IT研究会

電子指紋符号の最適な検出法

栗林 稔 (神戸大)

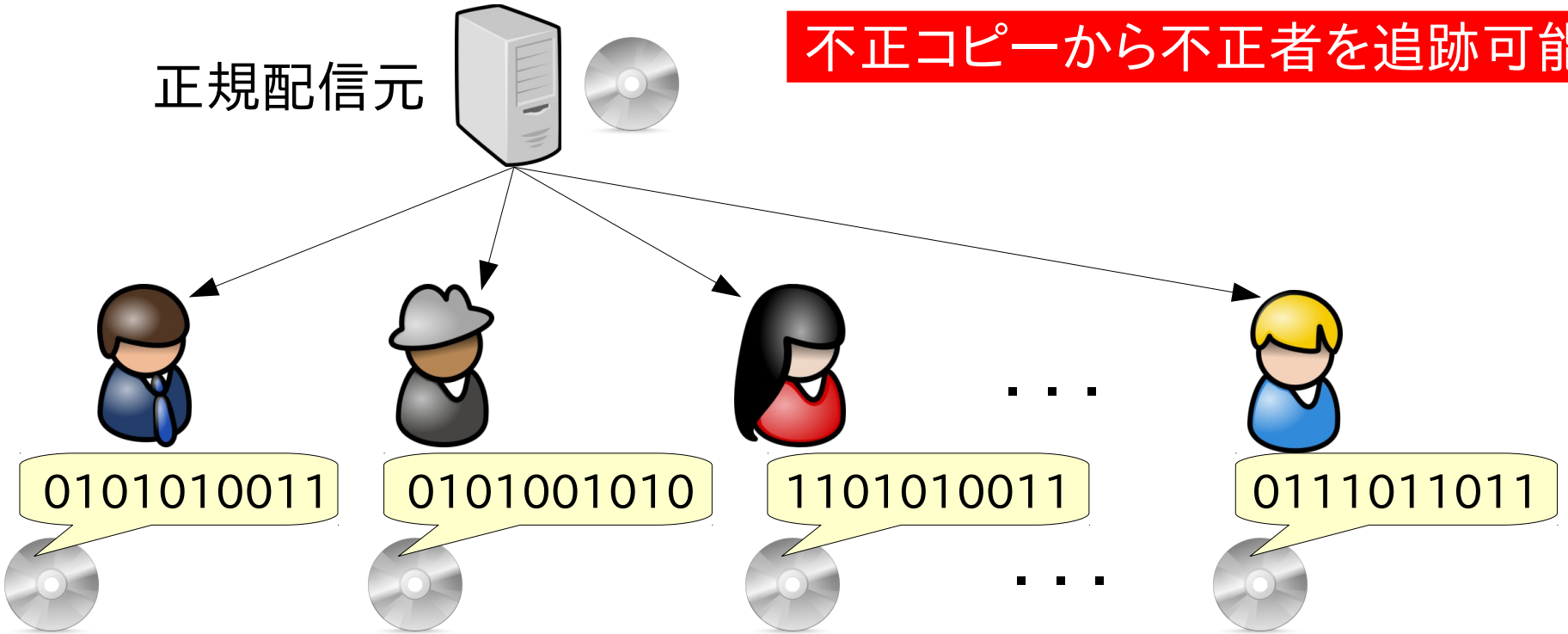
E-mail: kminoru@kobe-u.ac.jp

Outline

- 電子指紋符号とその検出器
- Tardos符号と関連研究
- 結託攻撃の定式化
- 最適な検出器の設計
- 最近の研究紹介
- 今後の展望

電子指紋符号

ユーザを識別可能な情報（電子指紋）を埋め込んだコンテンツを配信



ユーザの結託により，埋め込まれた情報が改変される可能性がある

結託攻撃

マーキング仮定

c人のユーザの符号語を用いて不正符号語を生成

$$x_1 = \{0\,1\,0\,1\,0\,1\,0\,0\,1\,1\}$$
$$x_2 = \{0\,1\,0\,1\,0\,0\,1\,0\,1\,0\}$$
$$x_3 = \{1\,1\,0\,1\,0\,1\,0\,0\,1\,1\}$$
$$x_4 = \{0\,1\,1\,1\,0\,1\,1\,0\,1\,1\}$$

$$y = \{?\,1\,?\,1\,0\,?\,?\,0\,1\,?\}$$

- 全て同じシンボルは変更不可

$$y_i \in \{x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}\}$$

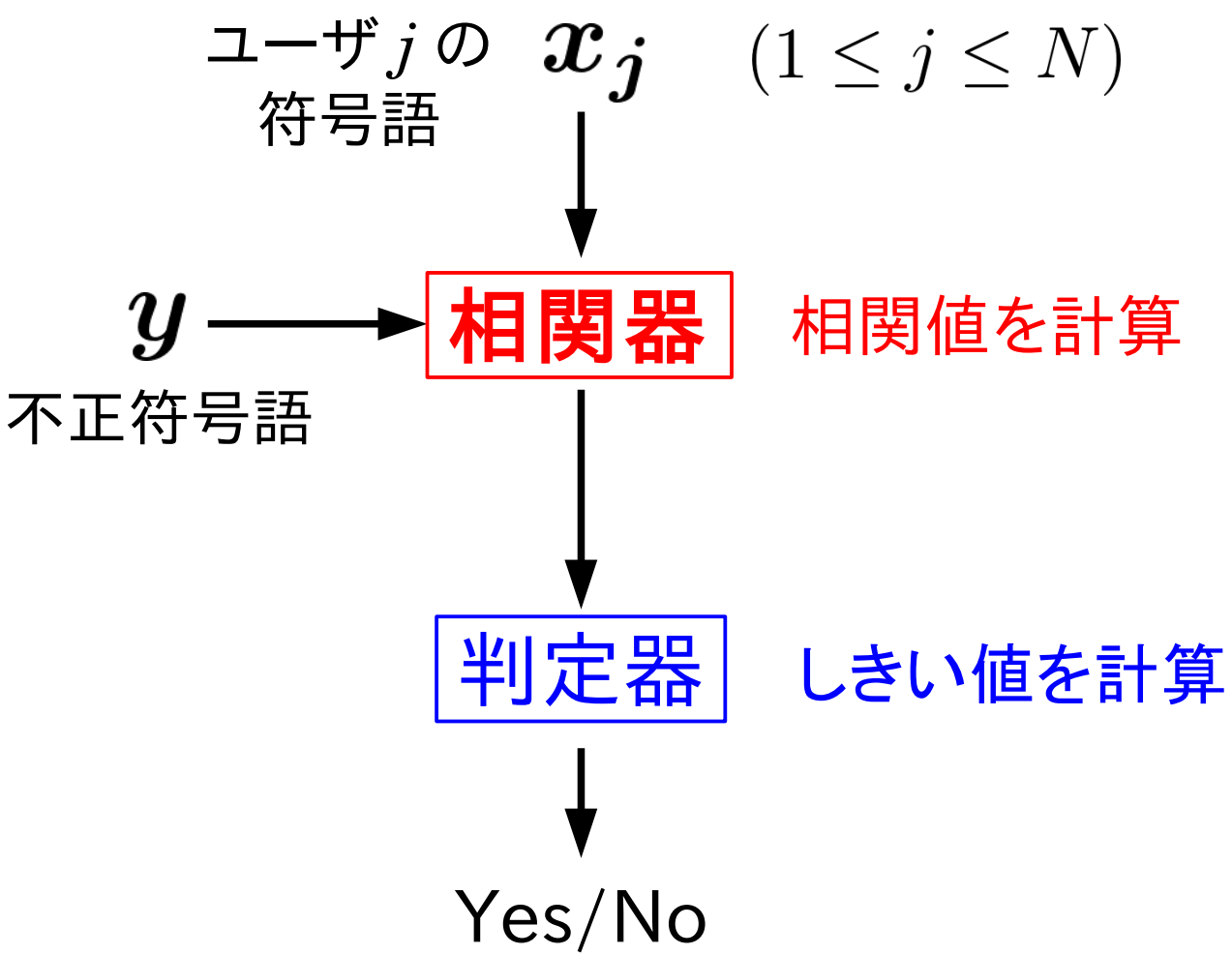
? : 0 or 1 を選択可能

シンボル単位での攻撃を想定

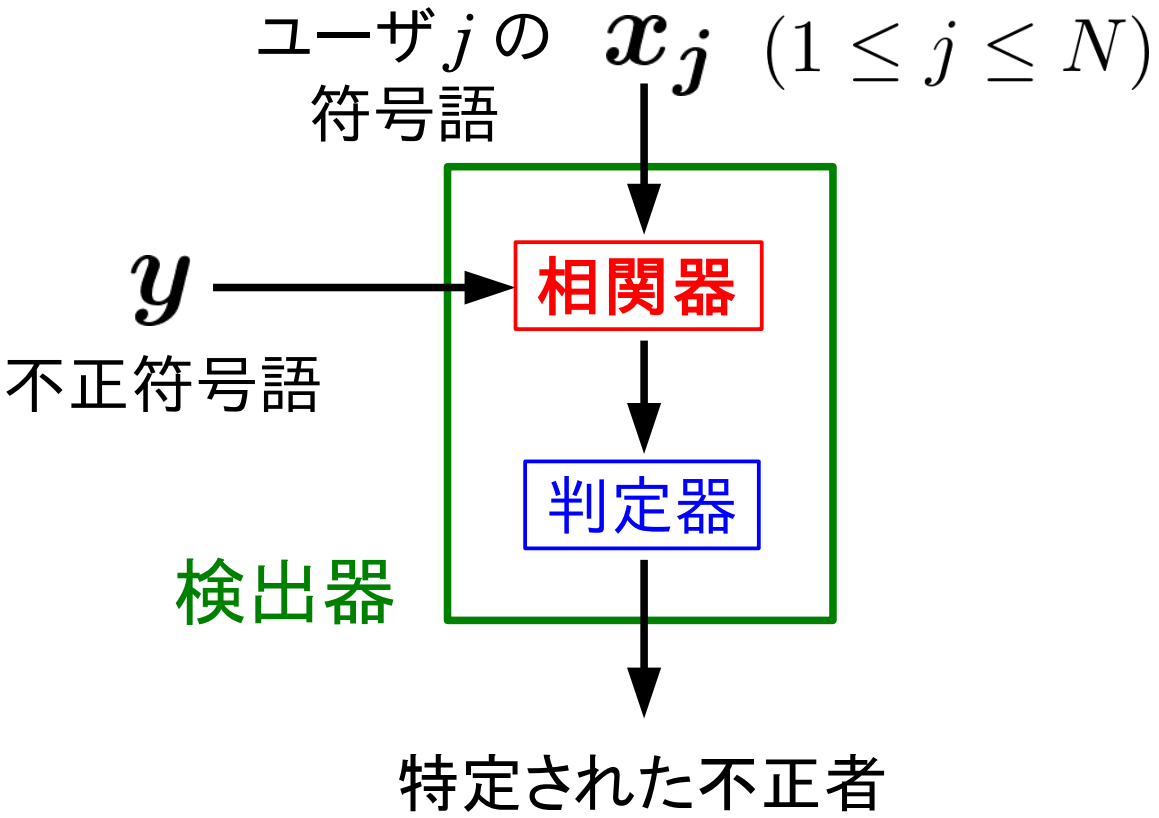
例) majority, minority, interleave, all-0, all-1, etc.

検出器

結託者の特定方法

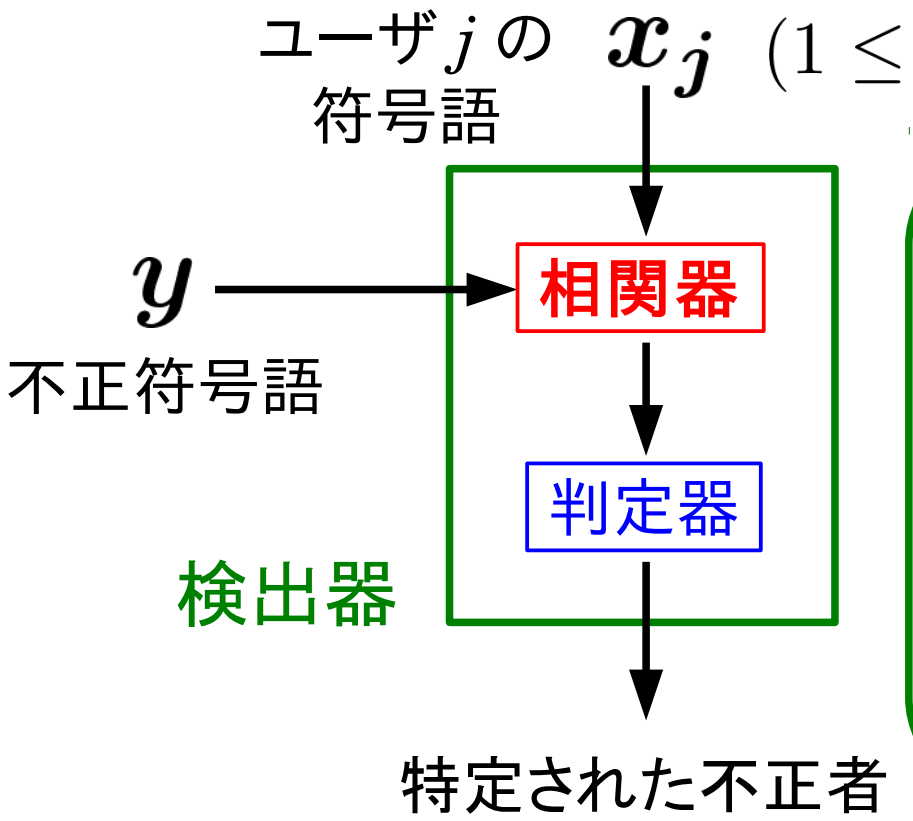


検出器の種類



何を優先して検出の方針を決定すれば良い？

検出器の種類



検出器の方針

- 不正者全員（catch all）
- 最も怪しい人だけ（catch one）
- 怪しい人をなるべく多く（catch many）

何を優先して検出の方針を決定すれば良い？

Outline

- 電子指紋符号とその検出器
- **Tardos符号と関連研究**
- 結託攻撃の定式化
- 最適な検出器の設計
- 最近の研究紹介
- 今後の展望

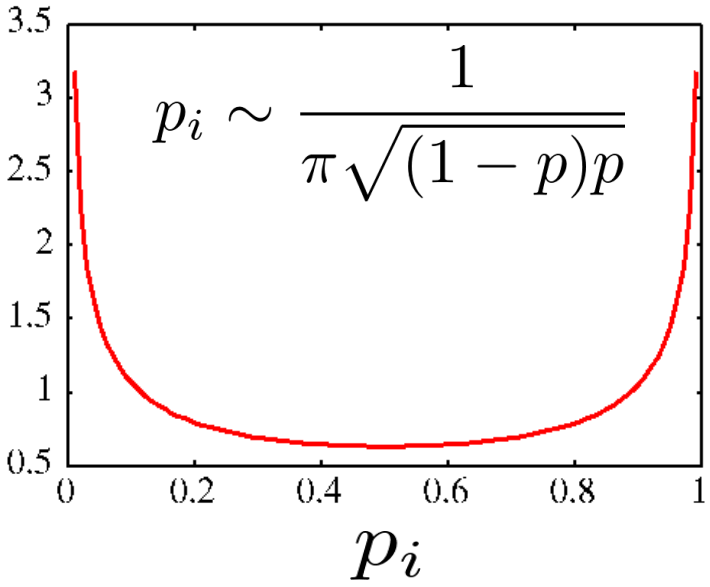
Tardos符号の生成

符号語 $\boldsymbol{x_j} = \{x_{j,1}, x_{j,2}, \ldots, x_{j,i}, \ldots, x_{j,L}\}$ L: 符号長

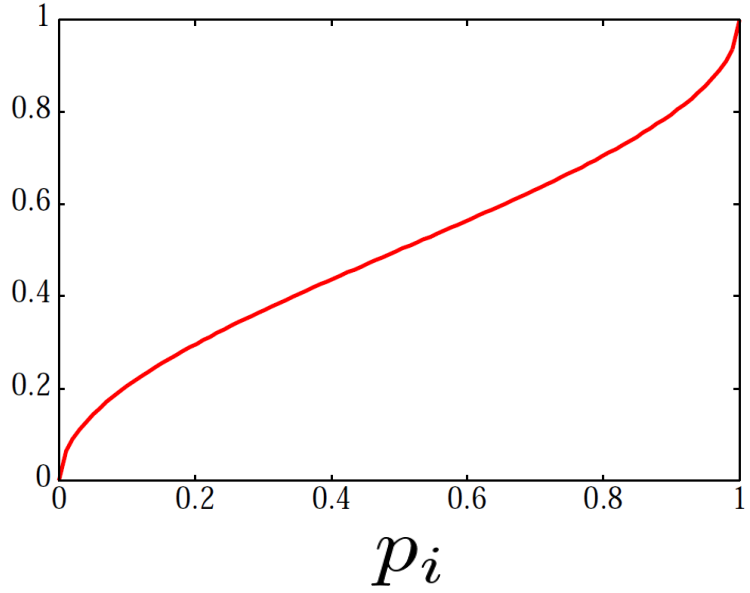
各要素はバイナリ $x_{j,i} \in \{0,1\}$ $\Pr[x_{j,i} = 1] = p_i$

確率p_iに基づきランダムに$x_{j,i} \in \{0,1\}$を選択

確率密度関数(PDF)



確率分布関数



符号生成例

p_i は 0 もしくは 1 に近い値になりやすい

p_i	0.10	0.98	0.07	0.99	0.02	0.89	0.40	0.10	0.93
$\boldsymbol{x_1}$	0	1	0	1	0	1	1	1	1
$\boldsymbol{x_2}$	0	0	1	1	0	1	0	0	1
$\boldsymbol{x_3}$	1	1	0	1	0	1	0	0	1
$\boldsymbol{x_4}$	0	1	0	1	1	1	1	0	0
$\boldsymbol{x_5}$	0	1	0	0	0	1	0	0	1
$\boldsymbol{x_6}$	0	1	0	1	0	0	1	0	1

Tardos符号の不正者検出

検出方法　結託符号語 $\boldsymbol{y} = \{y_1, y_2, \ldots, y_L\}$

相関値S_jがしきい値Zを超えればユーザiを不正者として検挙

$$S_j = \sum_{i=1}^{L} y_i U_{j,i}$$

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

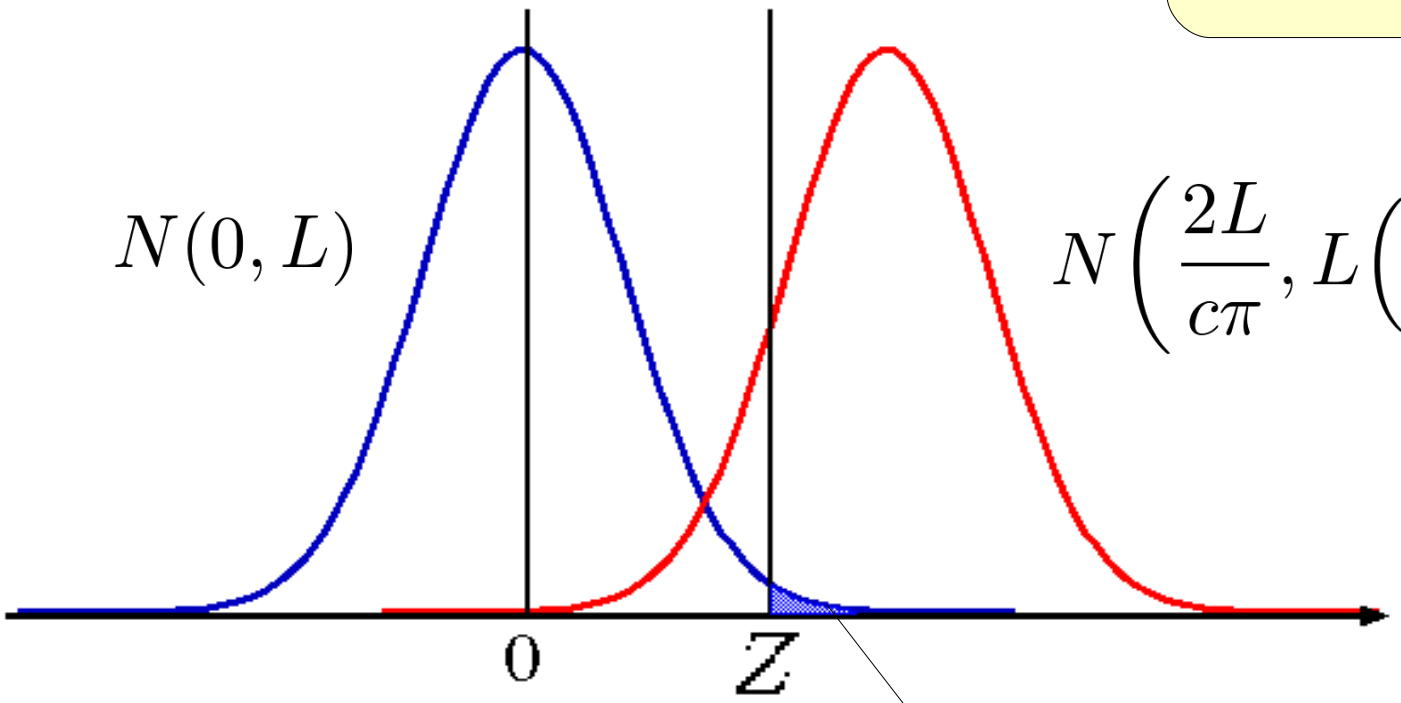
- 相関値の計算方法の修正（Skoric et al.）

$$S_j = \sum_{i=1}^{L} (2y_i - 1) U_{j,i}$$

分布の対称性から $y_i = 0$ のときも考慮

スコアの統計分布

中心極限定理より
正規分布で近似可能

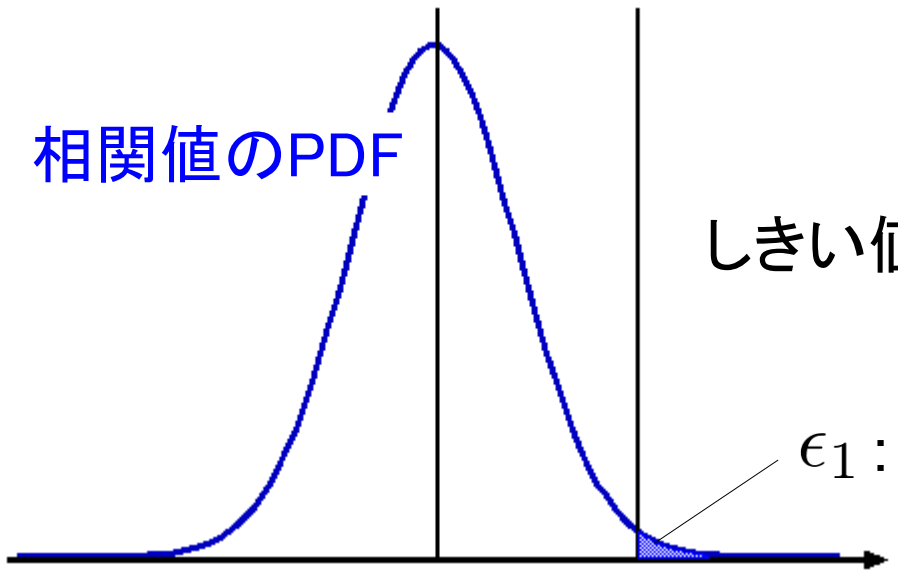


しきい値

ϵ_1 : 誤検出率
(false-positive probability)

しきい値の設定

誤検出率に応じて，しきい値を導出したい



正規分布の場合，
統計的な手法で導出できる

しきい値　$Z = \sqrt{2\sigma^2}\mathrm{erfc}^{-1}(2\epsilon_1)$

ϵ_1：誤検出率

問題点　誤検出率を極めて低く抑えたい場合，
正規分布の近似精度が悪い

実験的なしきい値の設定

しきい値の値に対して，厳密に誤検出率を求めるには

中心極限定理のような近似は不適切

→ 理論的に解析する場合，その下限や上限は導出可能

e.g.) Chernoff bound, union bound, nearest neighbor bound, etc.

実験的に推定する方法

モンテカルロ(MC)推定器

計算量が莫大

誤り確率が10^{-8}より低いと
実現が困難

しきい値の設定

Rare Event Simulator (Furon'09)

$$\epsilon_1 = f(Z)$$

しきい値 Z に対して誤り確率を導出

所望の誤り確率に対応するしきい値 Z を求めるには

→ 最急降下法などを用いて，何度か関数 f を実行すれば良い

現在のところ最も実用的な方法

Outline

- 電子指紋符号とその検出器
- Tardos符号と関連研究
- **結託攻撃の定式化**
- 最適な検出器の設計
- 最近の研究紹介
- 今後の展望

攻撃の定式化

結託攻撃のパラメータ: $\boldsymbol{\theta_c} = (\theta_0, \theta_1, \ldots, \theta_c)$

$$\theta_\rho = \Pr[y_i = 1 | \Phi = \rho]$$

$$\Phi = \sum X_{j,i} \quad \Phi \in \{0, 1, \ldots, c\}$$

マーキング仮定では $\theta_0 = 0, \theta_c = 1$ を保証

majorityの場合

$$\boldsymbol{\theta_5^{(maj)}} = (0, 0, 0, 1, 1, 1)$$

$$\boldsymbol{\theta_6^{(maj)}} = (0, 0, 0, \tfrac{1}{2}, 1, 1, 1)$$

minorityの場合

$$\boldsymbol{\theta_5^{(min)}} = (0, 1, 1, 0, 0, 1)$$

$$\boldsymbol{\theta_6^{(min)}} = (0, 1, 1, \tfrac{1}{2}, 0, 0, 1)$$

攻撃の分類(続き)

例) c=6の場合

$$\boldsymbol{x_1} = \{0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\}$$
$$\boldsymbol{x_2} = \{0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\}$$
$$\boldsymbol{x_3} = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\}$$
$$\boldsymbol{x_4} = \{0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\}$$
$$\boldsymbol{x_5} = \{0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\}$$
$$\boldsymbol{x_6} = \{0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\}$$

$$\Phi = \{1\ 6\ 2\ 5\ 1\ 3\ 4\ 0\ 5\ 4\}$$

攻撃の分類(続き)

例) c=6の場合

$$\boldsymbol{x_1} = \{0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\}$$
$$\boldsymbol{x_2} = \{0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\}$$
$$\boldsymbol{x_3} = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\}$$
$$\boldsymbol{x_4} = \{0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\}$$
$$\boldsymbol{x_5} = \{0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\}$$
$$\boldsymbol{x_6} = \{0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\}$$

$$\Phi = \{1\ 6\ 2\ 5\ 1\ \boxed{3}\ 4\ 0\ 5\ 4\}$$

majorityの場合

$$\boldsymbol{\theta_6^{(maj)}} = (0, 0, 0, \tfrac{1}{2}, 1, 1, 1)$$

- $\Phi \leq 2$ のとき “0”
- $\Phi = 3$ のとき “0” or “1”
- $\Phi \geq 4$ のとき “1”

$$\boldsymbol{y} = \{0\ 1\ 0\ 1\ 0\ \boxed{0}\ 1\ 0\ 1\ 1\}$$

or

$$\boldsymbol{y} = \{0\ 1\ 0\ 1\ 0\ \boxed{1}\ 1\ 0\ 1\ 1\}$$

典型的な攻撃例

結託攻撃のパラメータ $\boldsymbol{\theta_c} = (\theta_0, \theta_1, \ldots, \theta_c)$

Random: $\boldsymbol{\theta_6^{(rand)}} = (0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1)$

All-0: $\boldsymbol{\theta_6^{(all0)}} = (0, 0, 0, 0, 0, 0, 1)$

All-1: $\boldsymbol{\theta_6^{(all1)}} = (0, 1, 1, 1, 1, 1, 1)$

interleave: $\boldsymbol{\theta_6^{(int)}} = (0, \frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, 1)$

攻撃者はどの攻撃手法を取れば有利？

◀▶ 検出側にとって最も嫌な攻撃方法は？

最悪攻撃 (WCA) のパラメータ $\boldsymbol{\theta_c^{(WCA)}}$ は？

達成可能レート

符号化レート

$$R = \log_2(N)/L$$

N : 総ユーザ数

L : 符号長

結託攻撃 $\boldsymbol{\theta_c}$ に対して達成可能レート(Achievable Rate)は

$$R(\boldsymbol{\theta_c}) = \mathbb{E}_P[I(Y;X|P=p)]$$

確率 P を条件とした X と Y の相互情報量の期待値

符号語 Y は結託攻撃 $\boldsymbol{\theta_c}$ に依存して作成される

最悪攻撃(WCA): 達成可能レートを最も小さくする攻撃

$$\boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{WCA})} = \arg\min_{\boldsymbol{\theta}_{\boldsymbol{c}}} R(\boldsymbol{\theta}_{\boldsymbol{c}})$$

例）

$$\boldsymbol{\theta}_{\boldsymbol{2}}^{(\boldsymbol{WCA})} = (0, 0.5, 1)$$

$$\boldsymbol{\theta}_{\boldsymbol{3}}^{(\boldsymbol{WCA})} = (0, 0.652, 0.348, 1)$$

$$\boldsymbol{\theta}_{\boldsymbol{4}}^{(\boldsymbol{WCA})} = (0, 0.488, 0.5, 0.512, 1)$$

$$\boldsymbol{\theta}_{\boldsymbol{5}}^{(\boldsymbol{WCA})} = (0, 0.594, 0.000, 1.000, 0.406, 1)$$

対称的な値 $\theta_\rho = 1 - \theta_{c-\rho}$

Outline

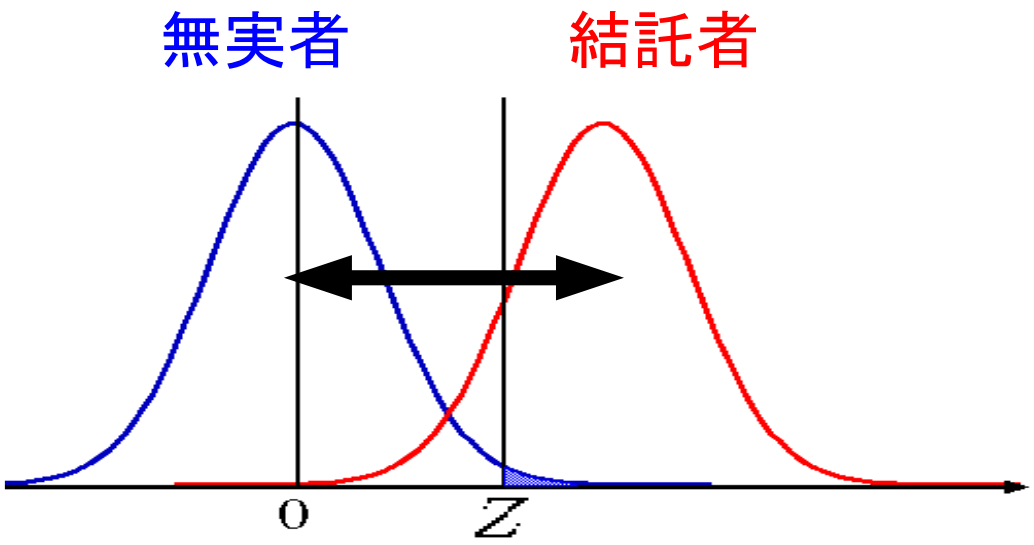
- 電子指紋符号とその検出器
- Tardos符号と関連研究
- 結託攻撃の定式化
- **最適な検出器の設計**
- 最近の研究紹介
- 今後の展望

次なる興味は

結託者の戦略: 理論上，最悪攻撃(WCA)がベスト

検出者の戦略: こちらも理論上最も良い検出器を構築したい

最適な検出器とは？



目標 2つの分布を最も効果的に分離できるスコアの導出

Optimal detector

最適な検出器

結託者数 c と結託攻撃のパラメータ $\boldsymbol{\theta}_c$を正しく推定できれば
最適な相関値を導出することが可能

最適な検出器　(Nayman-Peason lemmaより)

$$S_i^{(j)} = \log \frac{\Pr\left[y_i \middle| x_{j,i}, \boldsymbol{\theta_c}\right]}{\Pr\left[y_i \middle| \boldsymbol{\theta_c}\right]}$$

$$\Rightarrow \quad S^{(j)} = \sum_{i=1}^{L} S_i^{(j)}$$

総スコア

事後確率を最大にすることから
Maximum a Posteriori (MAP) detector
と呼ばれる

最適な検出器の導出(分母)

分母 $\Pr\left[y_i \middle| \boldsymbol{\theta_c}\right]$ を具体的に計算すると

$$\Pr\left[y_i = 1 \middle| \boldsymbol{\theta_c}\right] = \sum_{\rho=0}^{c} \theta_\rho \binom{c}{\rho} p_i^\rho (1-p_i)^{c-\rho}$$

$$\Pr\left[y_i = 0 \middle| \boldsymbol{\theta_c}\right] = 1 - \Pr\left[y_i = 1 \middle| \boldsymbol{\theta_c}\right]$$

符号生成確率の $\Pr[x_{j,i} = 1] = p_i$ と結託者数 c 及び

攻撃パラメータ $\boldsymbol{\theta_c} = (\theta_0, \theta_1, \ldots, \theta_c)$ が分かれば完全に導出できる

既知

未知

未知

最適な検出器の導出(分子)

分子 $\Pr\left[y_i \middle| x_{j,i}, \boldsymbol{\theta_c}\right]$ を具体的に計算すると

$$\Pr\left[y_i = 1 \middle| 0, \boldsymbol{\theta_c}\right] = \sum_{\rho=0}^{c-1} \theta_\rho \binom{c-1}{\rho} p_i^\rho (1-p_i)^{c-\rho-1}$$

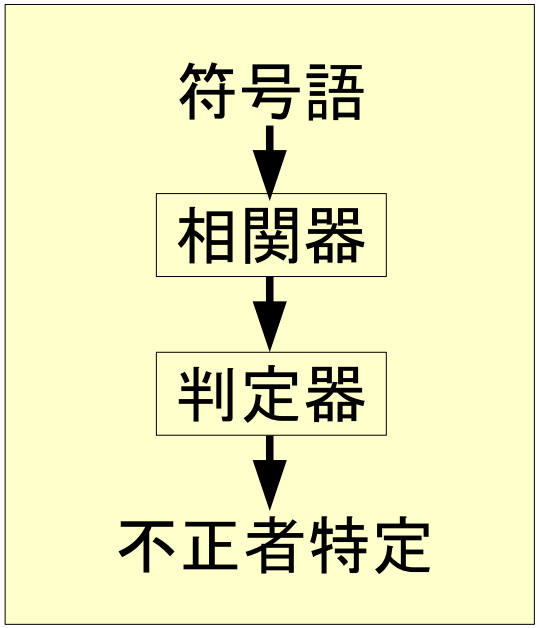
$$\Pr\left[y_i = 0 \middle| 0, \boldsymbol{\theta_c}\right] = 1 - \Pr\left[y_i = 1 \middle| 0, \boldsymbol{\theta_c}\right]$$

$$\Pr\left[y_i = 1 \middle| 1, \boldsymbol{\theta_c}\right] = \sum_{\rho=1}^{c} \theta_\rho \binom{c-1}{\rho-1} p_i^{\rho-1} (1-p_i)^{c-\rho}$$

$$\Pr\left[y_i = 0 \middle| 1, \boldsymbol{\theta_c}\right] = 1 - \Pr\left[y_i = 1 \middle| 1, \boldsymbol{\theta_c}\right]$$

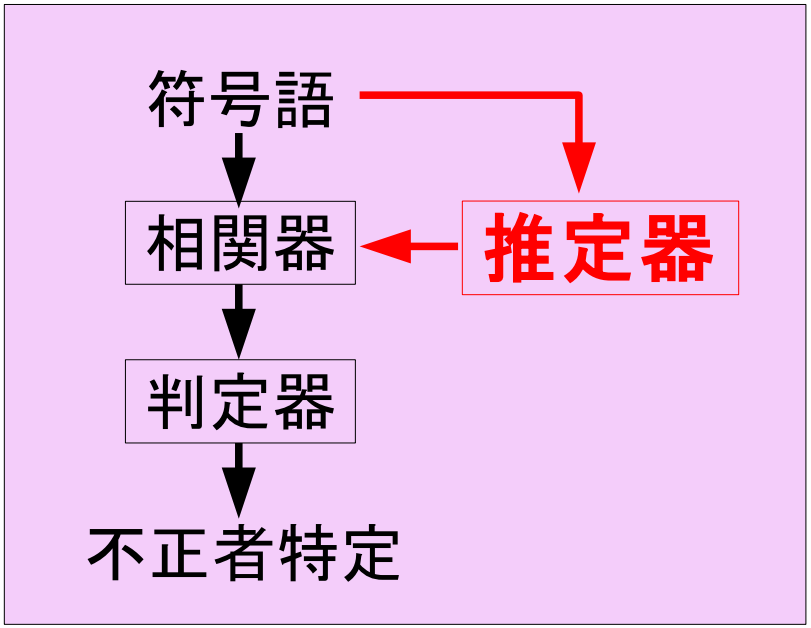
重要なポイント

従来モデル



攻撃の違いによる
検出性能の変化がない

新しいモデル

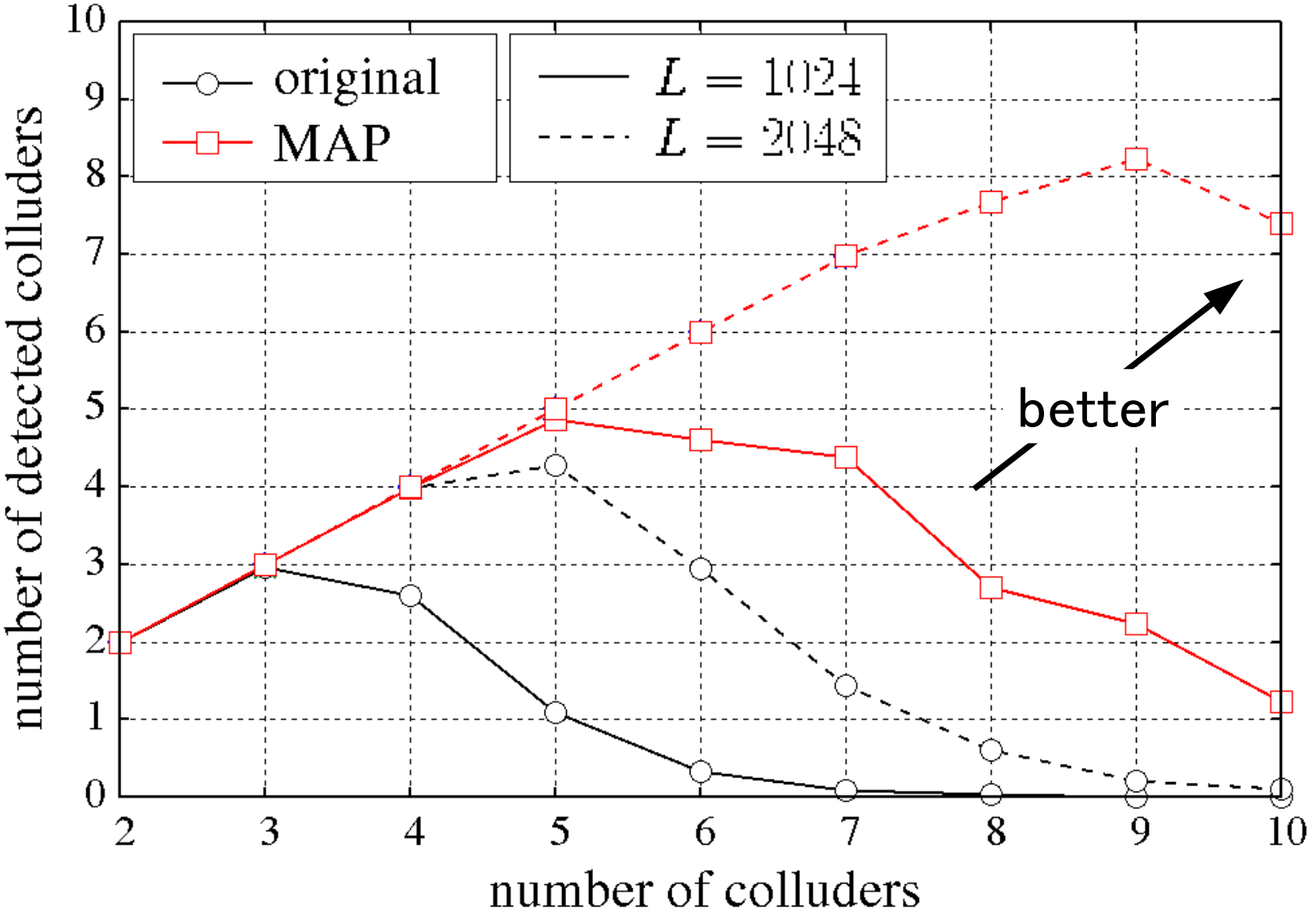


不正符号語から攻撃に関する情報を
推定する仕組みを導入

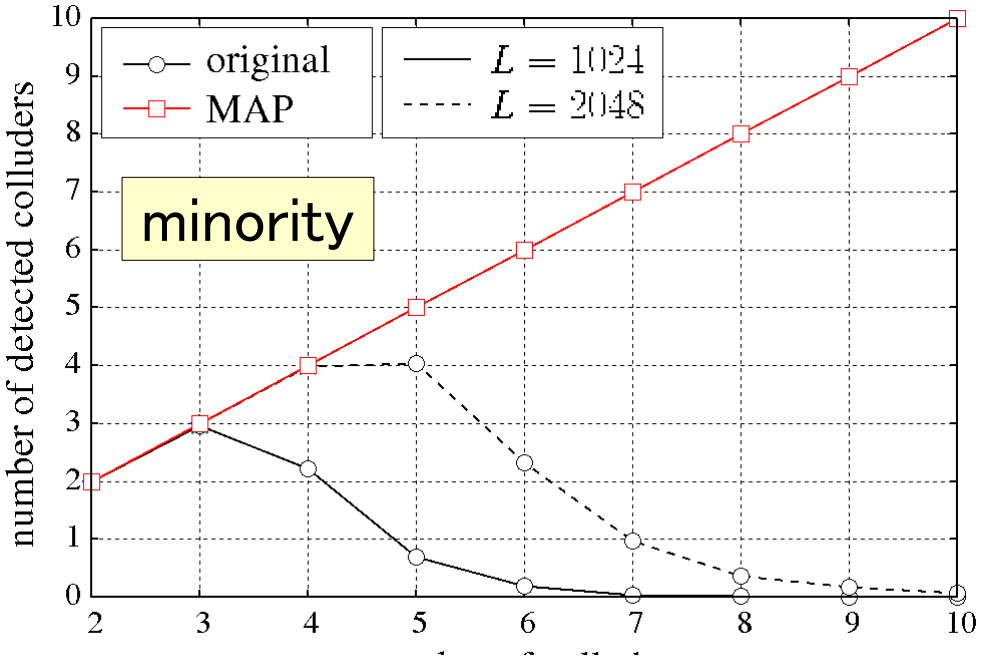
推定精度により検出性能が変化

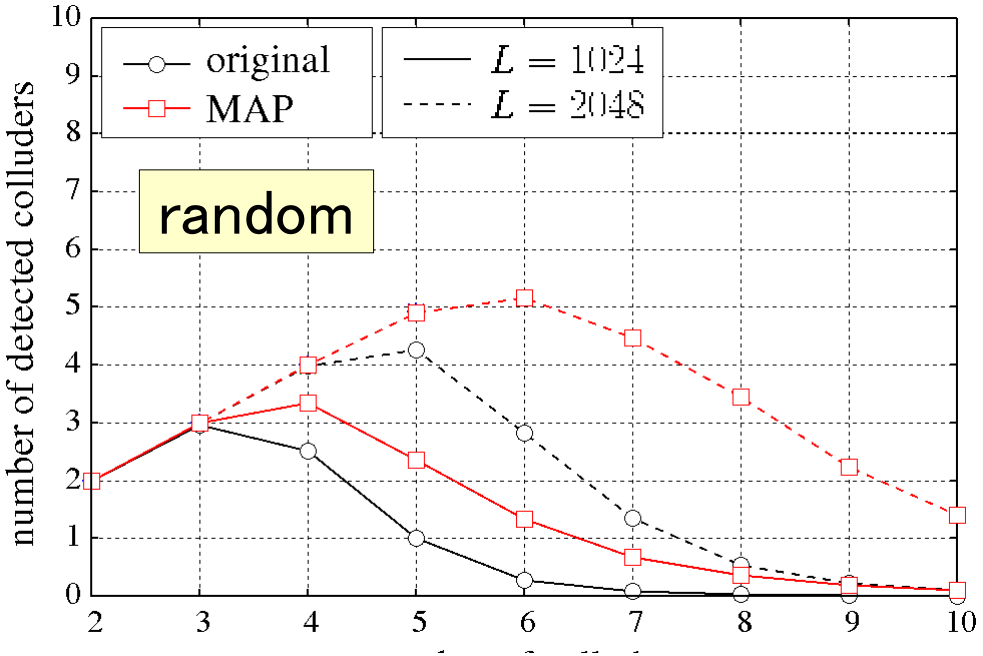
Majority攻撃に対する検出性能

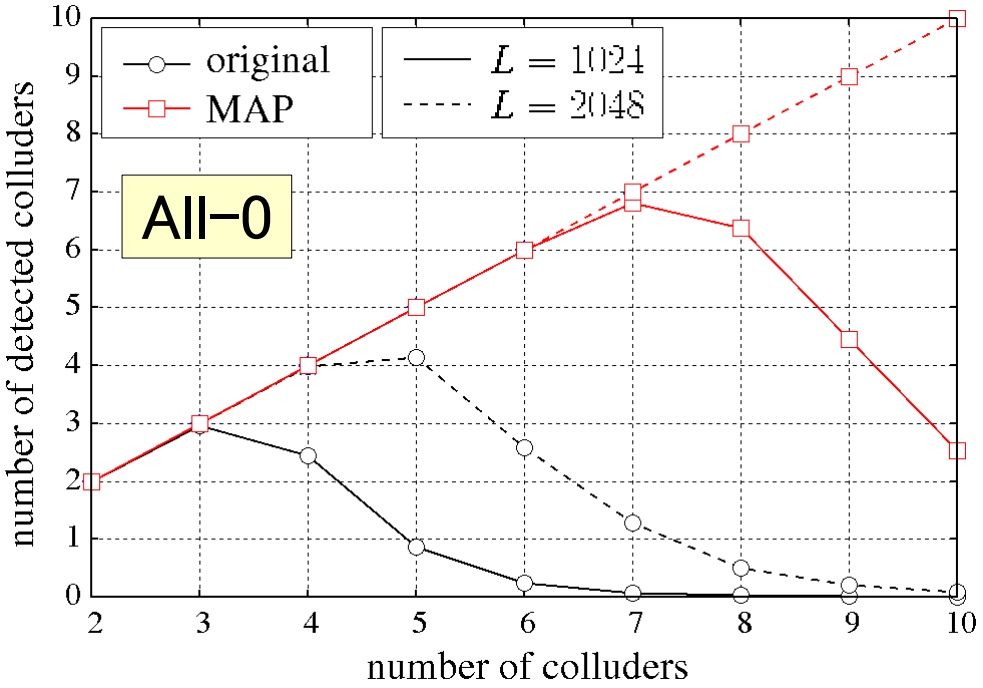
of users: 10000　　$\Pr[FP] = 10^{-8}$　　(Total: $\approx 10^{-4}$)

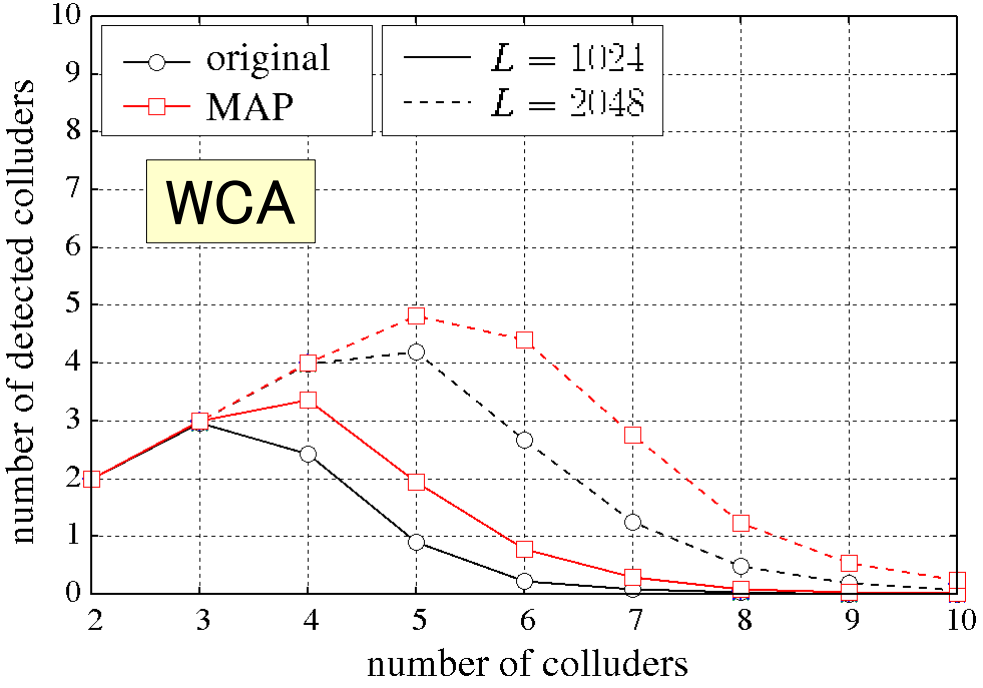


他の攻撃の場合


original
MAP
$L = 1024$
$L = 2048$
minority
number of detected colluders


original
MAP
$L = 1024$
$L = 2048$
random
number of detected colluders


original
MAP
$L = 1024$
$L = 2048$
All−0
number of detected colluders
number of colluders


original
MAP
$L = 1024$
$L = 2048$
WCA
number of detected colluders
number of colluders

Outline

- 電子指紋符号とその検出器
- Tardos符号と関連研究
- 結託攻撃の定式化
- 最適な検出器の設計
- **最近の研究紹介**
- 今後の展望

推定器の問題点

推定器　不正符号語から推定する

- 結託者数 c
- 結託攻撃パラメータ θ

問題点

- 莫大な計算量が必要
- 推定誤差の問題
- 雑音の存在する場合を考慮していない

簡略版MAP検出器

推定器が不要な簡略版の検出器の設計

M. Kuribayashi, "Simplified MAP detector for binary fingerprinting code embedded by spread spectrum watermarking scheme," IEEE Trans. Information Forensics and Security, vol.9, no.4, pp.610-623, 2014.

- スペクトル拡散型の埋め込み手法により，攻撃モデルを制限

  平均化攻撃 + 雑音付加

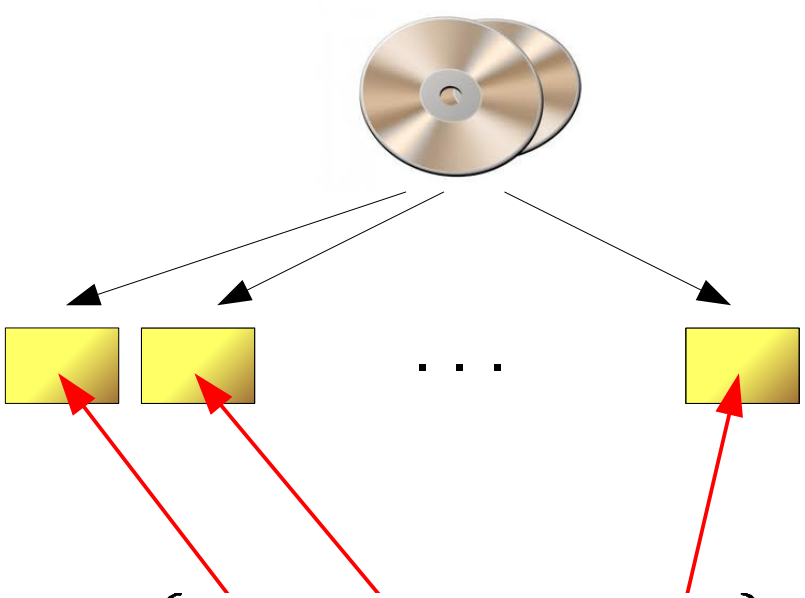
- 離散型のバイアス分布を利用

  符号語シンボルをグループ分け

- 二項分布を正規分布で近似

システムモデル

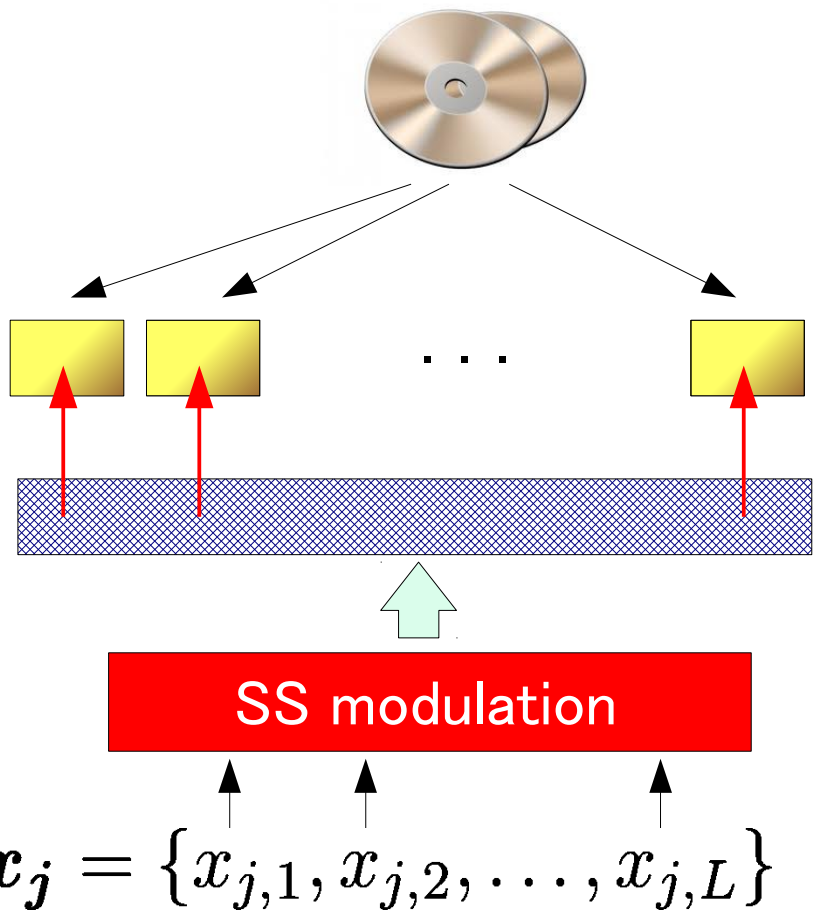
従来モデル



$$\boldsymbol{x}_j = \{x_{j,1}, x_{j,2}, \ldots, x_{j,L}\}$$

マーキング仮定に基づく
任意の攻撃が可能

提案モデル



$$\boldsymbol{x}_j = \{x_{j,1}, x_{j,2}, \ldots, x_{j,L}\}$$

この場合，平均化攻撃 が最も
信号レベルを減少できる

平均化攻撃によるシンボルの出現頻度

不正符号語 $y_i = \frac{1}{c}\sum_{t=1}^{c} x_{j_t,i} \quad (1 \le i \le L)$

(平均化攻撃を想定)

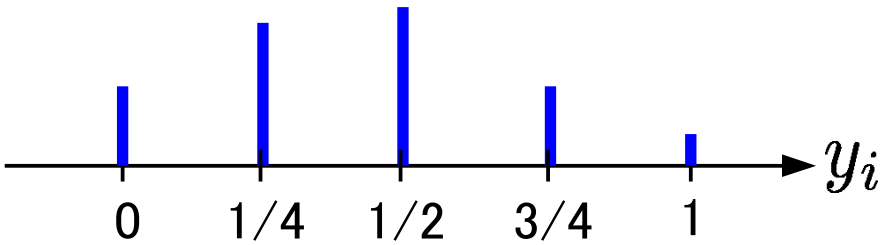
不正者数 : c

$y_i \in \left\{0, \frac{1}{c}, \frac{2}{c}, \ldots, 1\right\}$

bias probability

$\Pr[x_{j,i} = 1] = p_i$

例) 不正者数が c=4 のときの確率密度関数(PDF)は



二項分布となる

$$\Pr\left[y_i = \frac{\rho}{c}\middle|\boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right] = \binom{c}{\rho} p_i^{\rho}(1-p_i)^{c-\rho}$$

平均化攻撃 $\boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}$

MAP detector

ユーザ j の符号語　$\boldsymbol{x_j} = \{x_{j,1}, x_{j,2}, \ldots, x_{j,L}\}$　$x_{j,i} \in \{0, 1\}$

$$\Pr[x_{j,i} = 1] = p_i$$　(bias probability)

情報理論的に最適な検出器

$$y_i \in \left\{0, \frac{1}{c}, \frac{2}{c}, \ldots, 1\right\}$$

MAP detector

$$S_i^{(j)} = \log \frac{\Pr\left[y_i \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]}{\Pr\left[y_i \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]}$$

二項分布

$$\Pr\left[y_i = \frac{\rho}{c} \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right] = \binom{c}{\rho} p_i^{\rho} (1 - p_i)^{c-\rho}$$

同じように $\Pr\left[y_i \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]$ も計算できる

MAP detector

ユーザ j の符号語　$\boldsymbol{x_j} = \{x_{j,1}, x_{j,2}, \ldots, x_{j,L}\}$　$x_{j,i} \in \{0, 1\}$

$$\Pr[x_{j,i} = 1] = p_i$$　(bias probability)

情報理論的に最適な検出器

$$y_i \in \left\{0, \frac{1}{c}, \frac{2}{c}, \ldots, 1\right\}$$

MAP detector

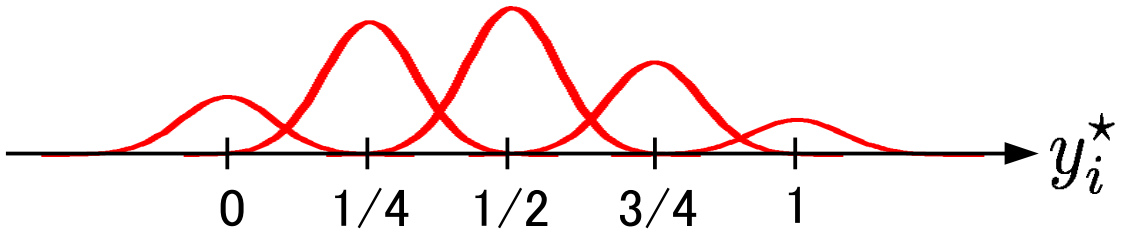
$$S_i^{(j)} = \log \frac{\Pr\left[y_i \middle| x_{j,i}, \boldsymbol{\theta_c^{(ave)}}\right]}{\Pr\left[y_i \middle| \boldsymbol{\theta_c^{(ave)}}\right]}$$

$$S_i^{(j)} = \begin{cases} \log \dfrac{1 - y_i}{1 - p_i} & \text{if } x_{j,i} = 0 \\ \log \dfrac{y_i}{p_i} & \text{otherwise} \end{cases}$$

AWGNを想定した場合

信号領域では，不正符号語に雑音が加わる

例）もしAWGNを仮定すると，PDFは



ガウス混合分布
(GMM)となる

$$pdf(y_i^\star) = \sum_{\rho=0}^{c} a_\rho \mathcal{N}\left(y_i^\star; \frac{\rho}{c}, \sigma_e^2\right)$$

where $\sum_{\rho=0}^{c} a_\rho = 1$ and $\mathcal{N}\left(y_i^\star; \frac{\rho}{c}, \sigma_e^2\right) = \frac{1}{\sqrt{2\pi\sigma_e^2}} \exp\left(-\frac{(y_i^\star - \frac{\rho}{c})^2}{2\sigma_e^2}\right)$

MAP detector (AWGN)

GMMのパラメータを正しく推定できれば，最適な検出器を利用可能

→ EMアルゴリズムを利用

MAP detector

$$S_i^{(j)} = \log \frac{\Pr\left[y_i^\star \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]}{\Pr\left[y_i^\star \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]}$$

$$\Pr\left[y_i^\star \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right] = \sum_{\rho=0}^{c} \mathcal{N}\left(y_i^\star; \frac{\rho}{c}, \sigma_e^2\right) \binom{c}{\rho} p_i^\rho (1-p_i)^{c-\rho}$$

同じように $\Pr\left[y_i^\star \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]$ も計算できる

Tardos符号の生成

符号語 $\boldsymbol{x_j} = \{x_{j,1}, x_{j,2}, \ldots, x_{j,i}, \ldots, x_{j,L}\}$ L: 符号長

各要素はバイナリ $= p_i$

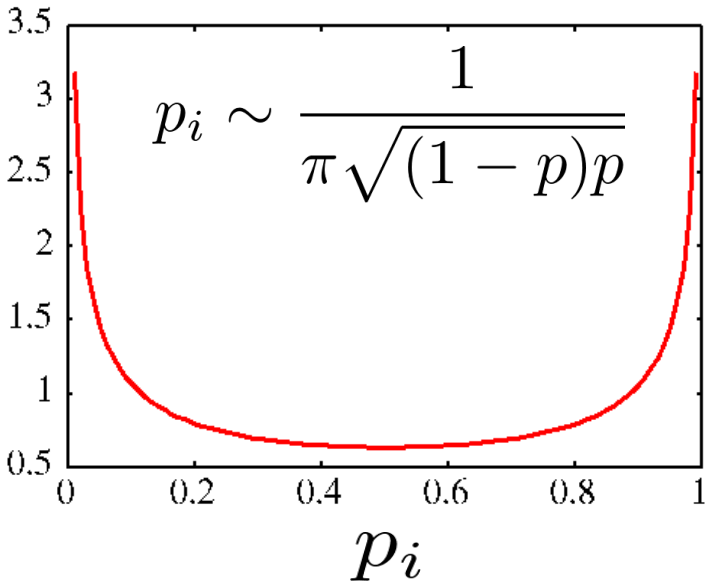
確率p_iに

Tardos符号では

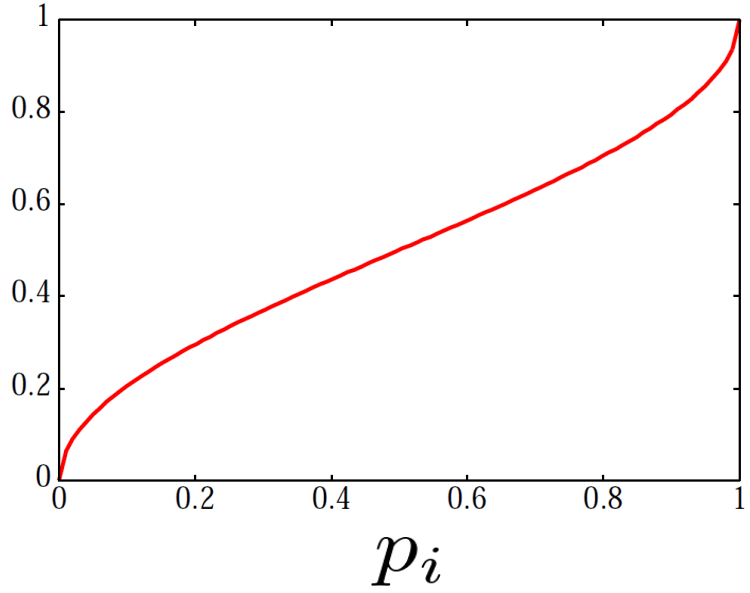
連続型のバイアス分布

を想定している

確率密度関数(PDF)



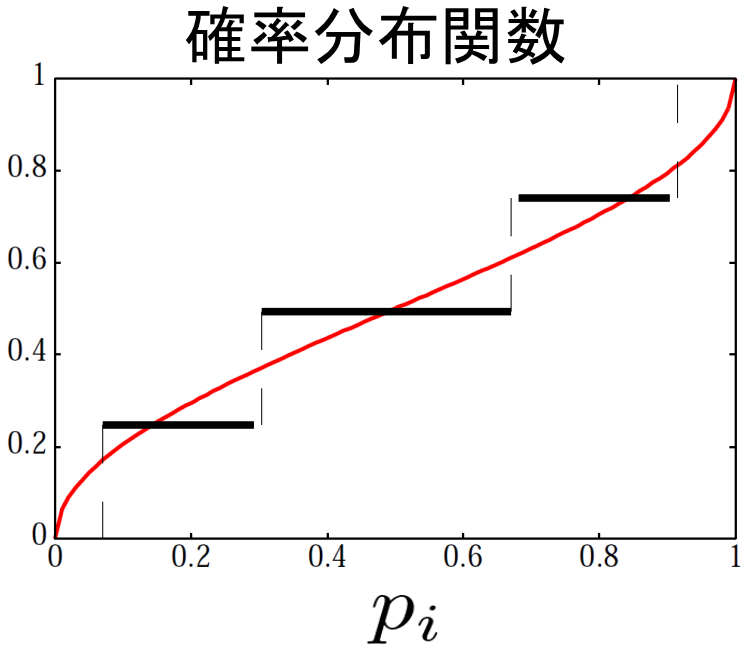
確率分布関数



離散型のバイアス分布

結託者数に応じて **離散的** に
確率 p_i を与える

離散型のバイアス分布



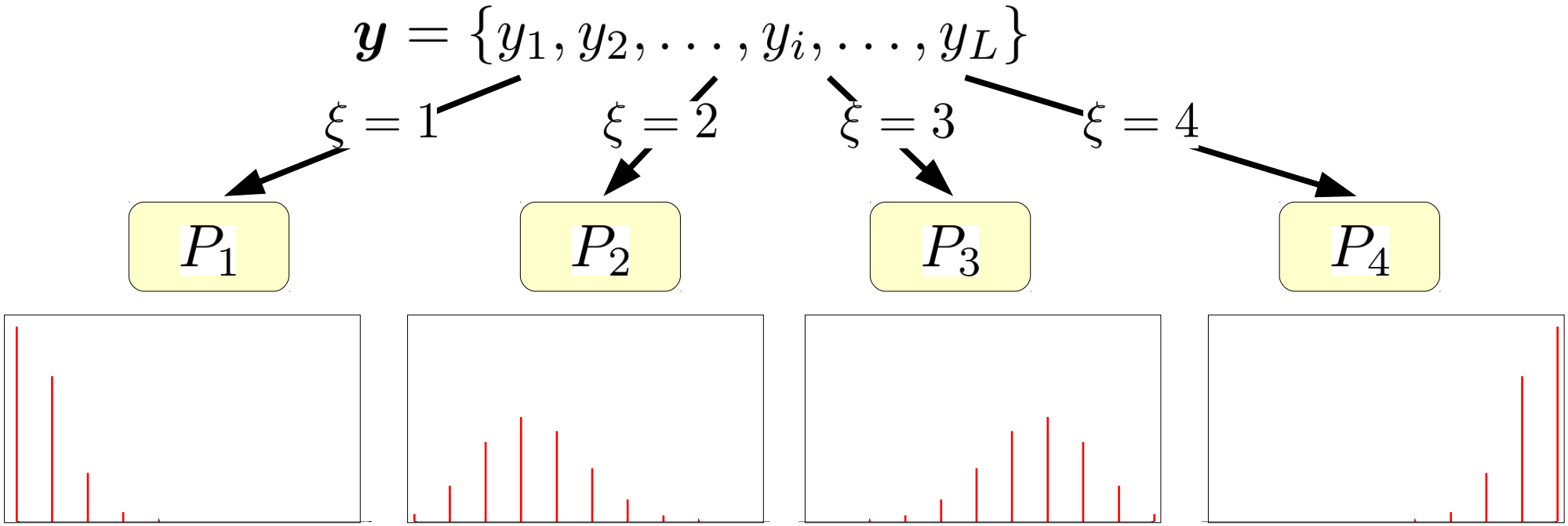
e.g) Nuida code $c_{max} = 7, 8$

ξ	p_i	q_i
1	0.06943	0.24833
2	0.33001	0.25167
3	0.66999	0.25167
4	0.93057	0.24833

離散型の確率を利用して
グループに分割

二項分布の近似

符号語を p_i に応じてグループに分割

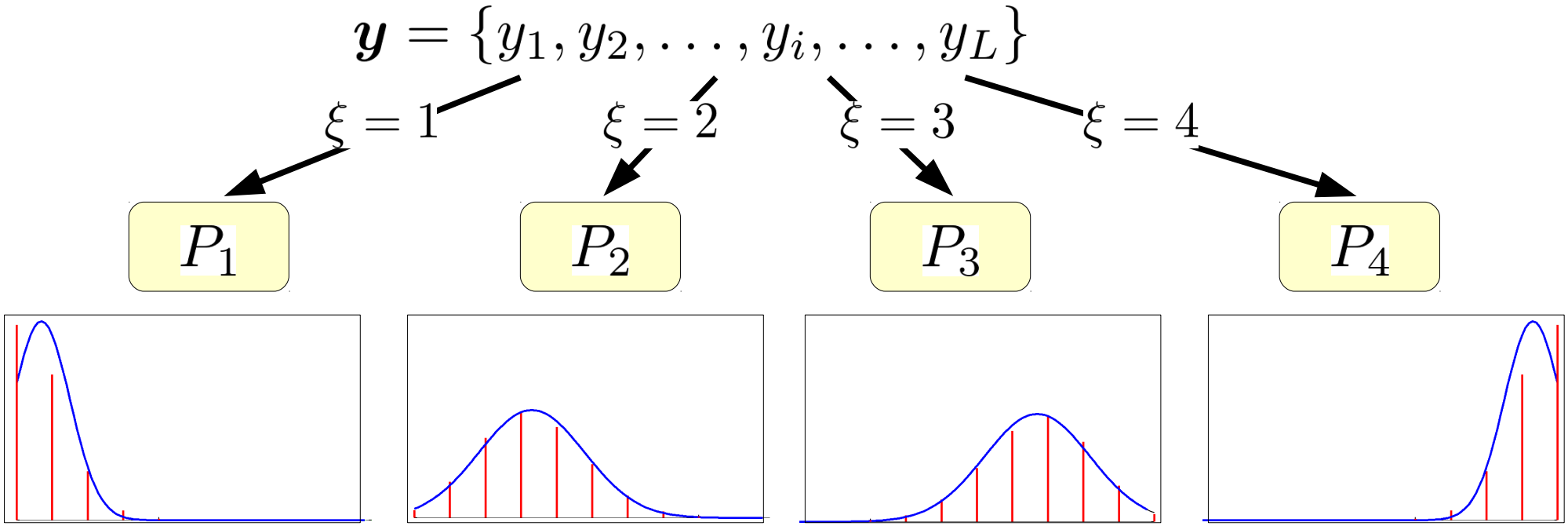


e.g) Distribution of $\Pr\left[y_i \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(ave)}\right]$ when c = 10.

結託者数 c が十分大きければ二項分布は正規分布に近似可能

二項分布の近似

符号語を p_i に応じてグループに分割



e.g) Distribution of $\Pr\left[y_i \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}\right]$ when c = 10.

近似式 $\Pr\left[y_i \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right] \approx \frac{1}{c}\mathcal{N}(y_i; P_\xi, \sigma_\xi^2)$ σ_ξ^2 : 分散値

雑音を想定した場合

雑音としてAWGNを仮定すると　$\boldsymbol{y}^{\star} = \boldsymbol{y} + \boldsymbol{e}$

$\boldsymbol{e} \sim \mathcal{N}(0, \sigma_e^2)$

AWGN

各グループ $1 \leq \xi \leq 4$ において相関値を計算

MAP detector

$$S_{i,\xi}^{(j)} = \log \frac{\Pr\left[y_i^{\star} \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right]}{\Pr\left[y_i^{\star} \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right]}$$

最終的に総スコアを求めれば良い

$$S^{(j)} = \sum_{\xi=1}^{4} \left(\sum S_{\xi,i}^{(j)} \right)$$

雑音を想定した場合

雑音としてAWGNを仮定すると　$\boldsymbol{y}^\star = \boldsymbol{y} + \boldsymbol{e}$

$\boldsymbol{e} \sim \mathcal{N}(0, \sigma_e^2)$

AWGN

各グループ $1 \leq \xi \leq 4$ において相関値を計算

MAP detector

$$S_{i,\xi}^{(j)} = \log \frac{\Pr\left[y_i^\star \middle| x_{j,i}, \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right]}{\Pr\left[y_i^\star \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right]}$$

最終的に総スコアを求めれ

$$S^{(j)} = \sum_{\xi=1}^{4} \left(\sum S_{\xi,i}^{(j)} \right)$$

近似式を用いれば

$$\Pr\left[y_i^\star \middle| \boldsymbol{\theta}_{\boldsymbol{c}}^{(\boldsymbol{ave})}, \xi\right] \approx \frac{1}{c} \mathcal{N}(y_i^\star; P_\xi, \tilde{\sigma}_\xi^2)$$

ただし $\tilde{\sigma}_\xi^2 = \sigma_\xi^2 + \sigma_e^2$

簡略化MAP検出器

更に近似計算を用いて簡略化すれば,

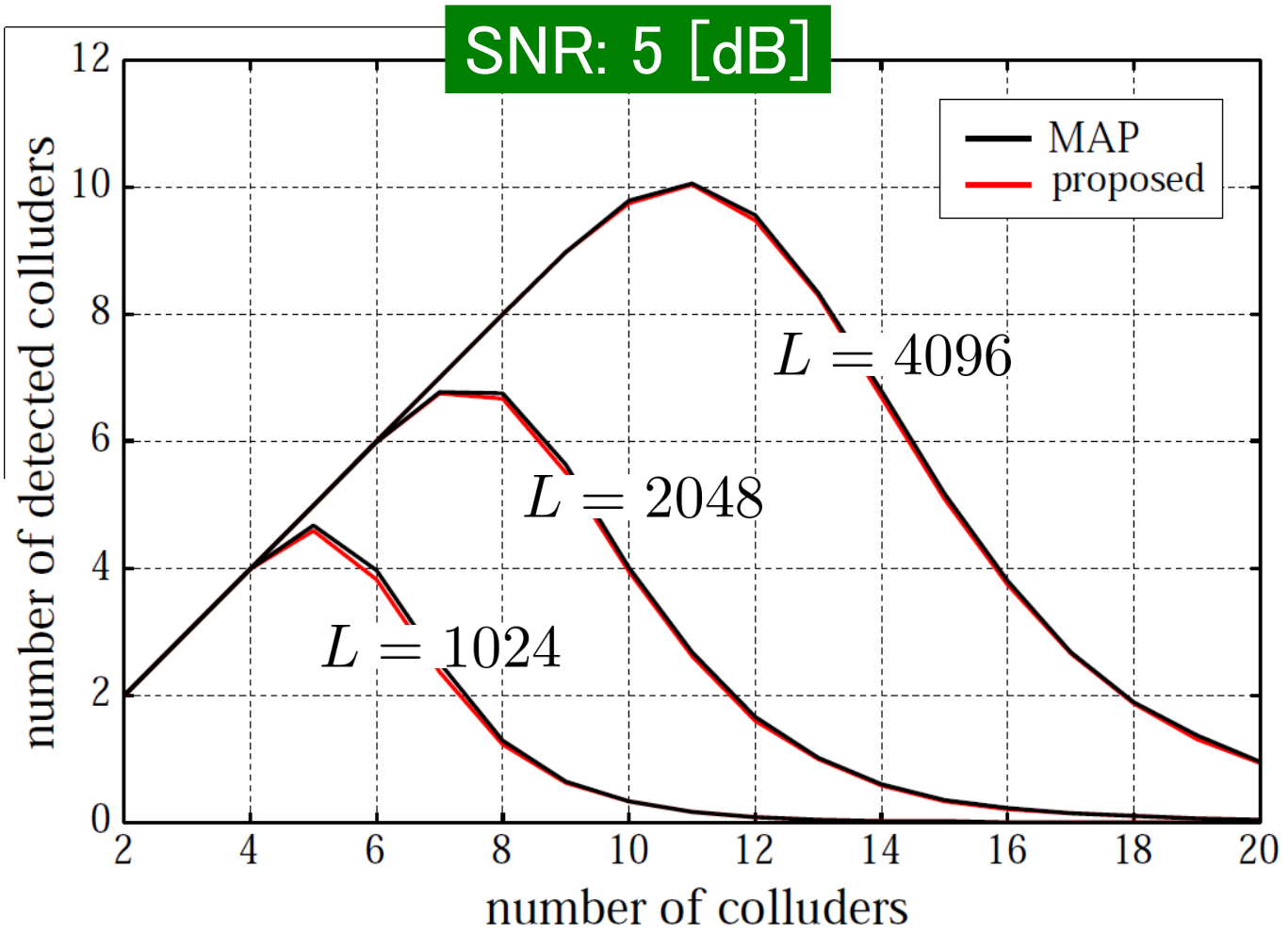
$$S_{\xi,i}^{(j)} = \begin{cases} 0 & \text{if } x_{j,i} = 0 \\ y_i^\star - P_\xi & \text{if } x_{j,i} = 1 \end{cases}$$

特徴

上記スコア $S_{\xi,i}^{(j)}$ は結託者数 c も分散値 σ_e^2 も含まない

近似式の有効性は計算機シミュレーションで確認

実験結果(検出性能)



# of users: 10000

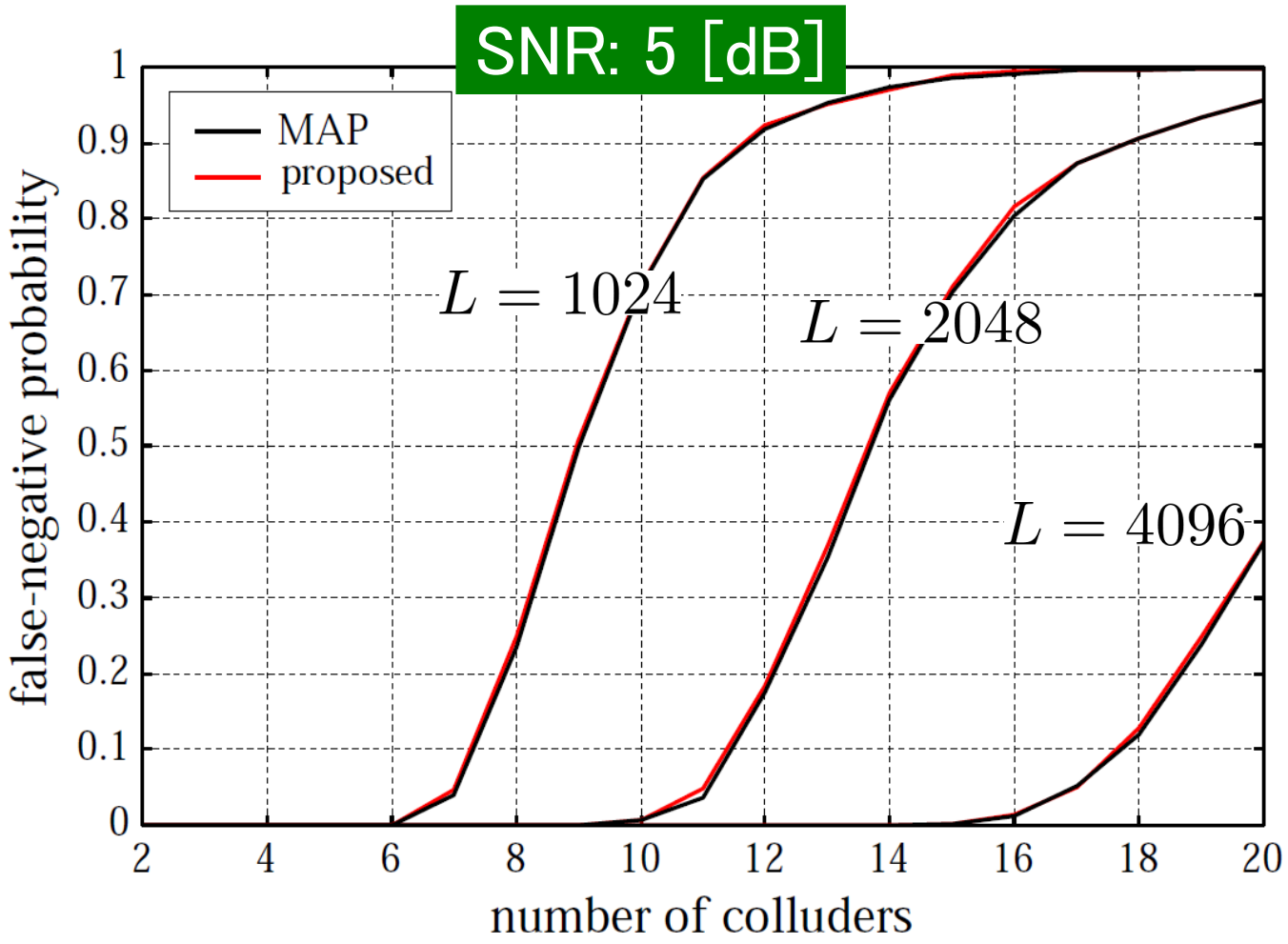
$\Pr[FP] = 10^{-8}$

(Total: $\approx 10^{-4}$)

MAP detector knows c, but estimates σ_e^2 using the EM algorithm.

簡略化MAP(提案方式)の性能は最適な検出器と極めて近い

実験結果(誤検出率)



# of users: 10000

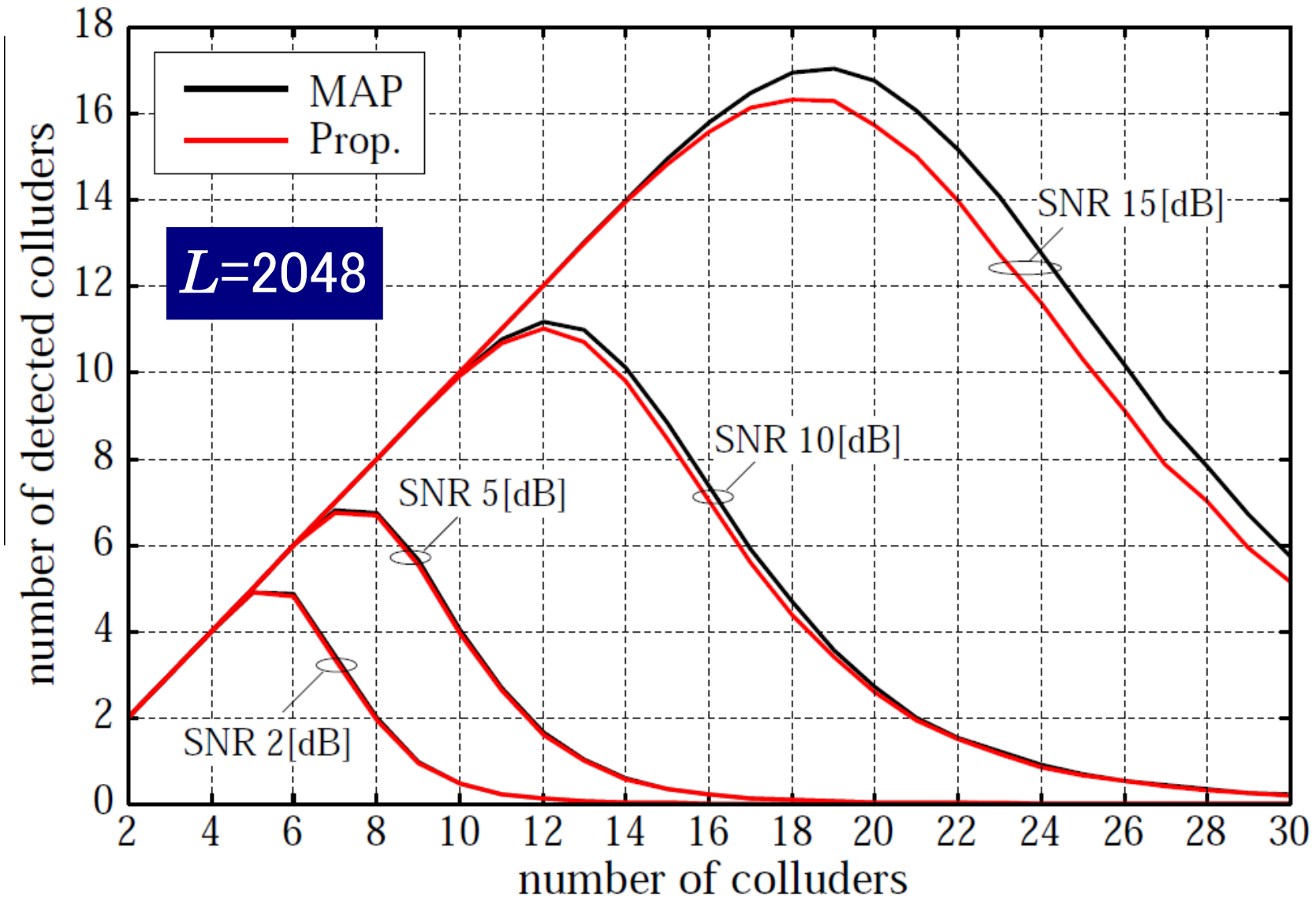
$\Pr[FP] = 10^{-8}$

(Total: $\approx 10^{-4}$)

MAP detector knows c,
but estimates σ_e^2
using the EM algorithm.

簡略化MAP(提案方式)の性能は最適な検出器と極めて近い

Comparison of Traceability



雑音が少ないと簡略化MAPの性能がわずかに低下

Outline

- 電子指紋符号とその検出器
- Tardos符号と関連研究
- 結託攻撃の定式化
- 最適な検出器の設計
- 最近の研究紹介
- **今後の展望**

今後の展望

- ユーザごとに相関値を計算せずに，数人ずつまとめる

  Single detector → Joint detector

- バイナリではなく多元化させる

  攻撃仮定も多様化，符号生成および検出器の設計が複雑化

- 離散型バイアス分布の再考察

- 電子透かし技術を用いた環境下での攻撃まで考慮

最後までお付き合い頂き
ありがとうございました