## Solution: Group testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Boris | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Caroline | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| David | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Eve | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Fred | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Gábor | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Henry | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Results | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |

1. An algorithm to construct group testing matrices

# Efficient probabilistic group testing

## Solution: Group testing

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Antonino | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Boris | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Caroline | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| David | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Eve | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Fred | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Gábor | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Henry | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| Results | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |

1. An algorithm to construct group testing matrices
2. An algorithm to link test results to infected people

# Efficient probabilistic group testing

## Solution: Group testing

1. An algorithm to construct group testing matrices
2. An algorithm to link test results to infected people

# Efficient probabilistic group testing

## Solution: Group testing

1. An algorithm to construct group testing matrices

2. An algorithm to link test results to infected people

# Score-based construction

## Overview

1. An algorithm to construct group testing matrices

2. An algorithm to link test results to infected people

TU/e

# Score-based construction

## Overview

1. An algorithm to construct group testing matrices
   - 1a. For each test $i$, generate $p_i \sim F$.
   - 1b. For each test $i$, person $j$, choose $X_{j,i} = 1$ with prob. $p_i$.
2. An algorithm to link test results to infected people
   - 2a. For each test $i$, person $j$, calculate $S_{j,i} = g(X_{j,i}, y_i, p_i)$.
   - 2b. Mark person $j$ infected iff $\sum_i S_{j,i}$ is "large".

TU/e

# Score-based construction

**The classical model $\cong$ The all-1 attack**

1. An algorithm to construct group testing matrices
   1a. For each test $i$, generate $p_i \sim F$.
   1b. For each test $i$, person $j$, choose $X_{j,i} = 1$ with prob. $p_i$.
2. An algorithm to link test results to infected people
   2a. For each test $i$, person $j$, calculate $S_{j,i} = g(X_{j,i}, y_i, p_i)$.
   2b. Mark person $j$ infected iff $\sum_i S_{j,i}$ is "large".

# Score-based construction

## The classical model ≅ The all-1 attack

1. An algorithm to construct group testing matrices
   - 1a. For each test $i$, generate $p_i \sim F$.
   - 1b. For each test $i$, person $j$, choose $X_{j,i} = 1$ with prob. $p_i$.
2. An algorithm to link test results to infected people
   - 2a. For each test $i$, person $j$, calculate $S_{j,i} = g(X_{j,i}, y_i, p_i)$.
   - 2b. Mark person $j$ infected iff $\sum_i S_{j,i}$ is "large".

$$F(p_i) = 1\left\{p_i \geq p \approx \frac{1}{c}\right\}$$

$$g(X_{j,i}, y_i, p_i) = \begin{cases} +p_i/(1-p_i) & (X_{j,i}, y_i) = (0,0) \\ -p_i(1-p_i)^{c-1}/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (0,1) \\ -1 & (X_{j,i}, y_i) = (1,0) \\ +(1-p_i)^c/(1-(1-p_i)^c) & (X_{j,i}, y_i) = (1,1) \end{cases}$$

$$\ell \sim 2c \ln n$$

# Results

## Previous results from group testing

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Classical model | $ec$ | [C+'11] | $\log_2(e)c$ | [Seb'85] |
| Noisy model | $\frac{4.36c}{(1-r)^2}$ | [C+'11] | $\Omega\left(\frac{c}{(1-r)^2}\right)$ | [AS'09] |
| Majority model | $O(c)$ | | $\Omega(c)$ | |
| Bernoulli gap | $\frac{4e^8\ln(2)c}{\pi^2}$ | [C+'13] | $\Omega(c)$ | |
| Linear gap | $2\log_2(e)c^2$ | [D+'05] | $\Omega(c)$ | |

TU/e

# Results

## Contributions

Table: Asymptotics of $L = \frac{\ell}{\ln n}$ for large $n$.

| | Efficient constr. | | Lower bounds | |
|---|---|---|---|---|
| Classical model | $2c$ | [Laa'13] | $\log_2(e)c$ | [Seb'85] |
| Noisy model | $\frac{2c}{(1-r)^2}$ | [Laa'13] | $\Omega\left(\frac{c}{(1-r)^2}\right)$ | [AS'09] |
| Majority model | $\pi c$ | [Laa'13] | $\Omega(c)$ | |
| Bernoulli gap | $4c$ | [Laa'13] | $\Omega(c)$ | |
| Linear gap | $2c^2$ | [OSD'13] | $2c^2$ | [HM'12] |

TU/e

# Conclusion

**Fighting against specific attacks in traitor tracing**

- If you know the attack, you can often find pirates much faster!
- Trick: Not only optimize $g$, but also $p$
- Code length often linear in $c$ with small constants

**Applications to probabilistic group testing**

- Group testing models $\cong$ Specific attacks in traitor tracing
- Classical model: Asymptotic improvement over best result
- Improvements for various other models as well

# Questions?