ICASSP2016

Benchmarking of Scoring Functions for Bias-Based Fingerprinting Code

Minoru Kuribayashi

Okayama University

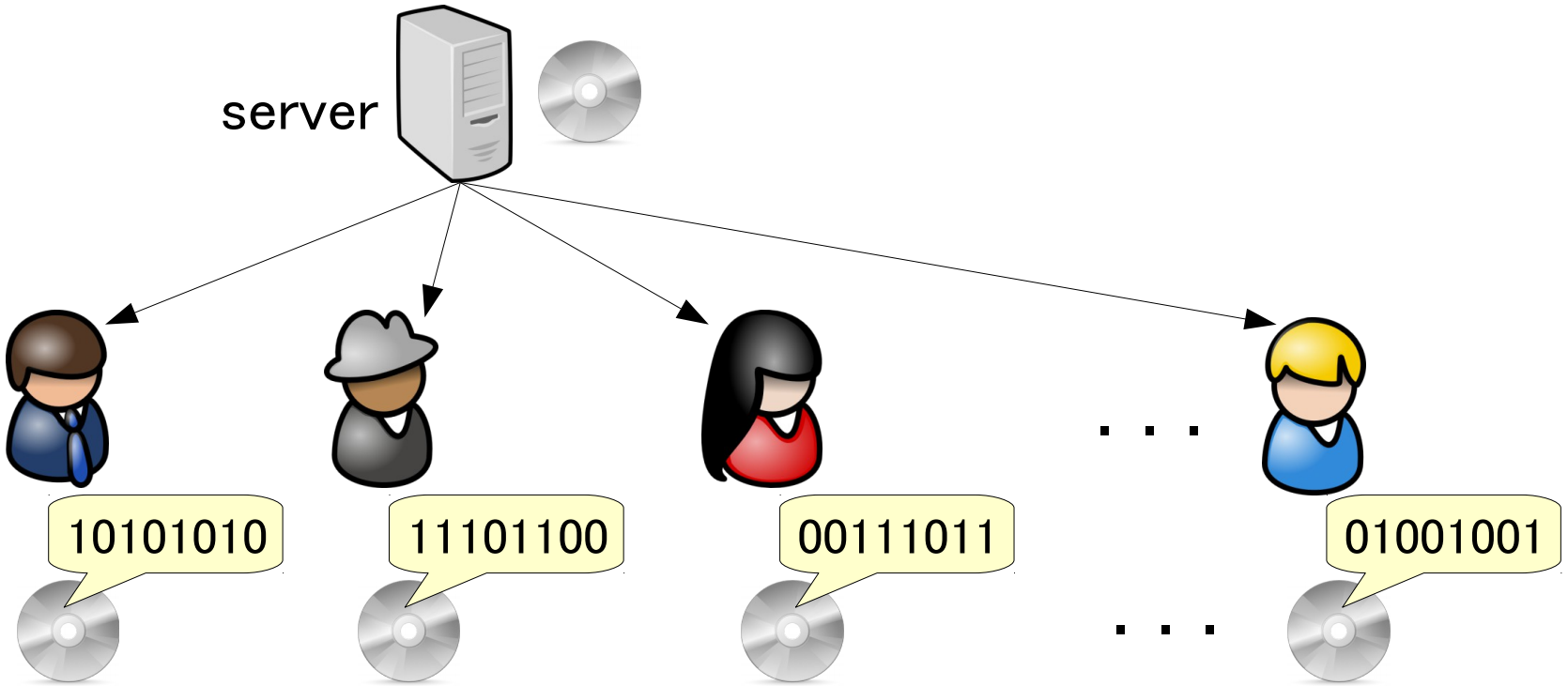
E-mail: kminoru@okayama-u.ac.jp

Content

- Background
- Conventional Scoring Functions
- Proposed Method
- Experimental Results
- Conclusion

What's Fingerprinting?

It enable a server to trace illegal users from a pirated copy.



Collusion Attack

A coalition of users try to remove the fingerprint.

A server distributes personal copies of a content to N users.
c colluders mix their copies to forge a pirated copy.

c-secure code:

If #colluders is equal or less than c,
at least one of them can be identified.

Boneh Shaw (1995) c-secure code (random construction)

Trappe (2002) anti-collusion code (algebraic construction)

Tardos (2003) bias-based code (probabilistic construction)

A server distributes personal copies of a content to N users.

c collud

Tardos Code

Codeword $\boldsymbol{X_j} = \{X_{j,1}, X_{j,2}, \ldots, X_{j,i}, \ldots, X_{j,L}\}$

binary $X_{j,i} \in \{0, 1\}$

Probabilistic Construction

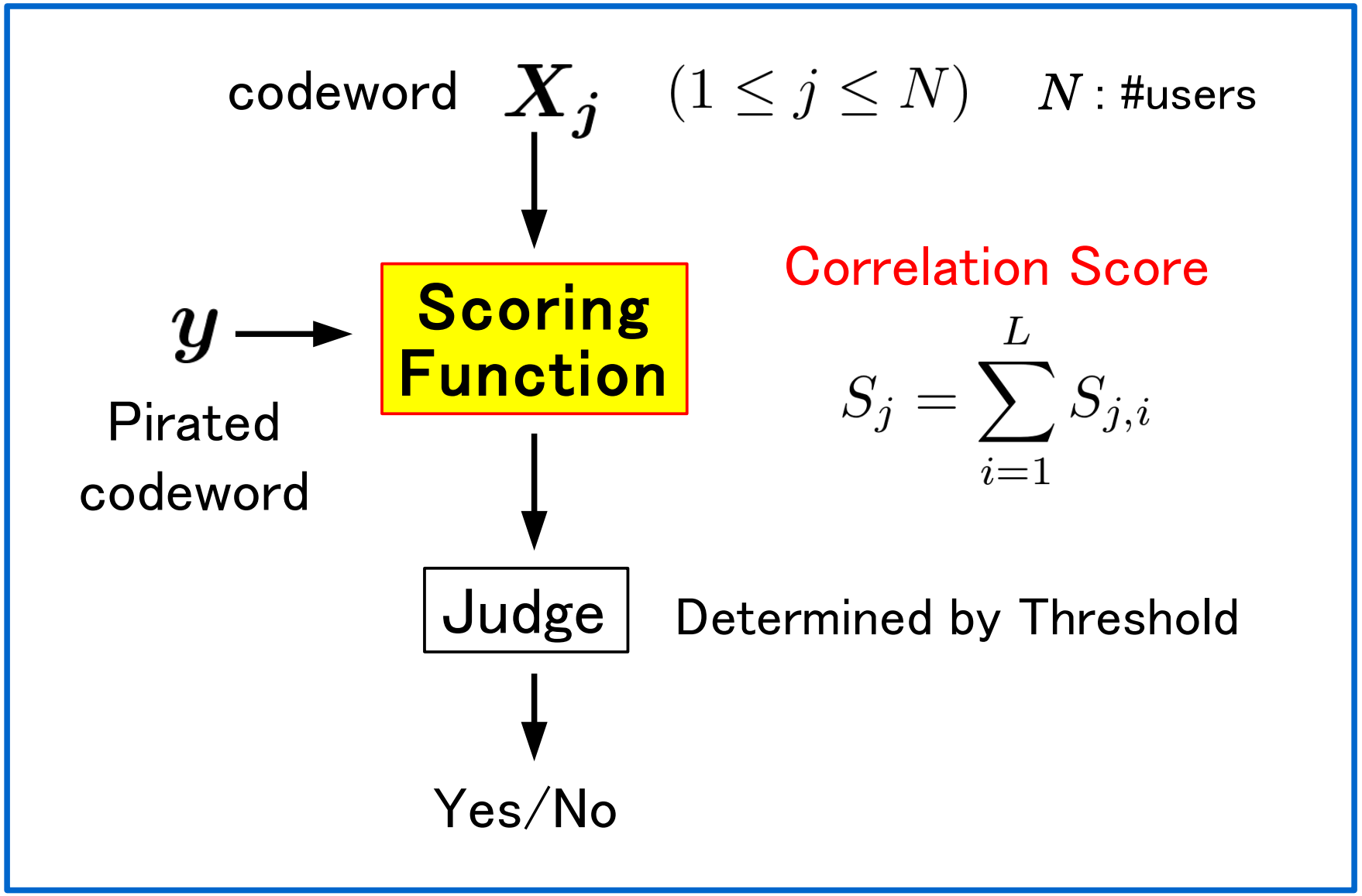
$\Pr(X_{j,i} = 1) = p_i$ Bias probability

Bo

Trappe (2002) anti-collusion code (algebraic construction)

Tardos (2003) bias-based code (probabilistic construction)

Tracing Algorithm



Design of Scoring Function

Pirated codeword $\boldsymbol{y} = \{y_1, y_2, \ldots, y_L\} \quad y_i \in \{0, 1\}$

[Tardos2003]

$$S_{j,i} = y_i U_{j,i}$$

Weight parameter

$$U_{j,i} = \begin{cases} \sqrt{\frac{1-p_i}{p_i}} & \text{if } X_{j,i} = 1 \\ -\sqrt{\frac{p_i}{1-p_i}} & \text{if } X_{j,i} = 0 \end{cases}$$

[Skoric2008]

$$S_{j,i} = (2y_i - 1)U_{j,i}$$

Symmetric Decoder

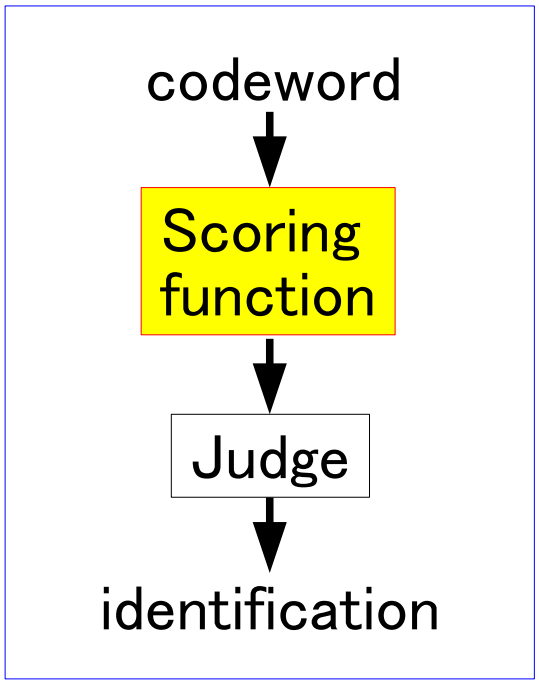
[Furon2009]

$$S_{j,i} = \log \frac{\Pr\left[y_i \middle| X_{j,i}, \boldsymbol{\theta_c}\right]}{\Pr\left[y_i \middle| \boldsymbol{\theta_c}\right]}$$

Optimal Decoder

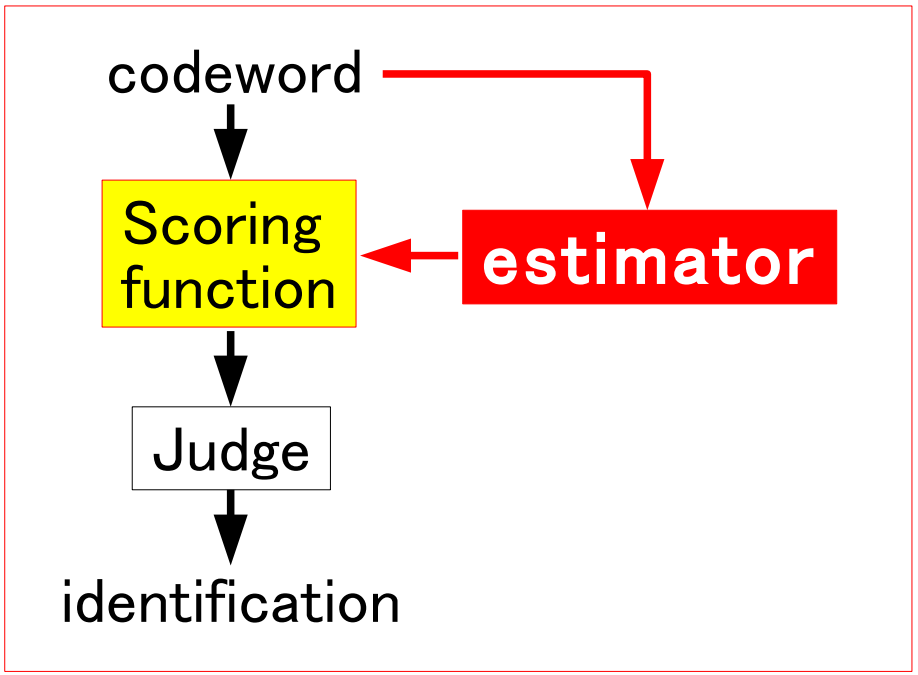
c : #users $\quad \boldsymbol{\theta_c}$: attack parameter

Symmetric Detector



Stable for any attack strategy

Optimal Detector



Estimate #users and attack strategy.

Traceability strongly depends on the accuracy of estimator.

Optimal Detector needs an accurate estimator.

→ Difficult

[Oosterwijk2013] analyzed the impact of estimation error.

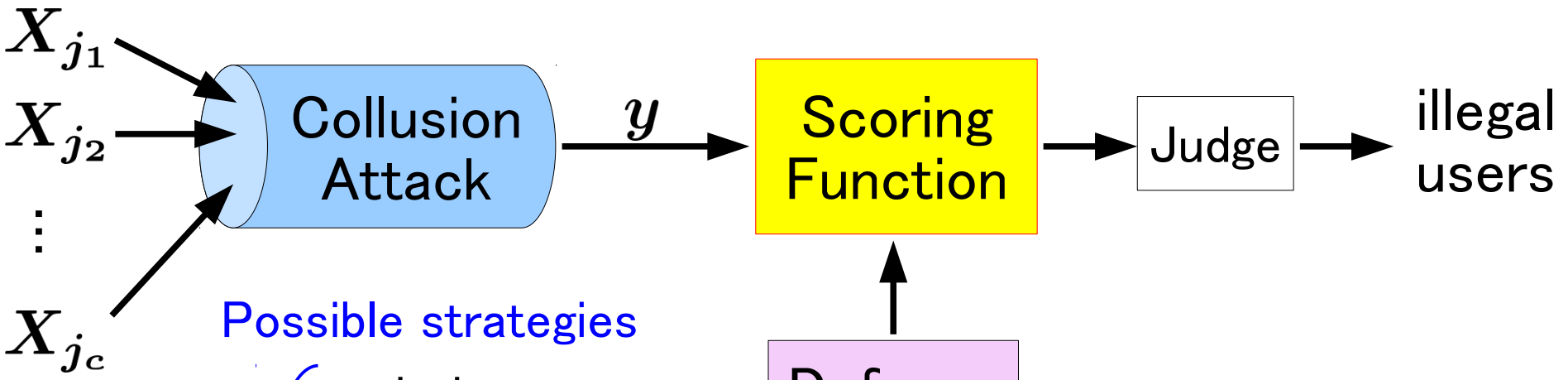
The interleave defense should be employed.

→ Effective for other attack strategies

Universal decoder

For possible attack strategies,
the traceability is better than the symmetric detector.

Attacker vs. Detector

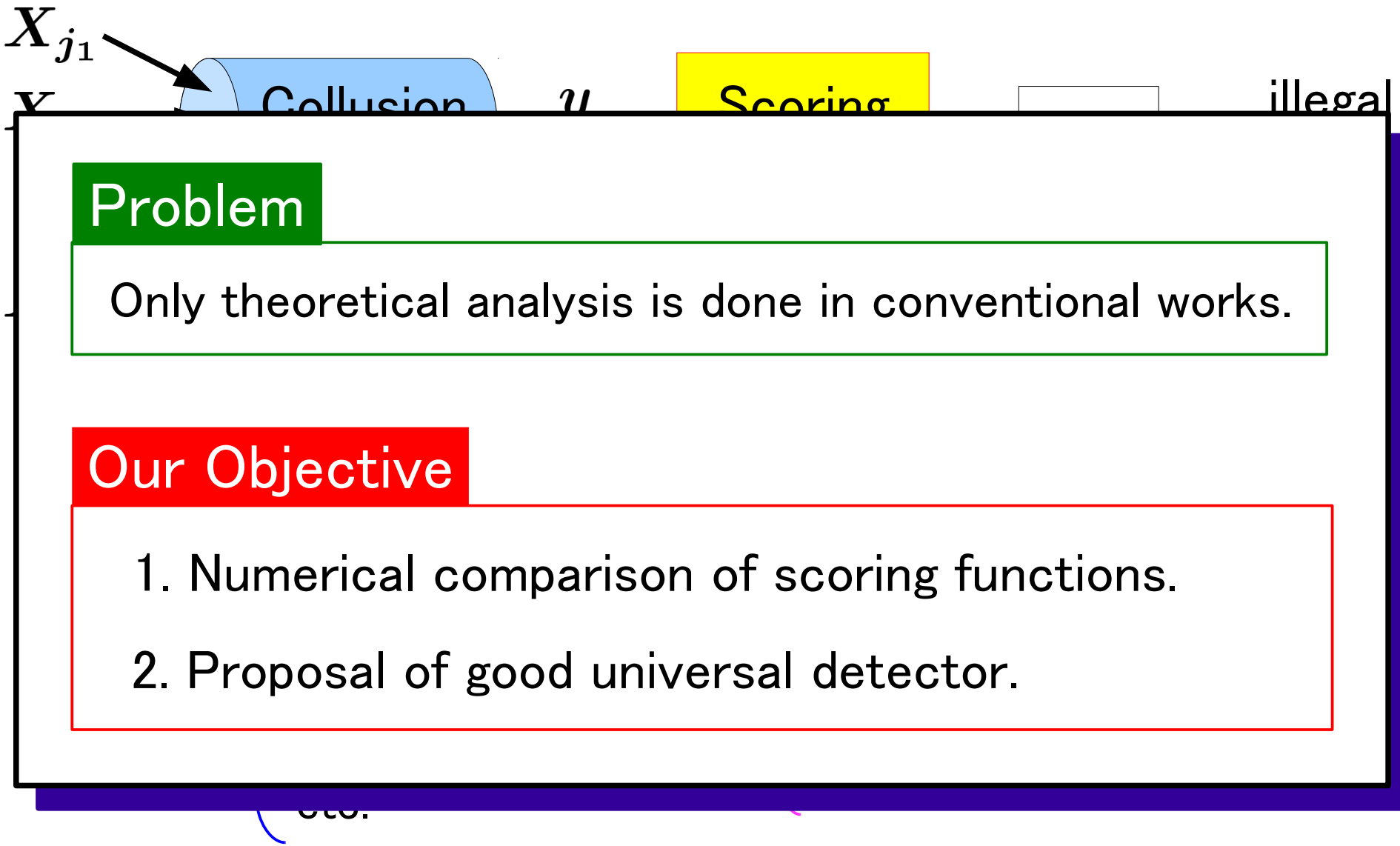


Possible strategies

- majority
- minority
- coin flip
- all-0
- all-1
- interleave
- WCA
- etc.

- **Interleave** [IH&MMSec13,14] + simple estimator
- **WCA** [TIFS12]
- **coin flip** [MMSP13]

Attacker vs. Detector



Problem

Only theoretical analysis is done in conventional works.

Our Objective

1. Numerical comparison of scoring functions.
2. Proposal of good universal detector.

Interleave Defense

Oosterwijk et al. [IH&MMSec13] No estimator

$$S_{j,i}^{Oos} = \begin{cases} \frac{1}{1-p_i} - 1 & \text{if } X_{j,i} = y_i = 0 \\ -1 & \text{if } X_{j,i} \neq y_i \\ \frac{1}{p_i} - 1 & \text{if } X_{j,i} = y_i = 1 \end{cases}$$

Laarhoven et al. [IH&MMSec14] #users c

$$S_{j,i}^{Laa} = \begin{cases} \log\left(1 + \frac{p_i}{c(1-p_i)}\right) & \text{if } X_{j,i} = y_i = 0 \\ \log\left(1 - \frac{1}{c}\right) & \text{if } X_{j,i} \neq y_i \\ \log\left(1 + \frac{1-p_i}{cp_i}\right) & \text{if } X_{j,i} = y_i = 1 \end{cases}$$

WCA Defense

Meerwald et al. [IEEE TIFS12] No estimator

$$S_{j,i}^{Mee} = \max_{1 \le t \le c_{max}} \left\{ \log \left(\frac{\Pr[y_i | X_{j,i}, p_i, \boldsymbol{\theta}_t^{WCA}]}{\Pr[y_i | p_i, \boldsymbol{\theta}_t^{WCA}]} \right) \right\}$$

Coin-Flip Defense

Desoubeaux et al. [MMSP13] No estimator

$$S_{j,i}^{Des} = \log \left(\sum_{t=1}^{c_{max}} t \cdot \left(\frac{\Pr[y_i | X_{j,i}, p_i, \boldsymbol{\theta}_t^{coin}]}{\Pr[y_i | p_i, \boldsymbol{\theta}_t^{coin}]} \right) \right)$$

Bias Equalizer [IH12]

No estimator

Symmetric decoder meets **Special Weights.**

$$S_{j,i} = (2y_i - 1)U_{j,i}$$

Reconsider the weights.

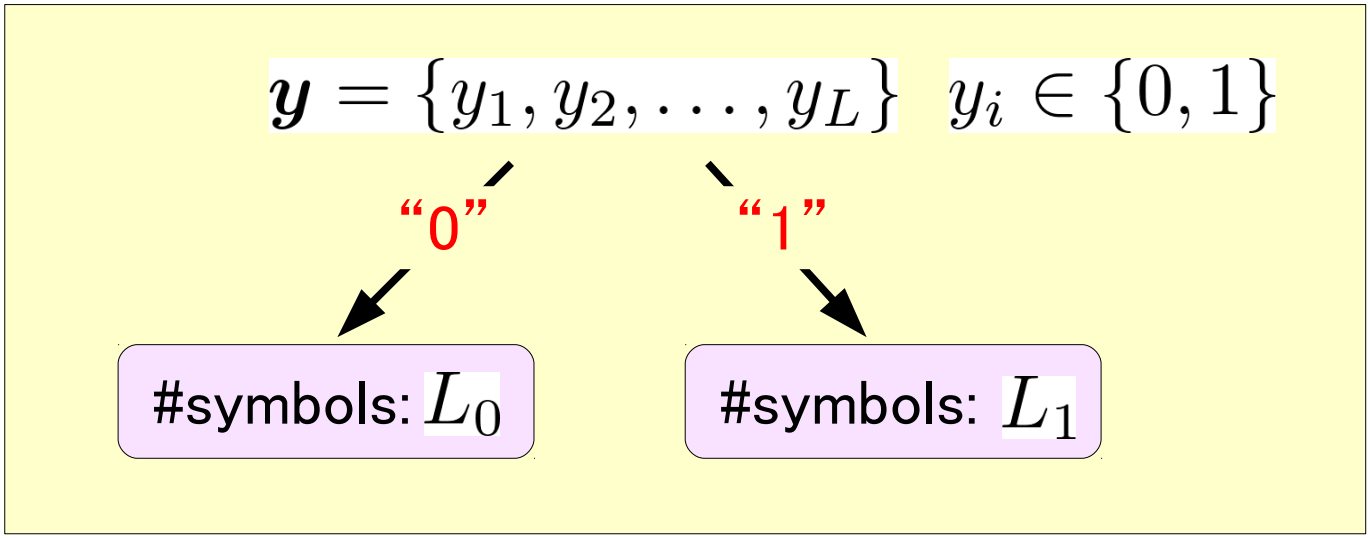
Original weights $$U_{j,i} = \begin{cases} \sqrt{\frac{1-p_i}{p_i}} & \text{if } X_{j,i} = 1 \\ -\sqrt{\frac{p_i}{1-p_i}} & \text{if } X_{j,i} = 0 \end{cases}$$

Bias probability $$\Pr(X_{j,i} = 1) = p_i$$

Exploit the bias of symbols “0” and “1”.

Correlation Score $S_{j,i} = (2y_i - 1)U_{j,i}$

Suppose that symbols in a pirated codeword is classified into two sets.



Bias Equalizer

Correlation Score $S_{j,i} = (2y_i - 1)U_{j,i}$

Supp d into two sets.

Special Weights

$$U_{j,i}^{Bias} = \begin{cases} \frac{L_1}{L} U_{j,i} & \text{if } y_i = 0 \\ \frac{L_0}{L} U_{j,i} & \text{if } y_i = 1 \end{cases}$$

, 1}

#symbols: L_0

#symbols: L_1

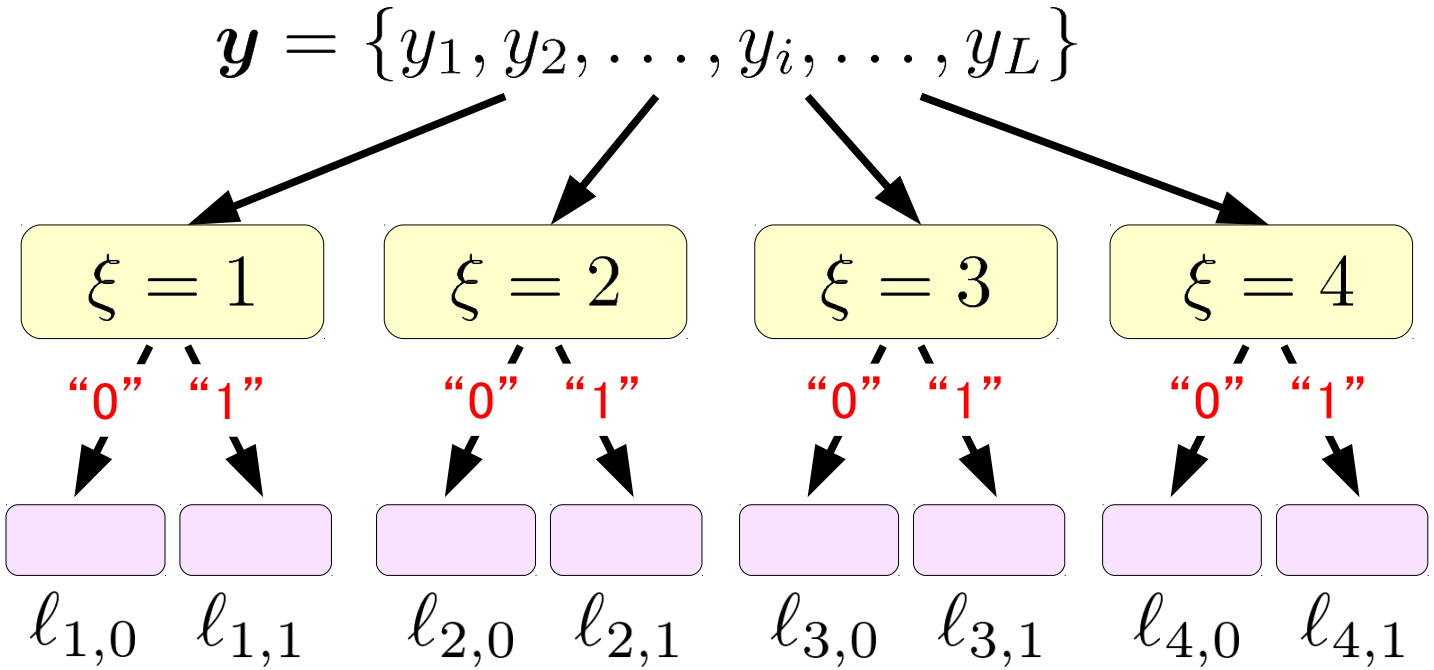
We can calculate from the observation of pirated codeword.

$$\Pr[y_i = 0] = \frac{L_0}{L} \qquad \Pr[y_i = 1] = \frac{L_1}{L}$$

Correlation Score $S_{j,i} = (2y_i - 1)U_{j,i}$

Discrete bias probability $\Pr(X_{j,i} = 1) = p_i$

In case of that a codeword is classified into 4 groups,



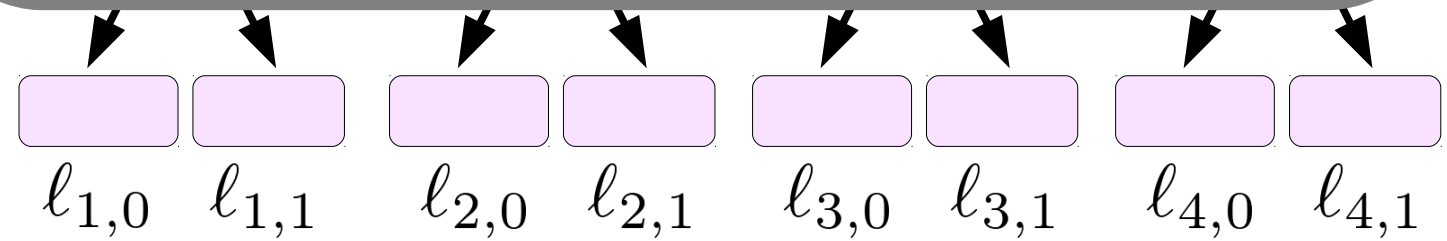
Correlation Score $S_{j,i} = (2y_i - 1)U_{j,i}$

Di

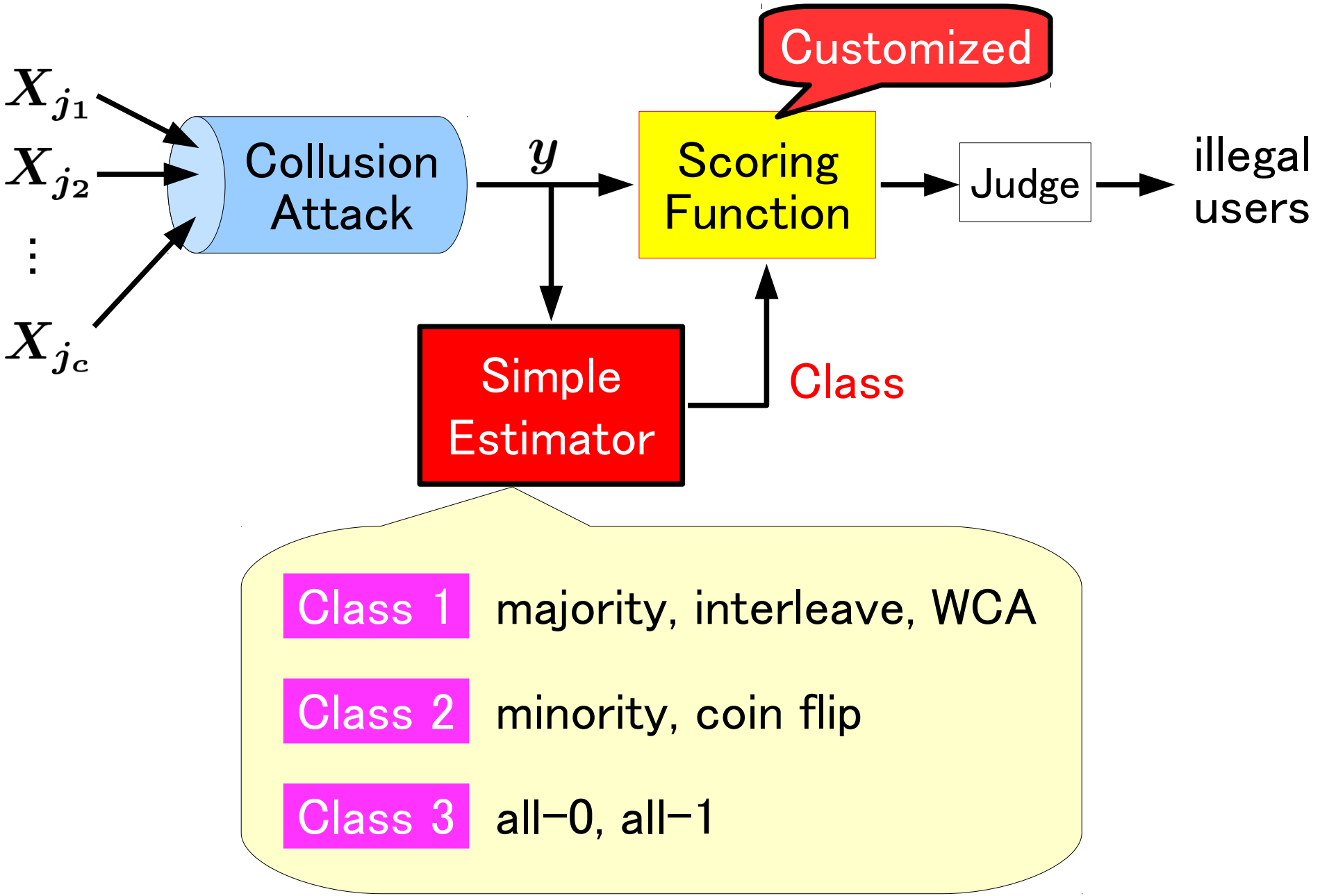
In

Proposed Method

1. Observing #symbols for each group.
2. Classify attack strategies into 3 classes.
3. For each class, special weights are further customized to improve the performance.



Proposed Method



Experiment

Fingerprinting code : Nuida Code

$c_{max} = 8$

(Discrete Bias Probability)

$$\Pr(X_{j,i} = 1) = p_i$$

4 candidates

Code Length : L=1024, 2048

#users : 10^6

Pr[FP] : 10^{-10} (total 10^{-4})

Benchmarking Score

Sum of detected colluders

At most $54 = \sum_{c=2}^{10} c$

Experimental Results (L=1024)

#users : 10^{6} Pr[FP] : 10^{-10} (total 10^{-4})

	Maj	Min	Coin flip	All-0	All-1	Int.	WCA	total
symmetric	7.16	**6.32**	6.75	6.73	6.72	6.93	6.72	47.33
MAP (optimal)	21.26	53.70	9.37	30.30	30.62	9.94	**8.65**	163.84
Ooserwijk	17.17	8.19	7.81	7.87	7.76	8.62	**7.45**	64.87
Laarhoven	16.54	**5.82**	7.80	7.85	7.76	9.96	7.77	63.50
Meerwald	9.83	11.11	9.00	9.08	9.02	8.73	**8.64**	65.41
Desoubeaux	9.76	10.90	9.01	9.08	9.01	8.68	**8.64**	65.08
Bias equalizer	21.14	**6.69**	7.72	18.58	18.65	9.70	7.69	90.17
Proposed	21.14	32.72	7.70	24.65	24.76	9.70	**7.39**	128.06

*** : worst case

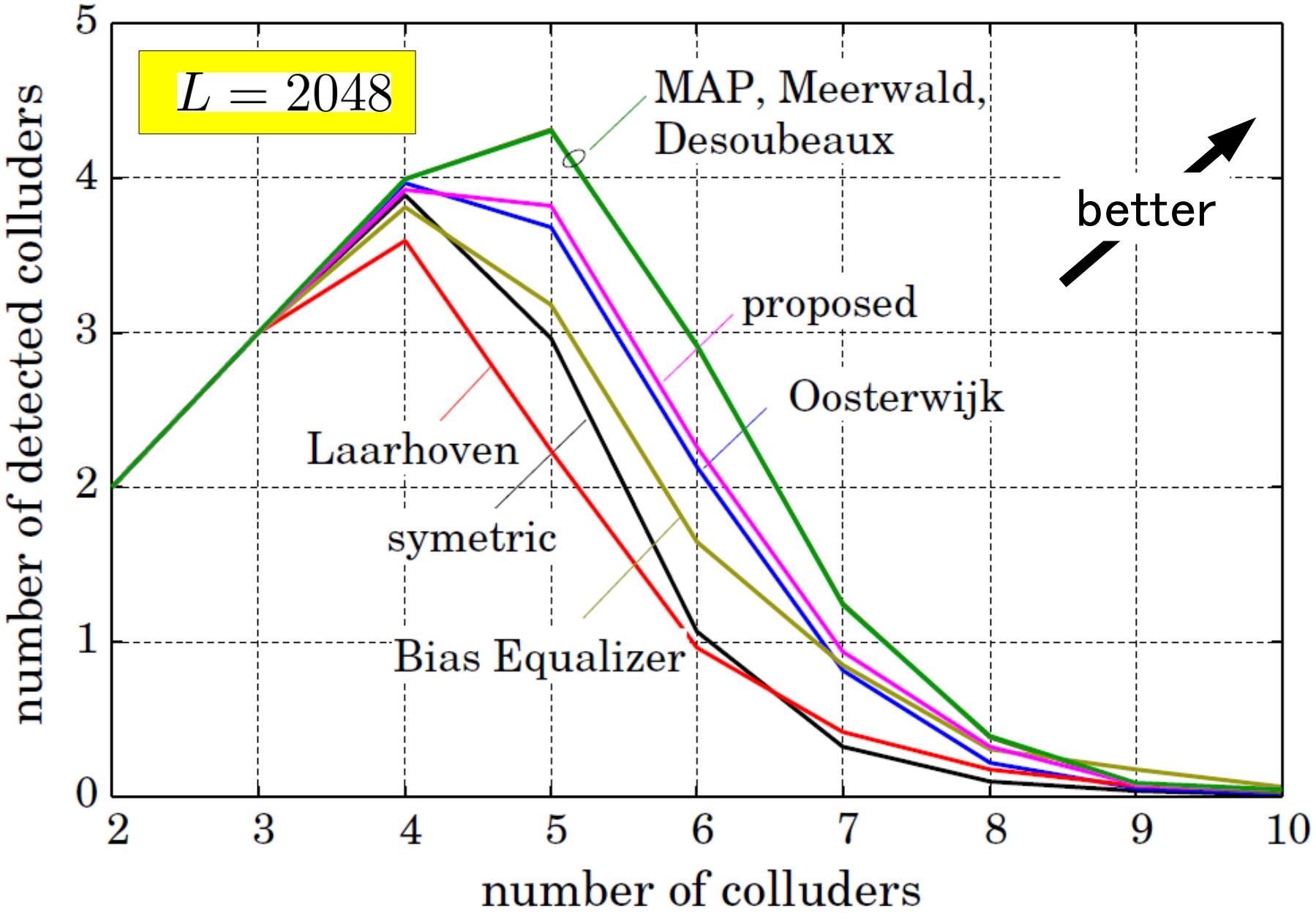
Experimental Results (L=2048)

#users : 10^{6} Pr[FP] : 10^{-10} (total 10^{-4})

	Maj	Min	Coin flip	All-0	All-1	Int.	WCA	total
symmetric	14.65	**13.39**	13.88	13.91	13.94	14.33	14.05	98.15
MAP (optimal)	45.33	54.00	23.16	53.97	53.85	21.88	**17.97**	270.03
Ooserwijk	36.84	19.43	17.47	17.30	17.44	20.06	**15.89**	144.43
Laarhoven	35.32	**12.49**	16.12	15.98	16.10	21.91	16.62	134.54
Meerwald	18.89	23.07	20.32	20.16	20.18	18.70	**17.97**	139.29
Desoubeaux	18.74	22.91	20.08	19.93	19.96	19.10	**17.95**	138.67
Bias equalizer	45.09	**15.02**	15.71	43.60	43.57	21.40	16.45	200.84
Proposed	45.09	53.82	19.18	52.40	52.37	21.40	**16.39**	260.65

*** : worst case

Worst case


$L = 2048$
MAP, Meerwald, Desoubeaux
proposed
Oosterwijk
Laarhoven
symetric
Bias Equalizer
better
number of detected colluders
number of colluders
0
1
2
3
4
5
2
3
4
5
6
7
8
9
10

Benchmarking some scoring functions

- **MAP** Optimal, but the accurate estimation of attack parameters is difficult to realize.

- **Meerwald, Desoubeaux**

  In the worst case, the performance is very close to MAP.

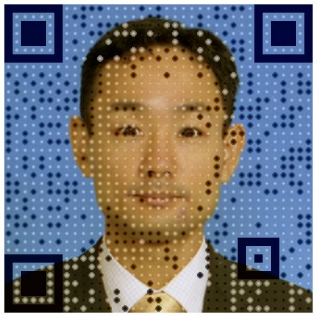
- **Proposed Method** Bias equalizer + simple estimator

  Total balance against some attack strategies is good.

Future work : theoretical analysis of the proposed method.

Thank you for your attention.

Any Question?



Minoru Kuribayashi

Okayama University

E-mail: kminoru@okayama-u.ac.jp