SITA2009 ワークショップ

# スペクトル拡散技術と電子透かし

栗林 稔

神戸大学大学院工学研究科

# 目次

- スペクトル拡散技術を用いた電子透かし
- CDMA技術に基づく電子指紋方式
- 干渉成分の抑制と除去
- 量子化誤差による影響
- 今後の展望

# 電子透かし

ディジタルコンテンツに密かに別の情報を埋め込む技術

- fragile watermark （弱い電子透かし）

  コンテンツに少しでも加工が加えられると検出できない

  → コンテンツの原本性を保障

  改ざん検知機能，改ざん位置特定機能，reversibility，etc.

- robust watermark

  悪意のある攻撃に対して耐性を有する

  → 著作権保護，不正者特定

  スペクトル拡散法，パッチワーク法，量子化法，etc.

# スペクトル拡散技術を用いた電子透かし

狭帯域の電子透かし信号を広帯域に拡散させてコンテンツに埋め込む

## 最初の論文

I. J. Cox, J. Kilian, F. Leighton, and T. Shamson,
“Secure Spread Spectrum Watermarking for Multimedia”
IEEE Trans. Image Process., vol.6, no.12, pp.1673-1687, 1997

## 各種攻撃に対して高い耐性

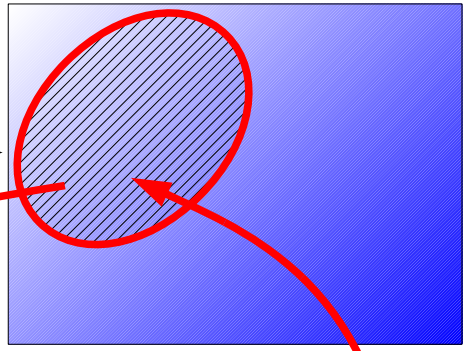
- 各種信号処理（非可逆圧縮，雑音付加，フィルタリング，etc.）
- 軽微な幾何学的改変（回転，拡大縮小，切り抜き，etc.）
- 結託攻撃

# Coxらの手法

## 埋め込み処理

spatial domain

直交変換

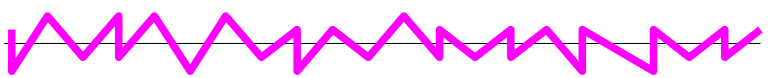


frequency domain

ランダムに選択

選択された周波数成分

信号の埋め込まれた周波数成分



スペクトル拡散系列

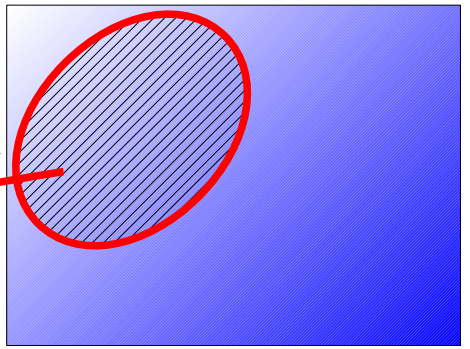
系列は正規分布 $N(0,1)$ に従う

# Coxらの手法（続き）

検出操作

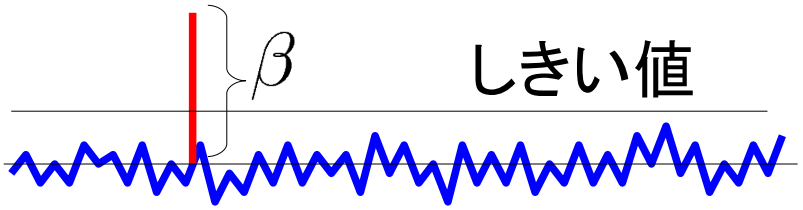
不正コピー

直交変換



frequency domain

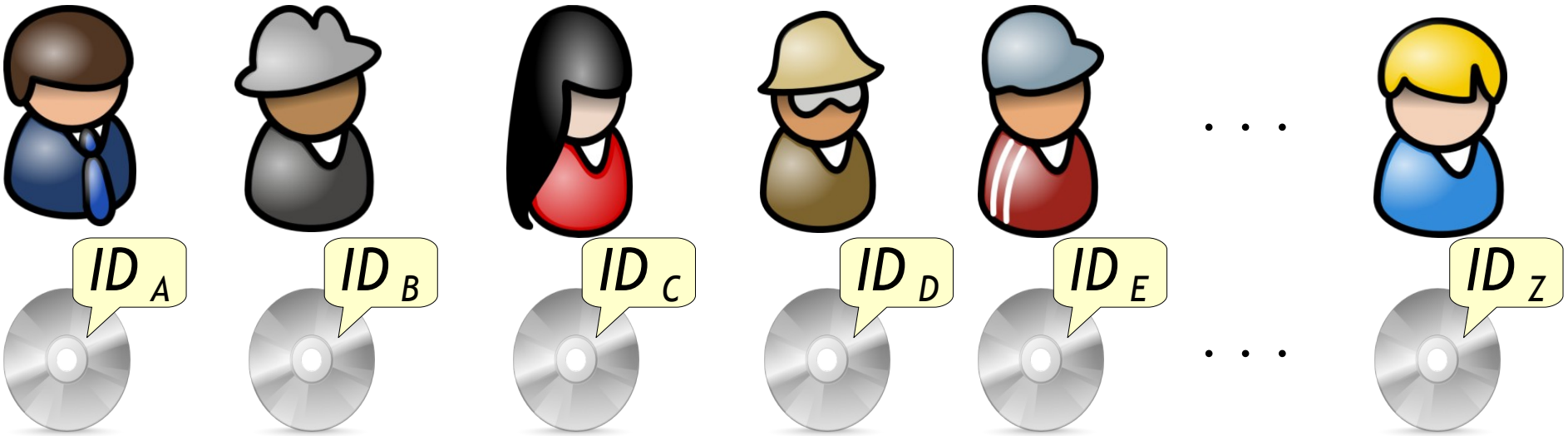
- 埋め込まれている信号を抽出
- 候補の信号との相関値を計算




相関値があるしきい値を超えれば
対応するユーザを不正者として検挙

# 結託攻撃

各ユーザは各自の電子指紋情報の埋め込まれたコンテンツを持つ




複数のユーザのコンテンツを比較すれば
その違いを調べて，指紋情報を除去/改変される

e.g.） averaging,　interleaving, etc.

# 結託攻撃(続き)

**線形結託攻撃**

$$\tilde{\boldsymbol{X}} = \sum_{i=1}^{c} a_i \boldsymbol{X_i} = a_1 \boldsymbol{X_1} + a_2 \boldsymbol{X_2} + a_3 \boldsymbol{X_3} + \cdots + a_c \boldsymbol{X_c}$$

$$\sum_{i=1}^{c} a_i = 1$$

**攻撃の目的** 不正コピーから結託者として検挙されないようにしたい

**攻撃モデル** 結託者は各自検挙されるリスクを背負いたくない

**不正コピー生成に対して各ユーザの貢献度は等しい**

# 結託攻撃による影響

H. Zhao, M. Wu, Z. Wang, and K. J. R. Liu,
“Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting”
IEEE Trans. Image, Process., vol.14, no.5, pp.646-661, 2005.

**スペクトル拡散技術を用いた電子透かしの場合**

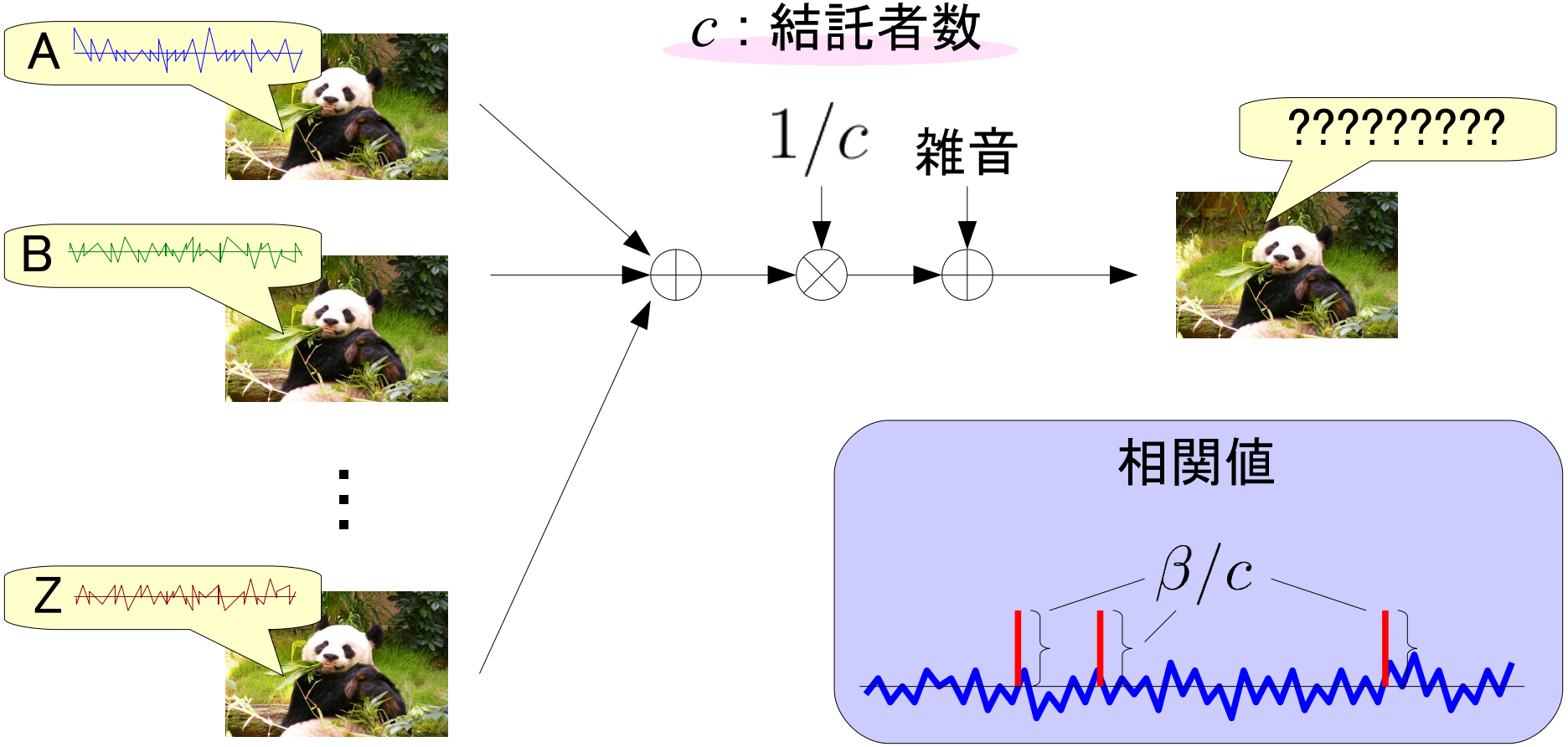
最悪の攻撃： 平均化攻撃

非線形な結託攻撃 ＝ 平均化攻撃 ＋ (ガウス)雑音付加

**結託攻撃モデル： 平均化攻撃 ＋ 雑音付加**

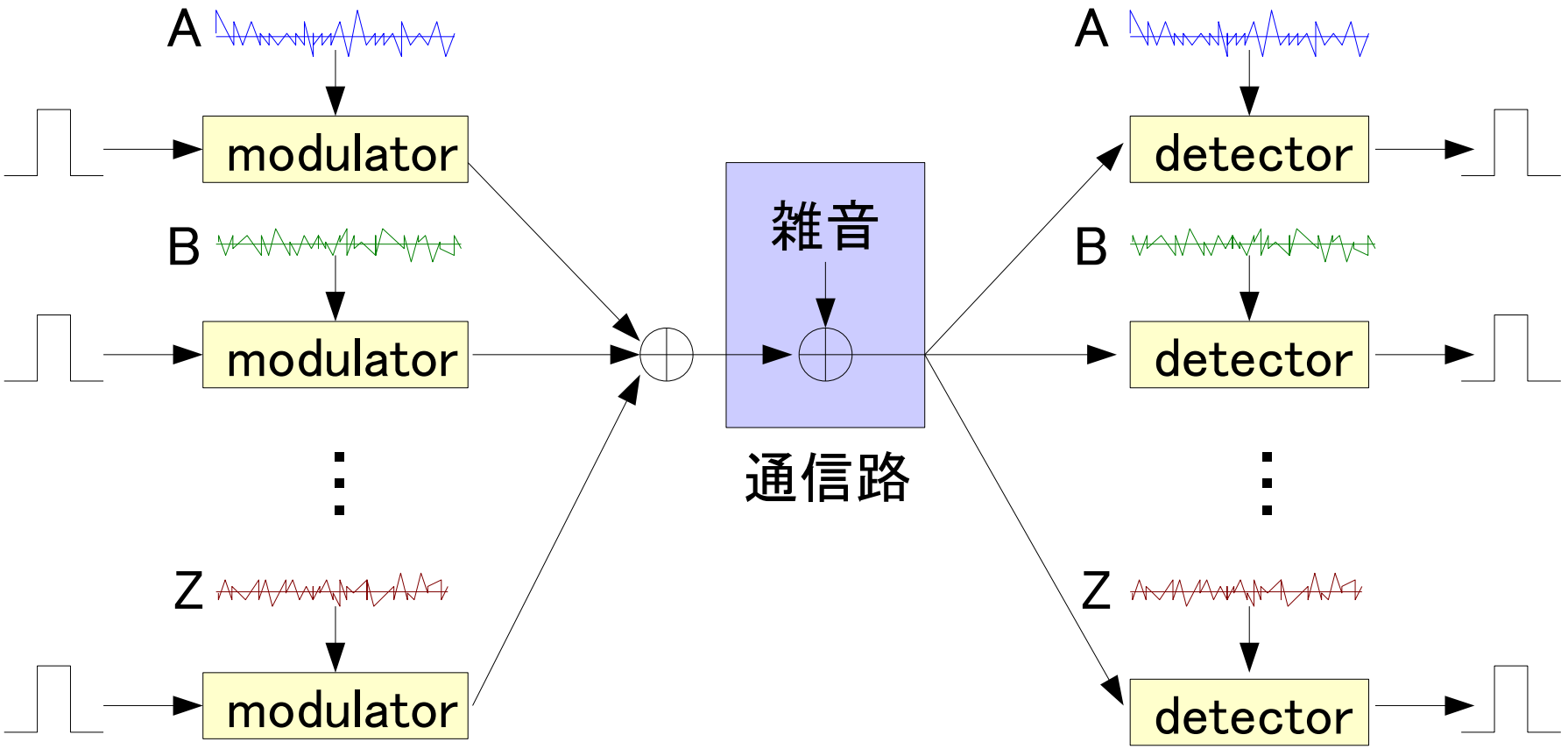
# 平均化攻撃

複数のコピーを平均化すれば，埋め込まれている信号が減衰する



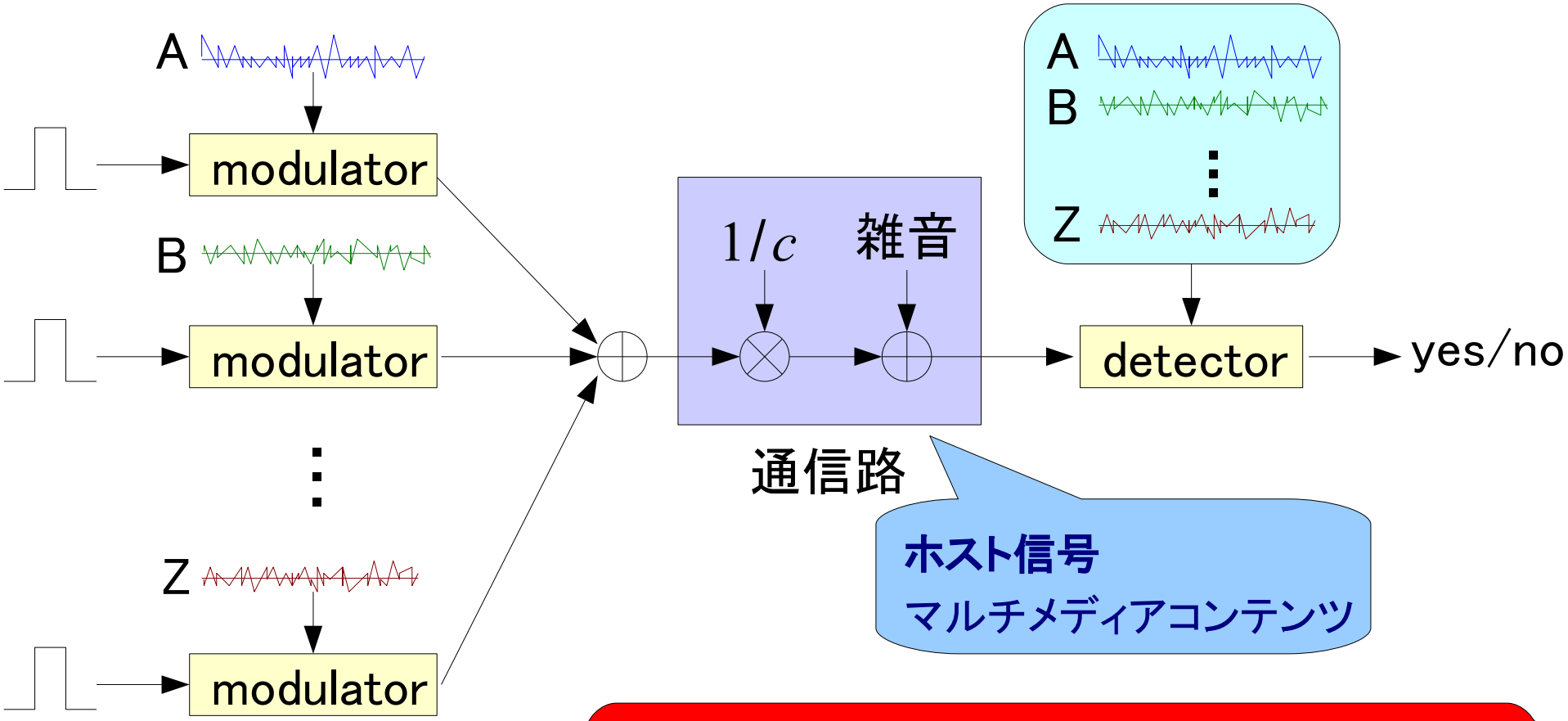
# Modeling

CDMA通信モデル



# Modeling

CDMA技術に基づく電子指紋技術のモデル

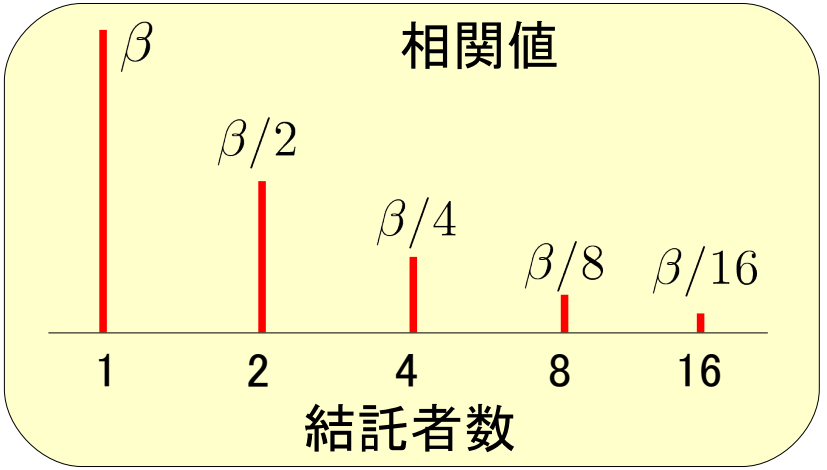



平均化攻撃 = 複数の電子指紋信号を多重化させて通信

# これまでの研究

スペクトル拡散技術を用いた電子透かしは，各種攻撃に対して強い耐性を有することが知られている

平均化攻撃を受けると，
相関値は結託者の人数$c$に
反比例して減衰する




結託者数が少なければ，適切に設定したしきい値を用いて結託者を特定可能

検出操作の計算量： $O(NL)$

$N$：総ユーザ数

$L$：系列長

# 目次

- スペクトル拡散技術を用いた電子透かし
- **CDMA技術に基づく電子指紋方式**
- 干渉成分の抑制と除去
- 量子化誤差による影響
- 今後の展望

# CDMA-Based Fingerprinting Scheme

N. Hayashi, M. Kuribayashi, M. Morii
“Collusion-Resistant Fingerprinting Scheme Based on the CDMA-Technique”
Proc. IWSEC2007, LNCS 4752, pp.28-43, Springer, 2007.

- 直交系列をPN系列で変調することで，理論的に疑似直交する拡散系列を生成

DCT基底をM系列で変調

- 擬似直交性を利用して，二種類のスペクトル拡散系列により階層構造を実現

グループID　ユーザID

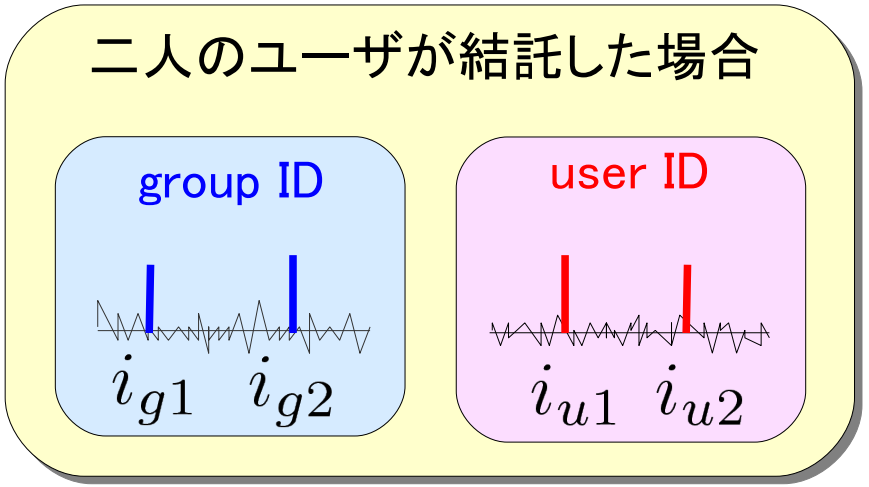
電子指紋情報 $(i_g, i_u)$

系列長 $\ell$ で
ユーザ数 $\ell^2$ を許容

- 設計上の誤検出率に基づいて，しきい値を計算

# 階層構造

もし二種類の系列を単純に組み合わせると




結託者IDの候補

Case1: $(i_{g1}, i_{u1})$ and $(i_{g2}, i_{u2})$

Case2: $(i_{g1}, i_{u2})$ and $(i_{g2}, i_{u1})$

一意に結託者を特定できない

**解決法**

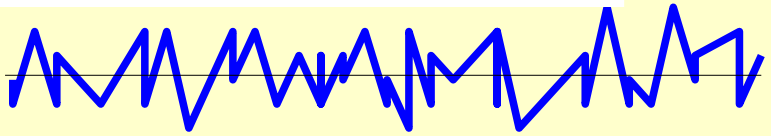
group ID と user ID の間に関係性を与える

# 電子指紋信号の生成

電子指紋情報 $(i_g, i_u)$ を含む系列の作成

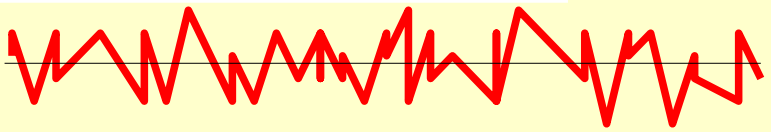
グループID　ユーザID

**グループIDを示す系列**



$$w_g = pn(s) \otimes dct(i_g, \beta_g)$$

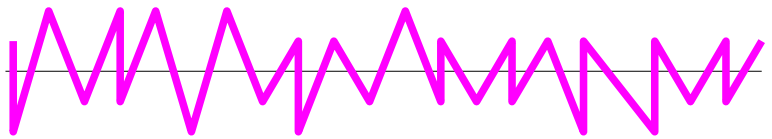
**ユーザIDを示す系列**



$$w_u = pn(i_g) \otimes dct(i_u, \beta_u)$$

秘密鍵 $s$ を基に
PN系列を生成

グループIDを基に
PN系列を生成



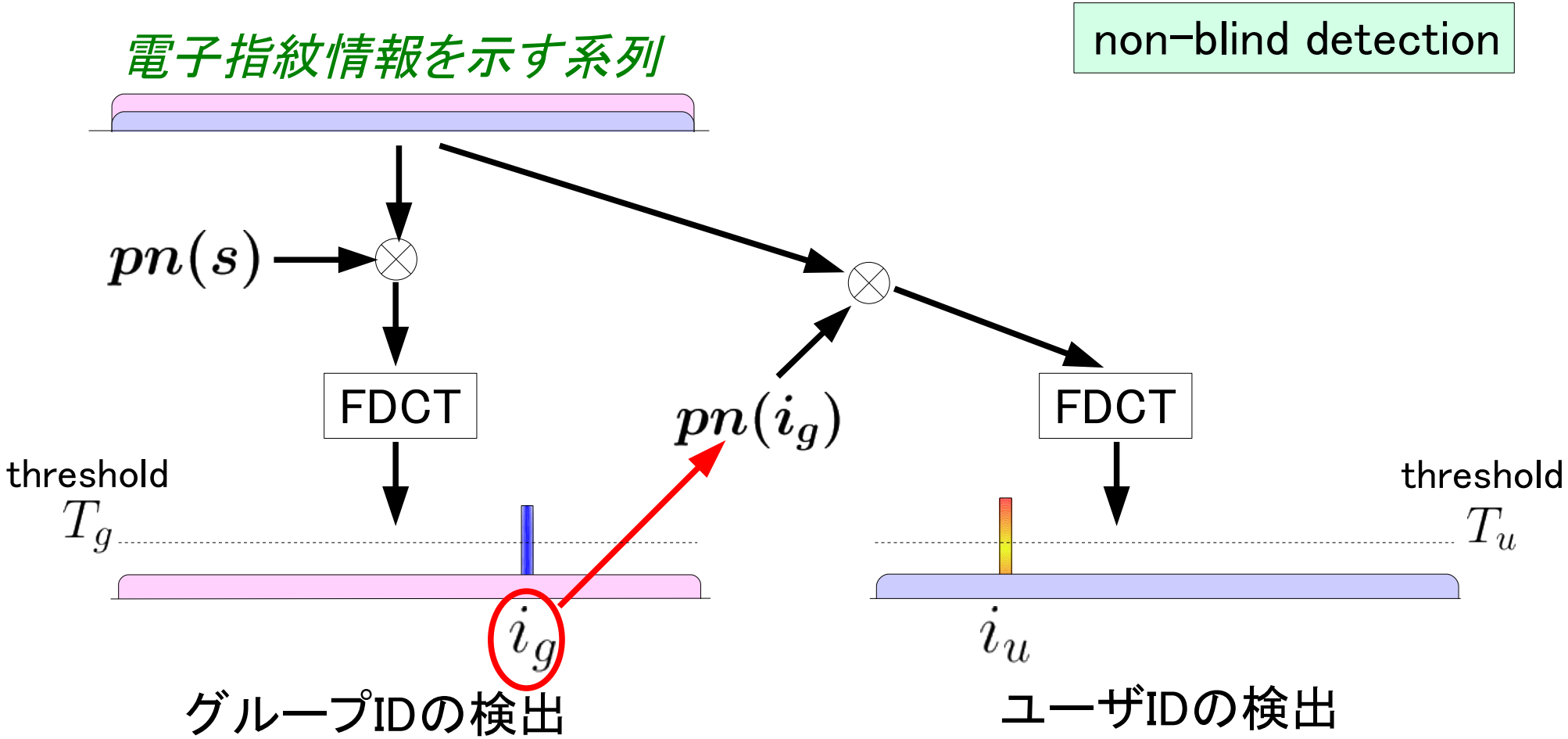
*電子指紋情報を示す系列*

$$w = w_g + w_u$$

# 検出手順

- 元のコンテンツを用いて不正コピーから電子指紋信号を検出

non-blind detection

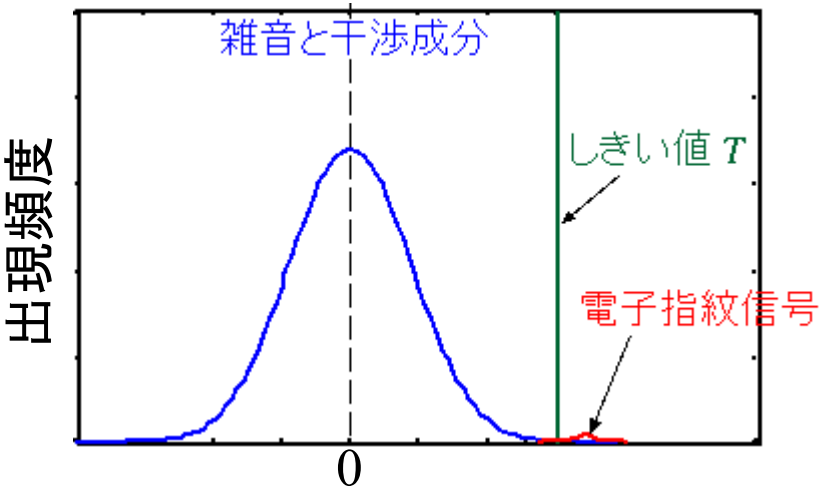



計算量: $\mathrm{O}(\sqrt{N}\log L)$　　(Coxらの手法: $\mathrm{O}(NL)$ )

# しきい値の求め方

結託者と無実のユーザのスペクトル拡散系列は擬似直交する

その干渉成分は平均0のガウス分布に近似できる




統計的な解析より

$$Pe = \frac{1}{2}\mathrm{erfc}\left(\frac{T}{\sqrt{2\sigma^2}}\right)$$

$Pe$ : false-positive probability

$\sigma^2$ : variance

誤検出率 $Pe$ が与えられれば，対応するしきい値 $T$ を計算できる

# 目次

- スペクトル拡散技術を用いた電子透かし
- CDMA技術に基づく電子指紋方式
- **干渉成分の抑制と除去**
- 量子化誤差による影響
- 今後の展望

# 繰り返し検出と干渉除去

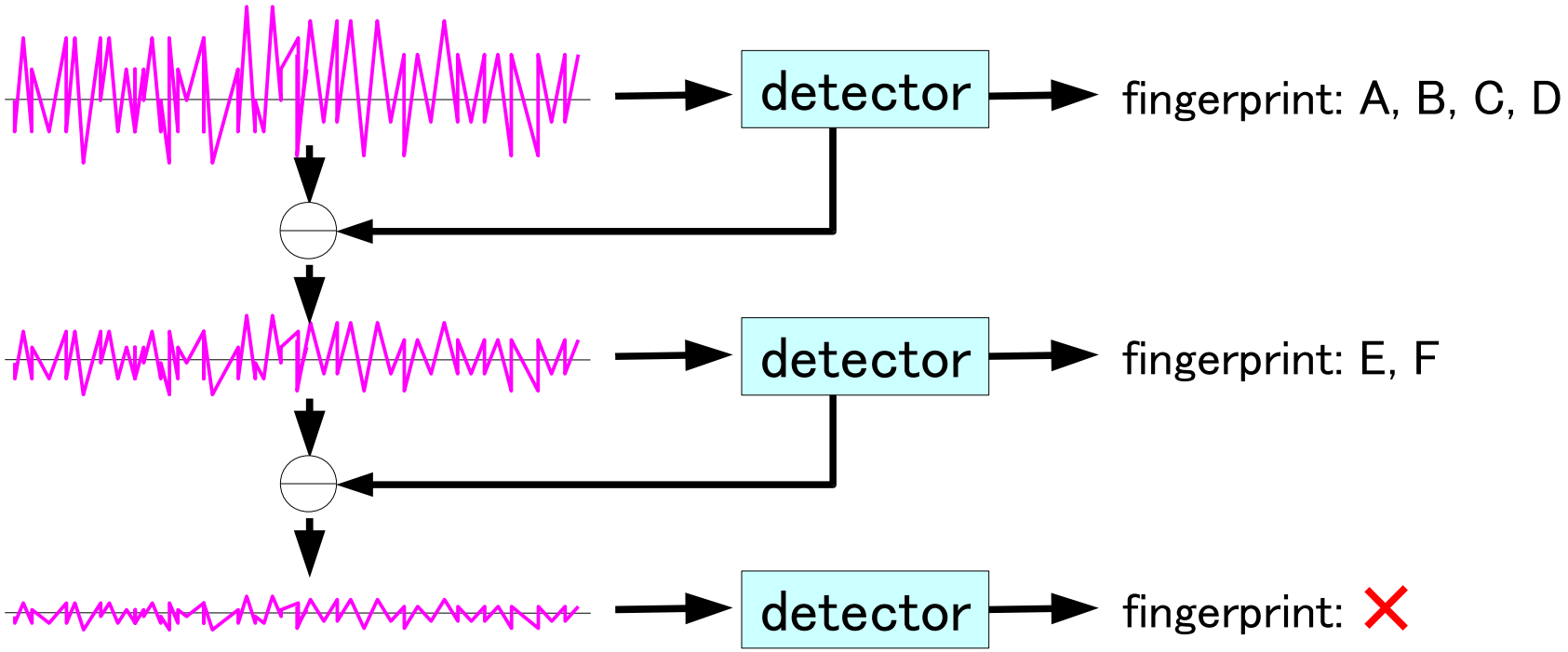
M. Kuribayashi and M. Morii
“Iterative Detection Method for CDMA-Based Fingerprinting Scheme,”
Proc. IH2008, LNCS 5284, pp.357-371, Springer, 2008.

- 干渉除去処理
  - 干渉成分を効果的に除去して検出性能を向上
- 繰り返し検出
  - 検出された電子指紋信号成分を除去した後に再度検出を試みることで，干渉成分に埋もれていた信号を検出できる
- 二種類のしきい値の設定
  - 信号除去と繰り返し検出の操作を効果的に行う

# 繰り返し検出と干渉除去

M. Kuribayashi and M. Morii
“Iterative Detection Method for CDMA-Based Fingerprinting Scheme,”
Proc. IH2008, LNCS 5284, pp.357-371, Springer, 2008.

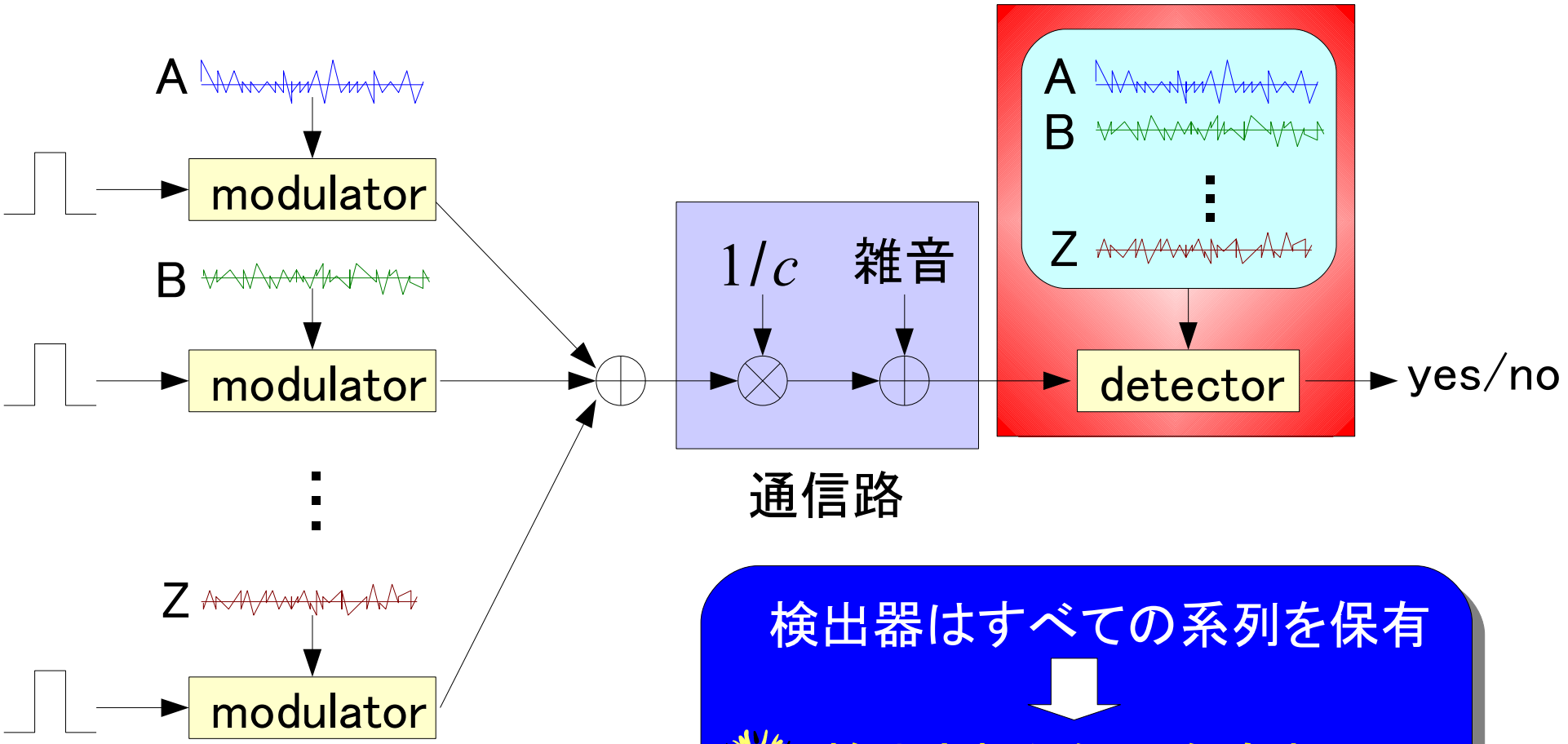
例) 結託者6人 (A, B, C, D, E, F)




電子指紋信号が検出されなくなれば繰り返し操作を終了

# Modeling

CDMA技術に基づく電子指紋技術のモデル




検出器はすべての系列を保有

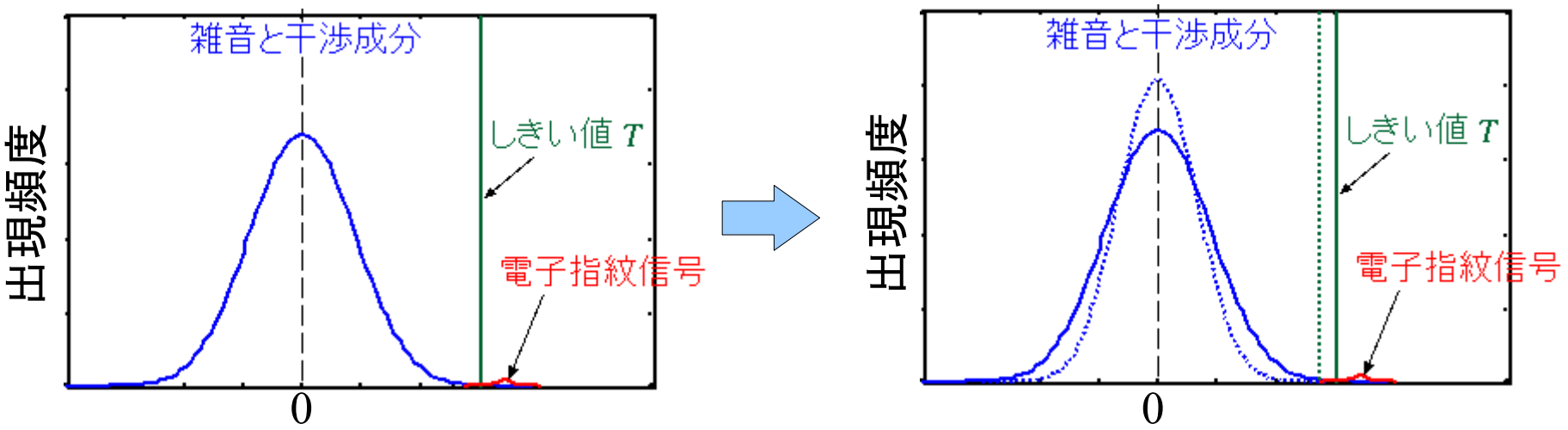
検出された信号を除去して
干渉成分を抑制

# 干渉除去による効果

誤検出率を設定して
しきい値$T$を計算

$$Pe = \frac{1}{2}\mathrm{erfc}\left(\frac{T}{\sqrt{2\sigma^2}}\right)$$

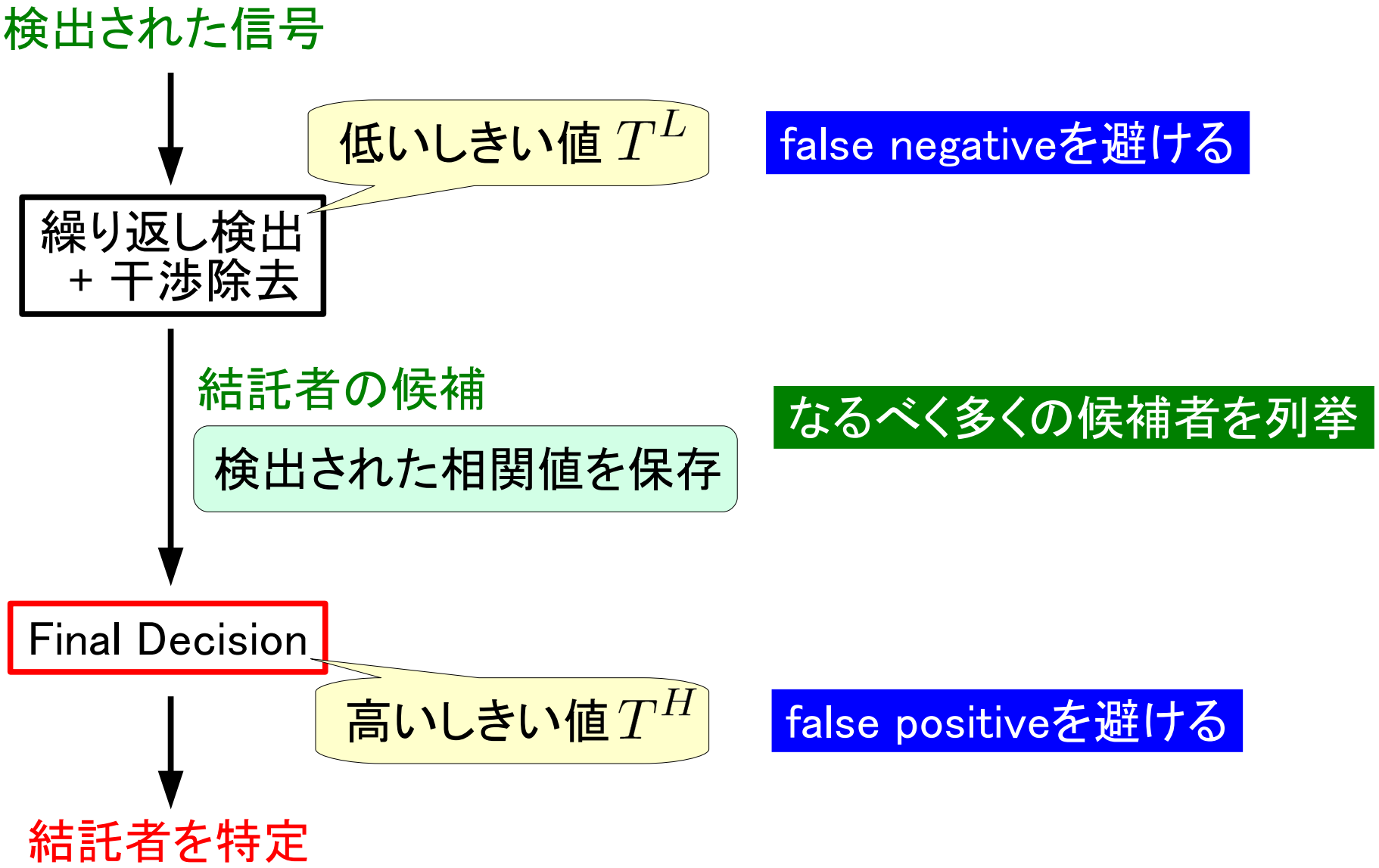
$Pe$ : false-positive probability
$\sigma^2$ : variance



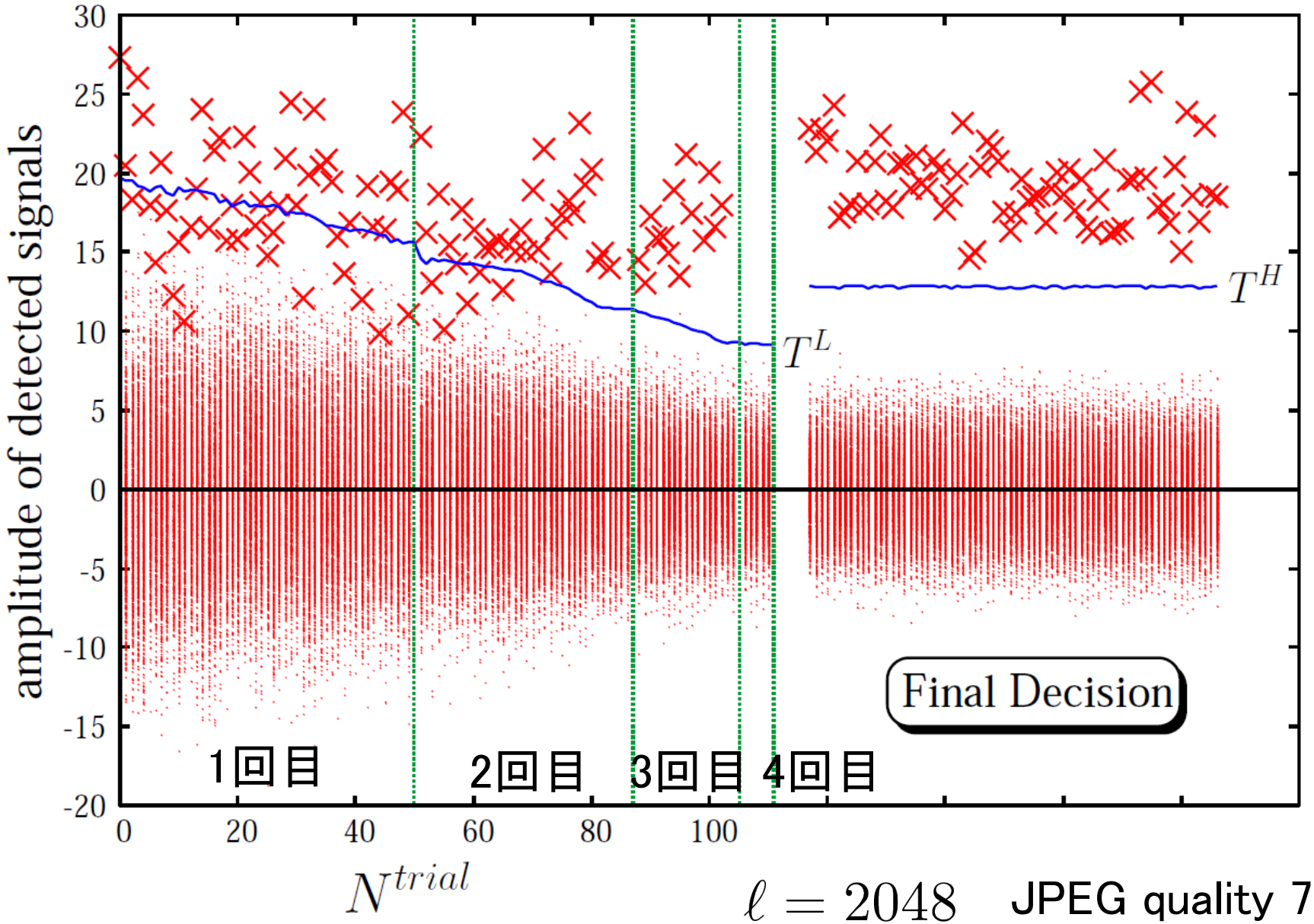

干渉成分が減少して分散値σが小さくなる

誤検出率は変化せず，しきい値$T$が低くなり，検出率が向上

# 二種類のしきい値

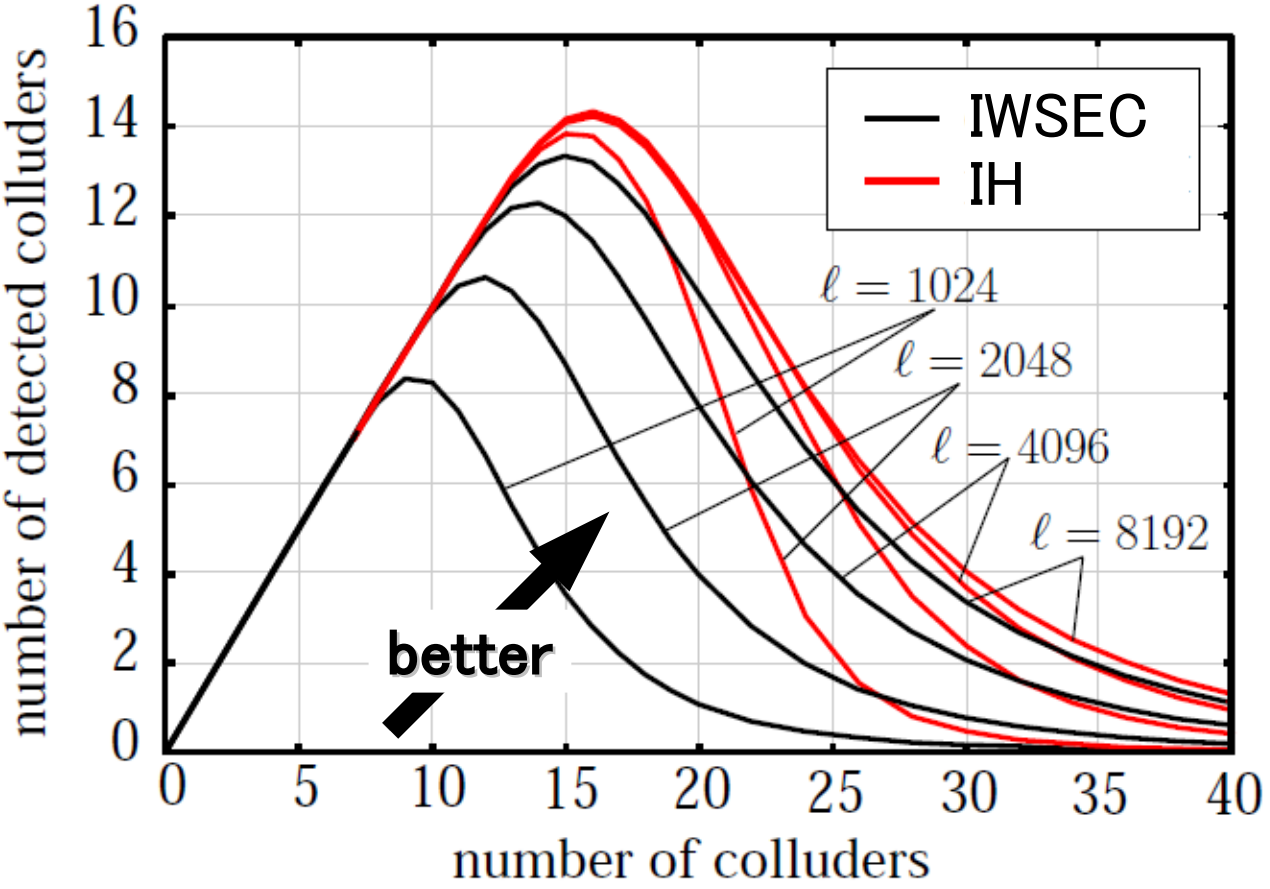

検出された信号
低いしきい値 $T^L$
false negativeを避ける
繰り返し検出
＋ 干渉除去
結託者の候補
検出された相関値を保存
なるべく多くの候補者を列挙
Final Decision
高いしきい値 $T^H$
false positiveを避ける
結託者を特定

# しきい値の推移




$\ell = 2048$ JPEG quality 75%

# 検出された結託者数




画像: lena (512×512画素)

ユーザ数: $2^{20}$ $(\approx 10^6)$

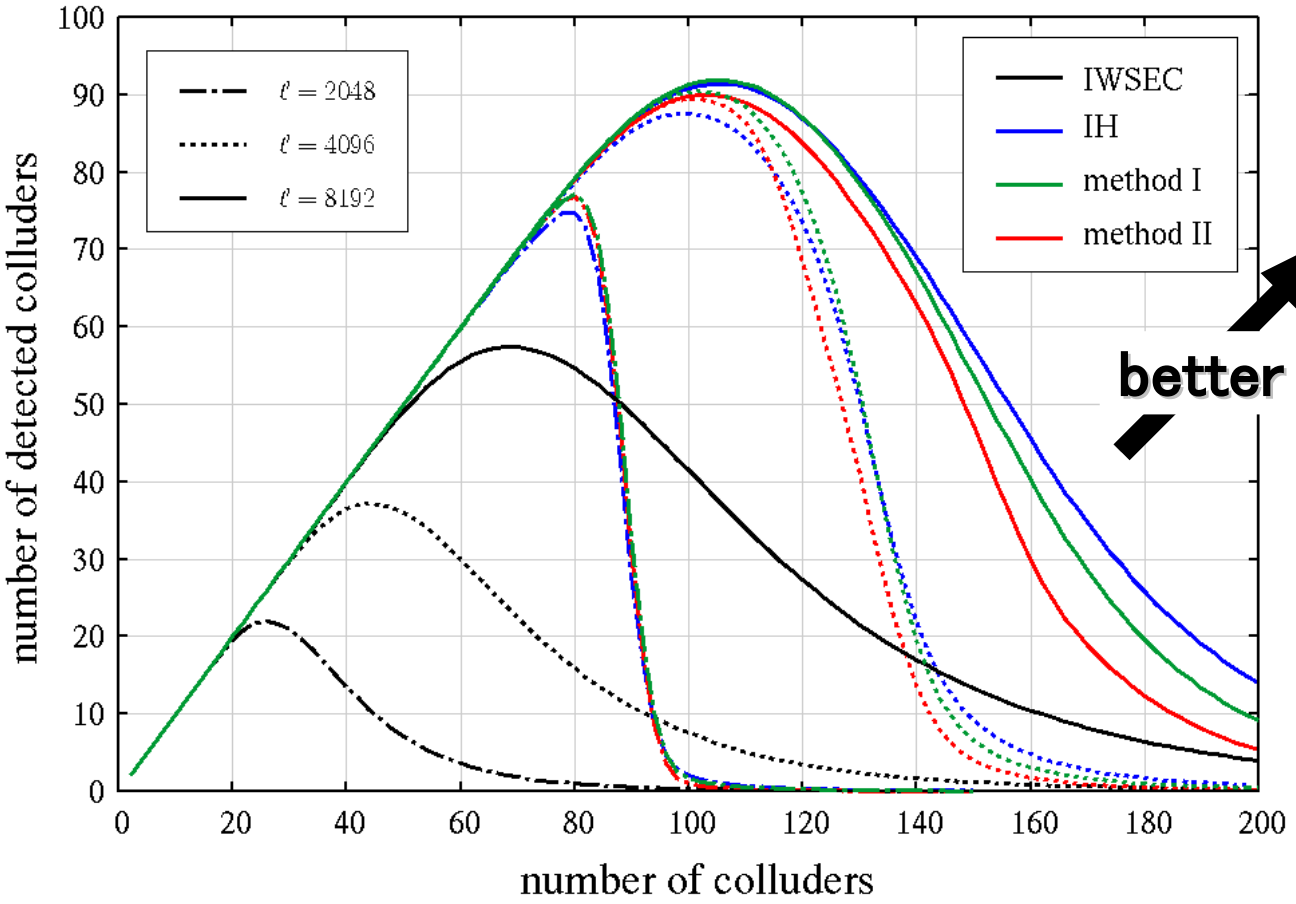
画質: 45dB

攻撃: 平均化攻撃
+ JPEG圧縮35%

雑音付加

**繰り返し検出と干渉除去により検出性能が向上**

# 雑音が少ない場合



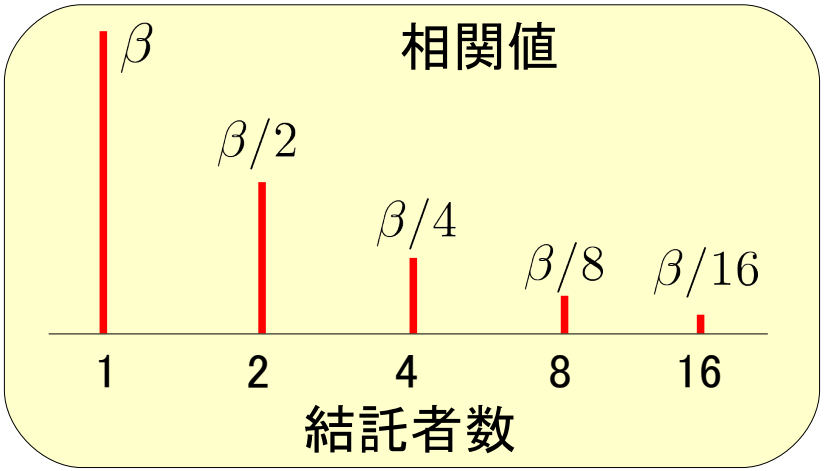

雑音: JPEG圧縮75%

結託者が100人を超えても，多くの結託者を特定できる

# 考察

## 検出できた結託者数が異常に多いように思われる

平均化攻撃を受けると，
相関値は結託者の人数$c$に
反比例して減衰する




**直感的に**

結託者が100人の場合，相関値が減衰しすぎて
検出は困難ではないか？

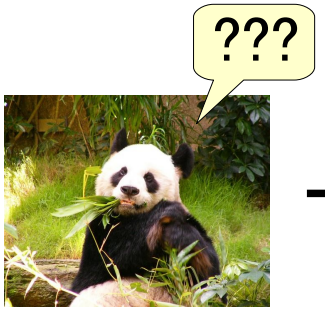
# 目次

- スペクトル拡散技術を用いた電子透かし
- CDMA技術に基づく電子指紋方式
- 干渉成分の抑制と除去
- **量子化誤差による影響**
- 今後の展望

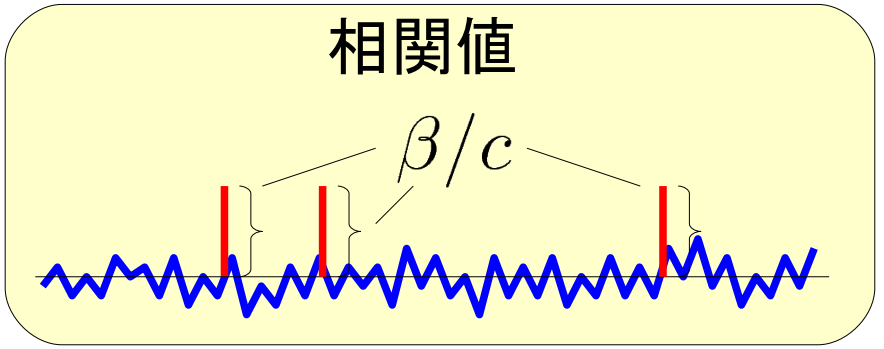
# Attenuation Factor

M. Kuribayashi, H. Kato, and M. Morii
“A Study of Rounding Error on CDMA-Based Fingerprinting Scheme,”
Proc. IIHMSP2009, pp.1286-1289, 2009.

**減衰量 $c'$** 理論的に相関値の減衰は $1/c$ となる $(c' = c)$




検出操作

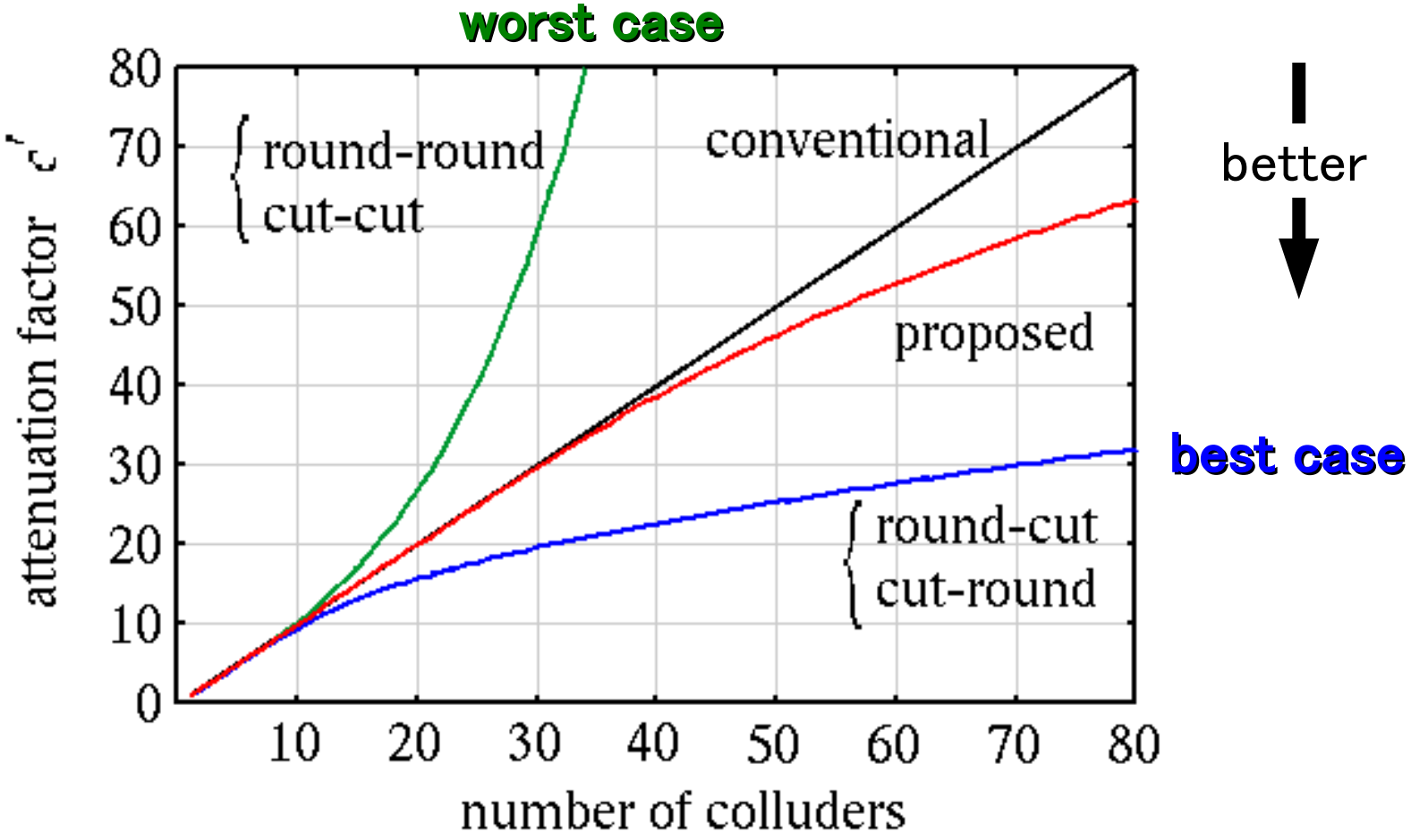



攻撃は平均化攻撃を想定

**研究結果**

**量子化誤差の丸め方によって信号の減衰量が著しく変動**

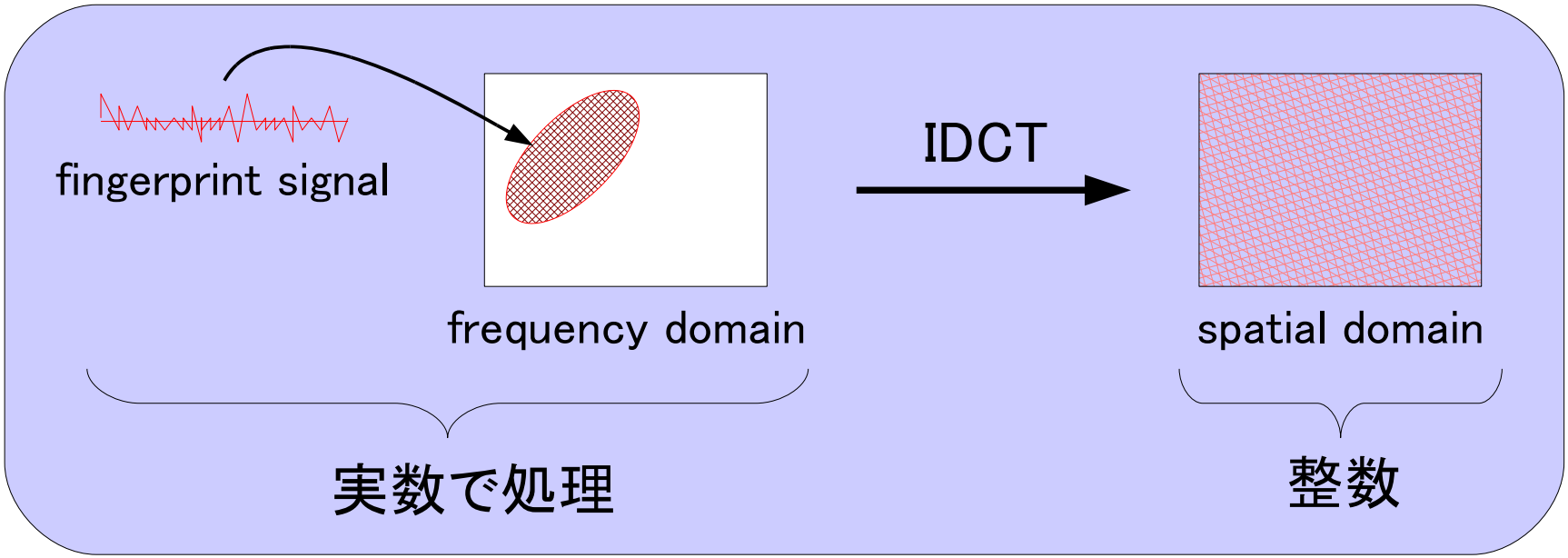
# 比較




減衰量は量子化の操作法によって激しく変動

# 埋め込み時の量子化処理

- 拡散された電子指紋信号は輝度領域において整数[0,255]に丸められる



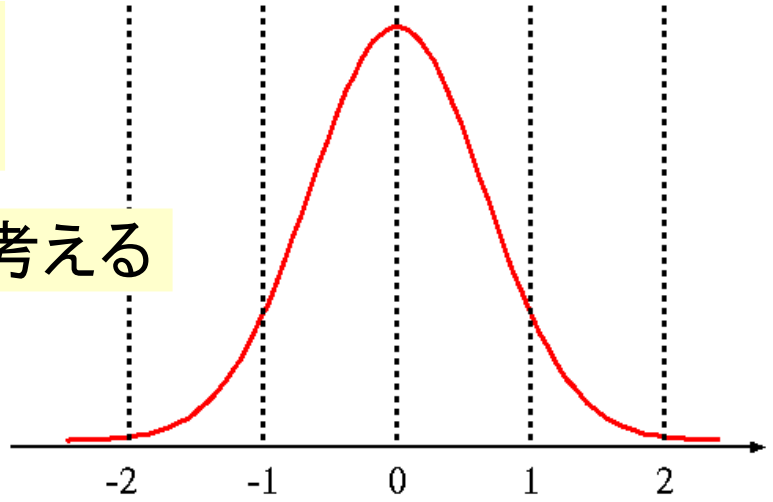

**仮定**

輝度領域に拡散された電子指紋信号は平均0のガウス分布

# 電子指紋信号の分布

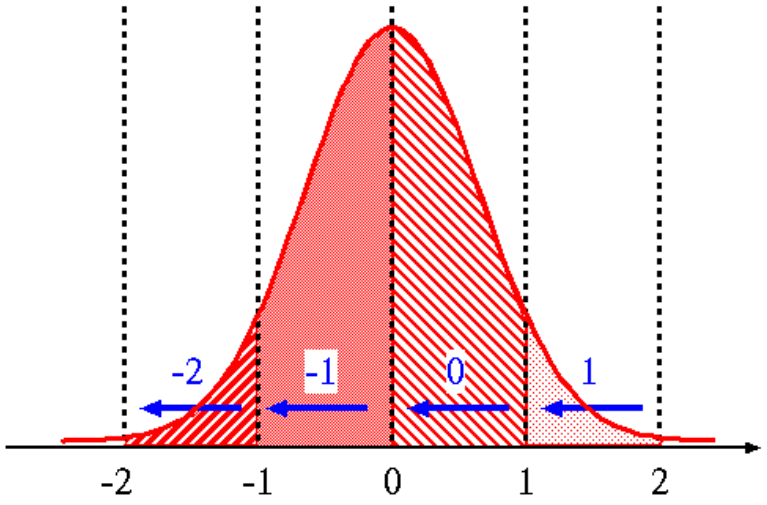
各画素で，電子指紋信号はガウス分布する

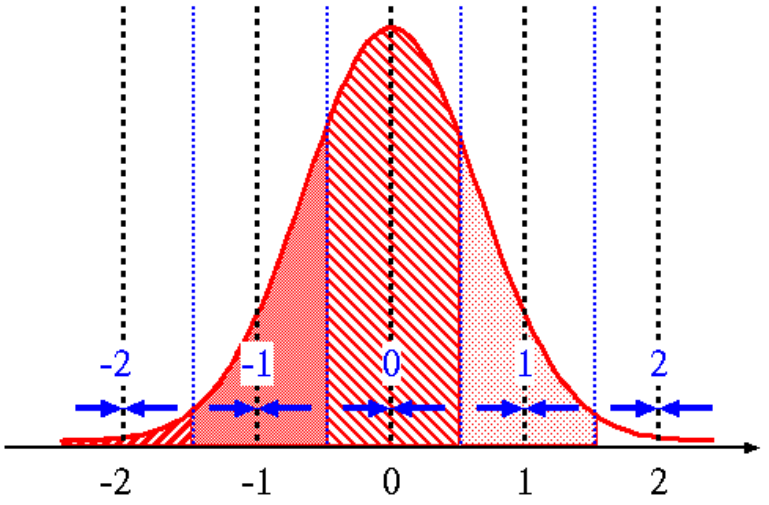
この分布を確率密度関数と考える




切り捨て

四捨五入

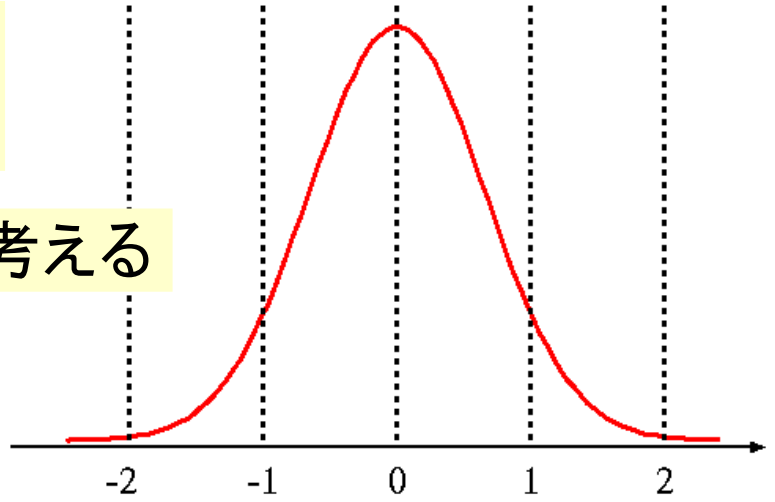


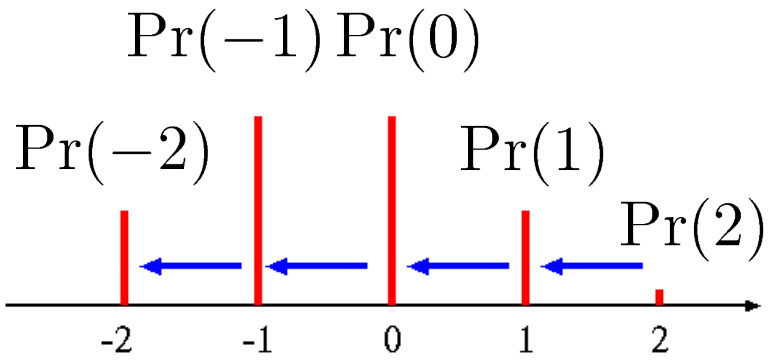
# 電子指紋信号の分布

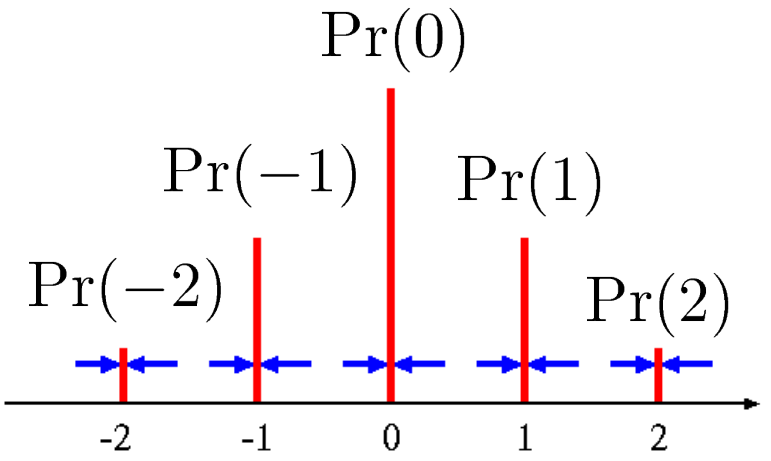
各画素で，電子指紋信号はガウス分布する

この分布を確率密度関数と考える



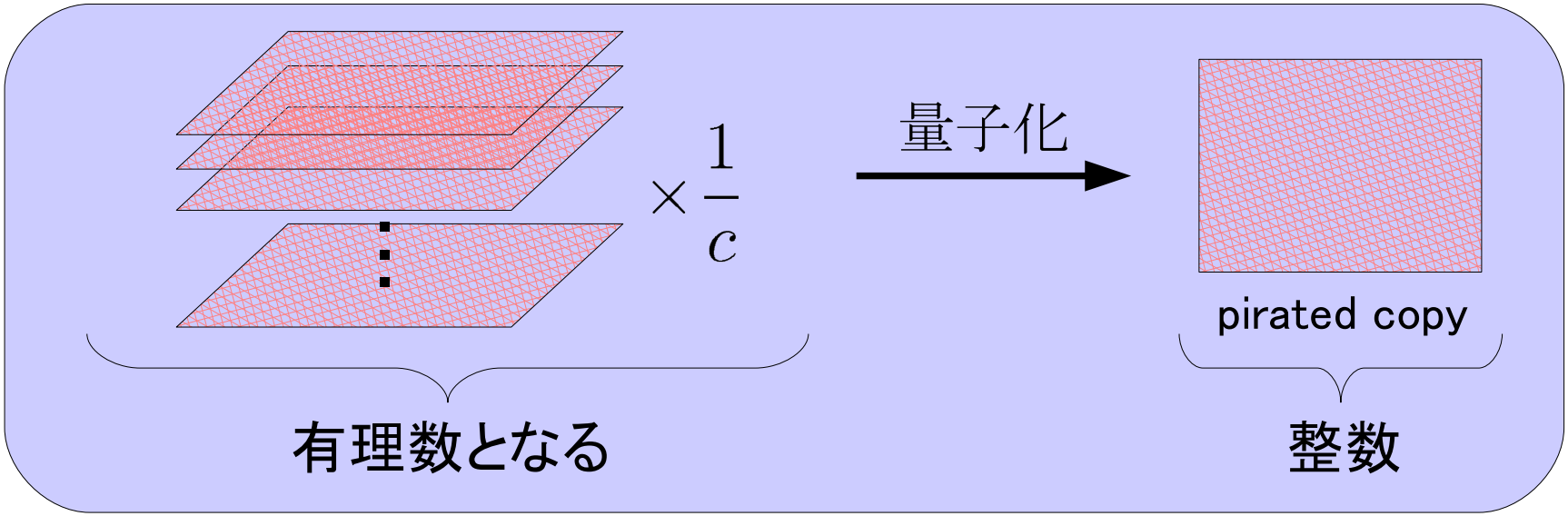

量子化処理後，丸め込まれる整数値の確率は処理法によって大きく異なる



# 不正コピー作成時の量子化処理

- $c$ 個の画像を平均化する場合



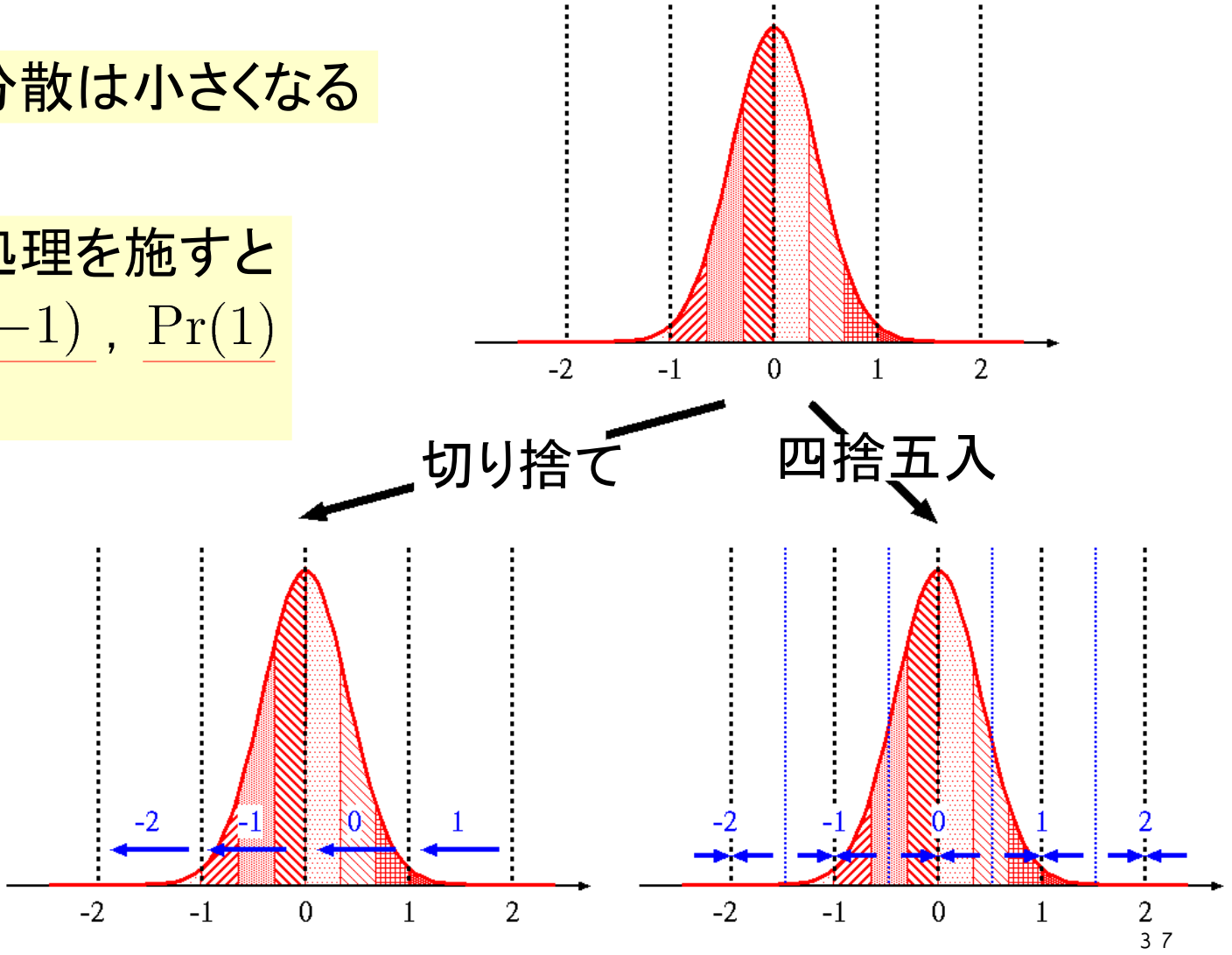

この時の量子化の手法によって電子指紋信号の減衰が大きく異なる

# 結託者が3人のとき

- **埋め込み時に四捨五入した場合**

確率密度関数の分散は小さくなる

結託者が量子化処理を施すと
確率の多くは $\Pr(-1)$ , $\Pr(1)$
$\Pr(0)$ に集中する

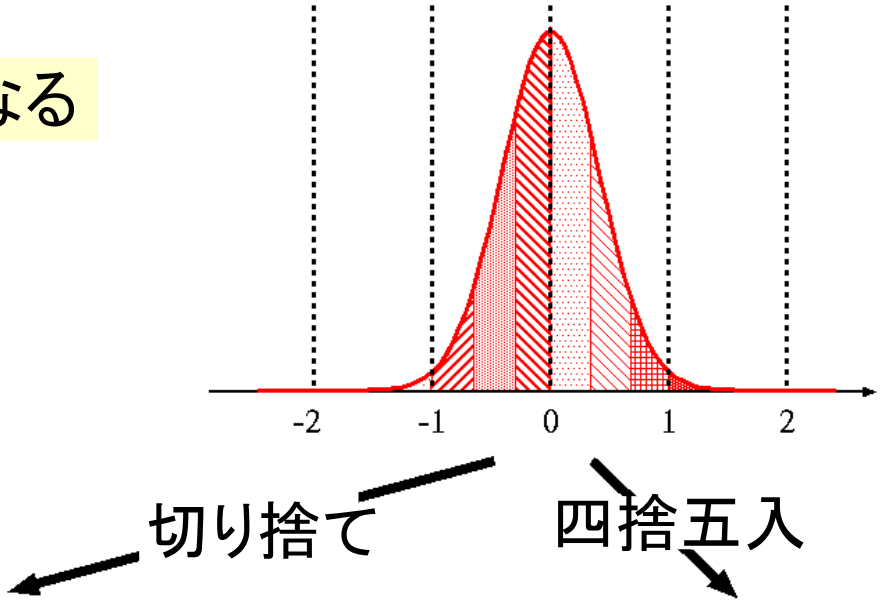


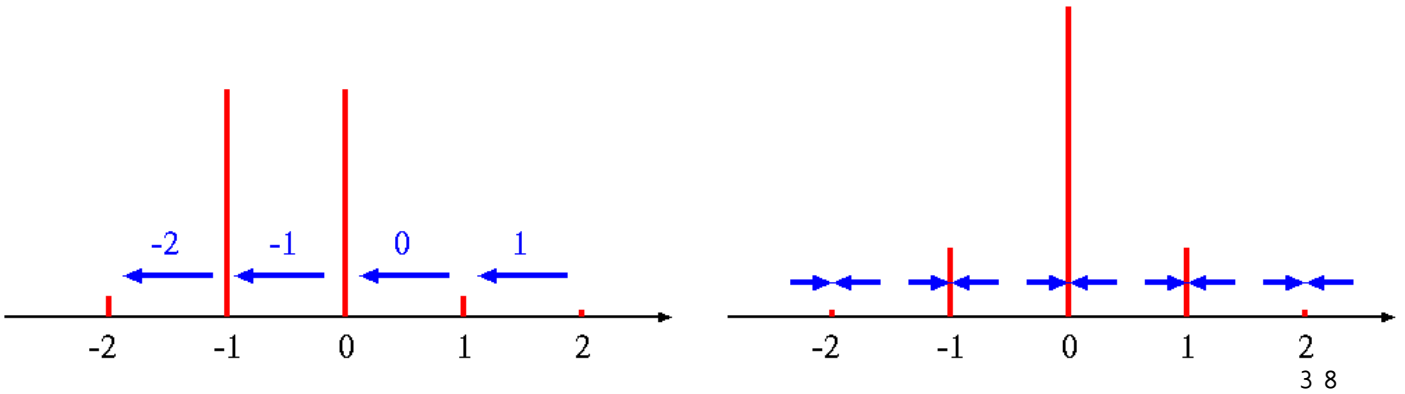
# 結託者が3人のとき

- **埋め込み時に四捨五入した場合**

確率密度関数の分散は小さくなる

結託者が量子化処理を施すと
確率の多くは $\Pr(-1)$ , $\Pr(1)$
$\Pr(0)$ に集中する

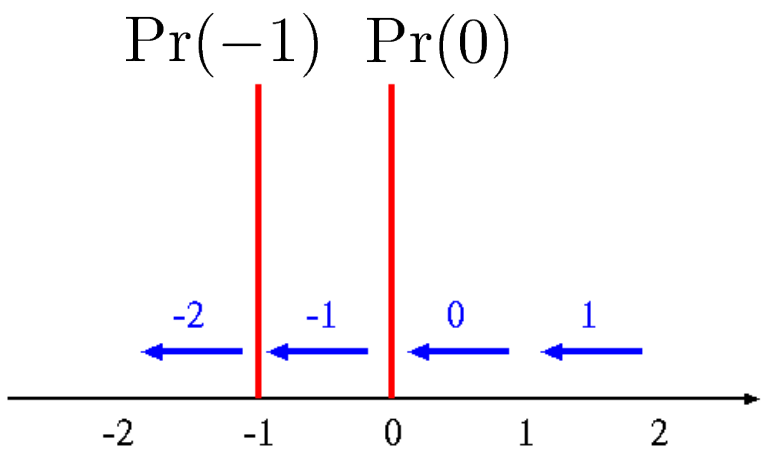


# 結託者数が増加した場合

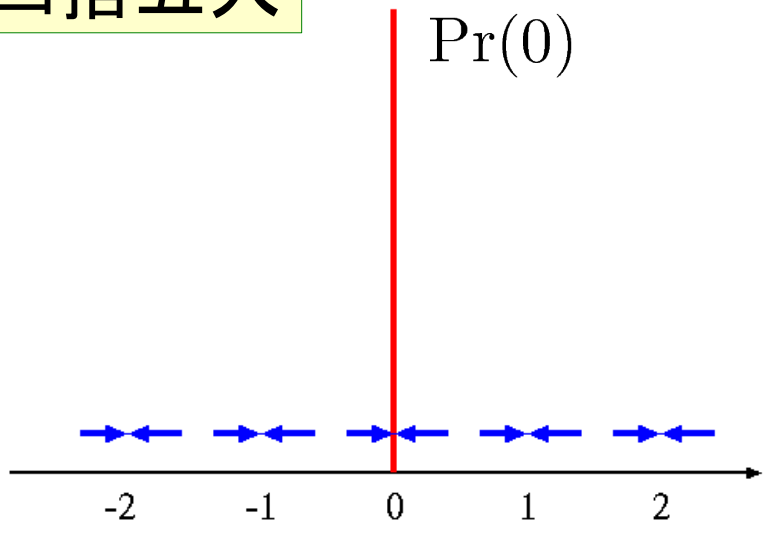
- **埋め込み時に四捨五入した場合**

**切り捨て**




電子指紋信号が消されずに残り続ける

**四捨五入**




電子指紋信号が急速に減衰して完全に消失する

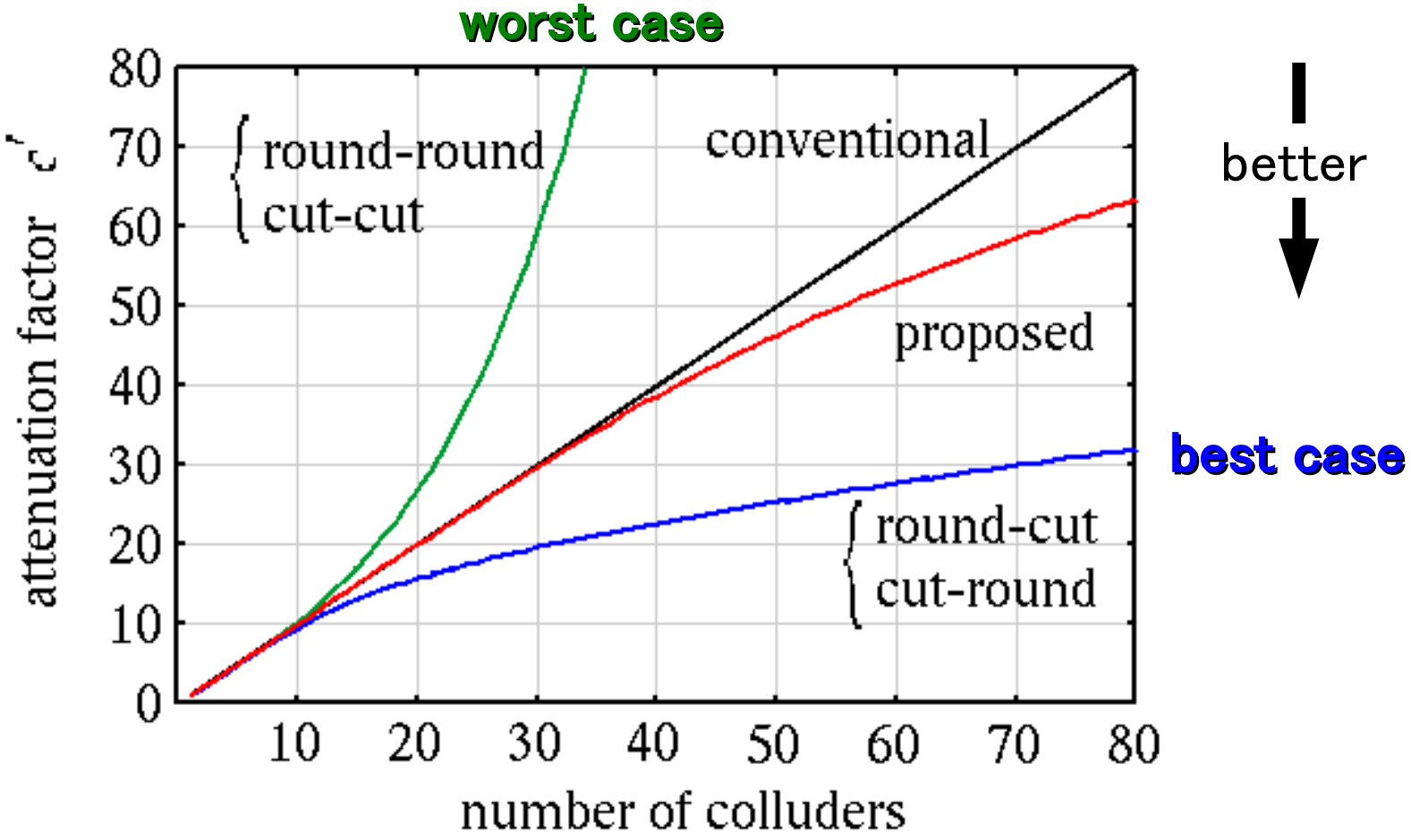
# 分類

| 埋め込み時 | 結託攻撃時 | 電子指紋信号 | 減衰量 |
|---|---|---|---|
| 四捨五入 | 切り捨て | **残り続ける** | **best case** |
| 四捨五入 | 四捨五入 | 消失 | **worst case** |
| 切り捨て | 切り捨て | 消失 | **worst case** |
| 切り捨て | 四捨五入 | **残り続ける** | **best case** |

**研究結果**

**量子化誤差の丸め方によって信号の減衰量が著しく変動**

# 比較




減衰量は量子化の操作法によって激しく変動

# 目次

- スペクトル拡散技術を用いた電子透かし
- CDMA技術に基づく電子指紋方式
- 干渉成分の抑制と除去
- 量子化誤差による影響
- **今後の展望**

# 今後の展望

- 電子指紋技術において　セキュリティ技術
  - 量子化雑音による影響の更なる解析
  - 暗号システムとの融合
- CDMAシステムに適用　通信技術
  - マルチユーザ検出における干渉除去
  - 量子化雑音による影響をうまく利用して減衰を抑制