視覚暗号の最近の進歩

筑波大学　システム情報系
古賀　弘樹

2020/12/01

視覚暗号(Visual Cryptography)とは

- Naor と Shamir により提案されたディジタル画像に対する秘密分散法の一種

M. Naor and A. Shamir, ``Visual Cryptography,'' Advances in Cryptology – EUROCRYPT 1994, LNCS 950, Springer-Verlag, 1995.

- 視覚復号型秘密分散法 (Visual Secret Sharing Scheme, VSSS)と呼ばれることもある.
- 本講演では 視覚暗号（Visual Cryptography Scheme, VCS)で統一.

視覚暗号(Visual Cryptography)とは

- Naor と Shamir により提案されたディジタル画像に対する秘密分散法の一種

M. Naor and A. Shamir, ``Visual Cryptography,'' Advances in Cryptology – EUROCRYPT 1994, LNCS 950, Springer-Verlag, 1995.

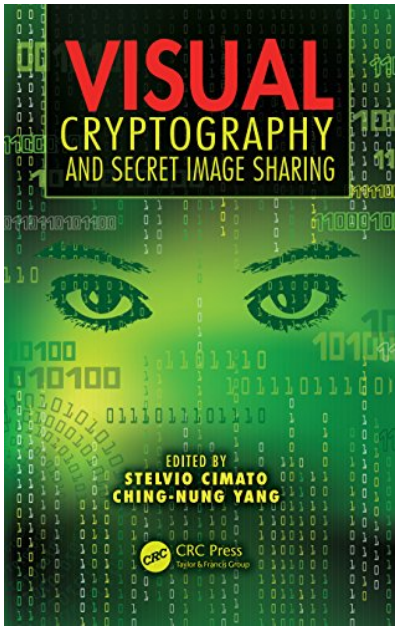
祝：25周年!

- 視覚復号型秘密分散法 (Visual Secret Sharing Scheme, VSSS)と呼ばれることもある.
- 本講演では 視覚暗号（Visual Cryptography Scheme, VCS)で統一.

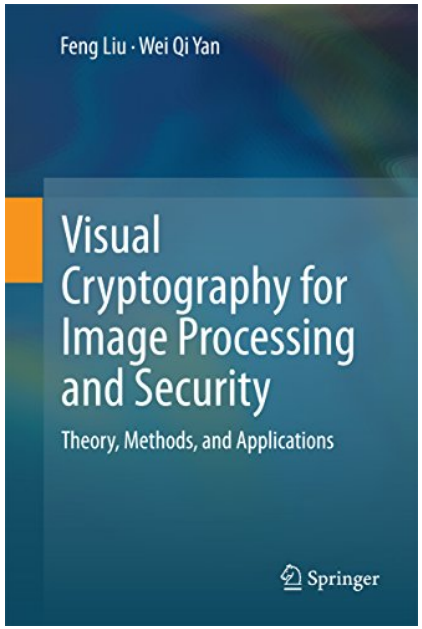
視覚暗号についての本

2004

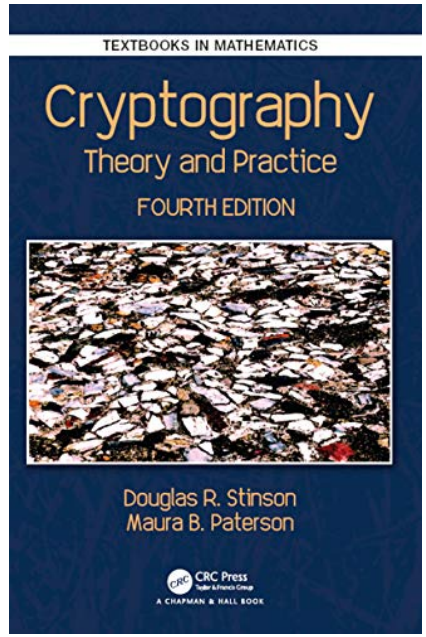
2 編 9 章
視覚的暗号



2011



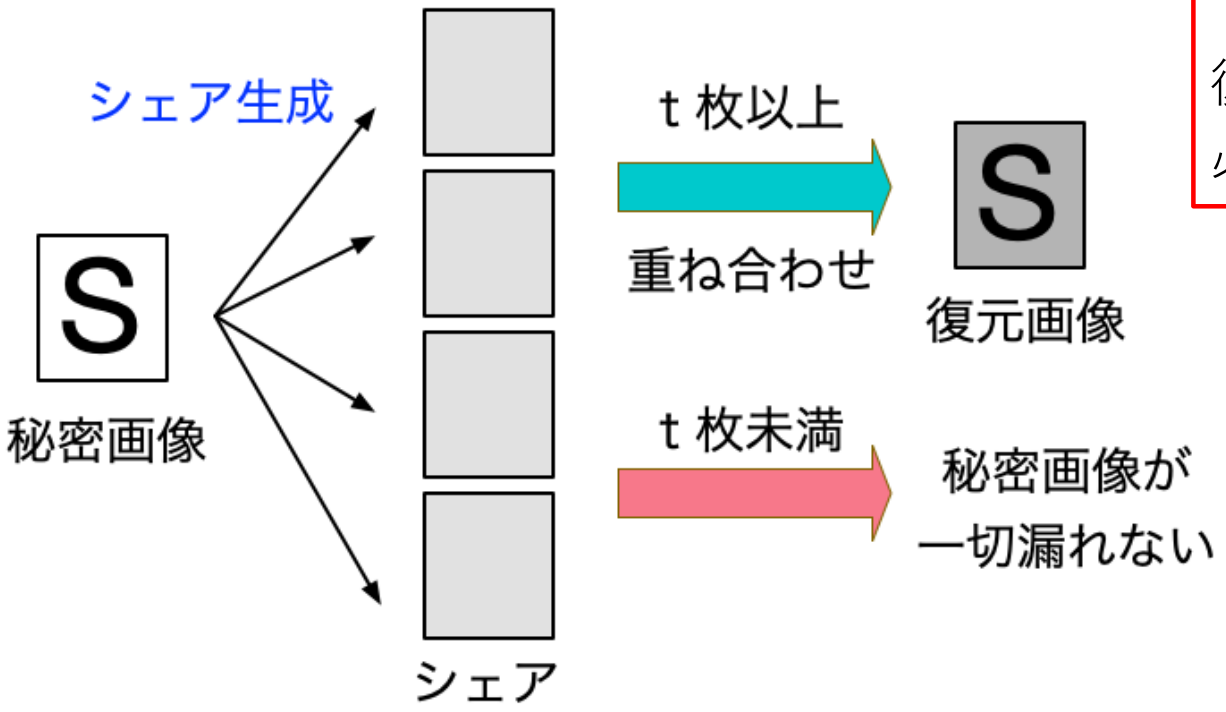
2014



2018

11.5節
Visual Threshold
Scheme

(t, n)しきい値型の視覚暗号



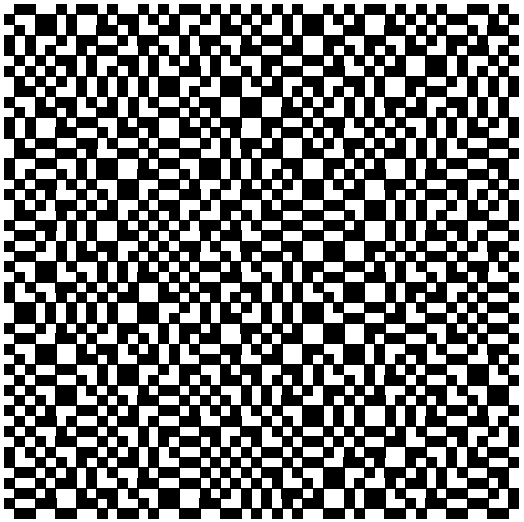
最大の特徴

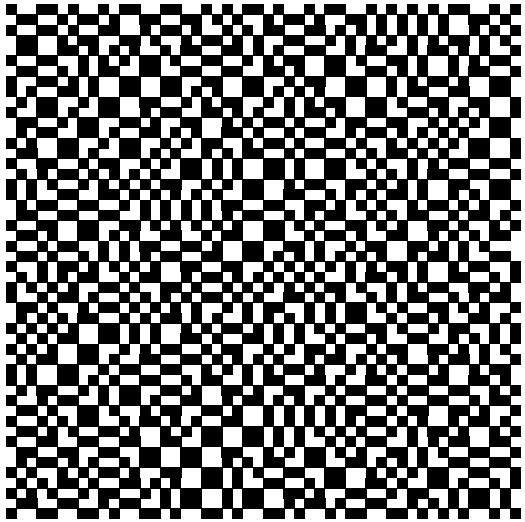
復号時に計算機を必要としない.

(2,2)しきい値型視覚暗号

秘密画像を暗号化した
透明なシート

それぞれのシートからは
元の画像を推測できない



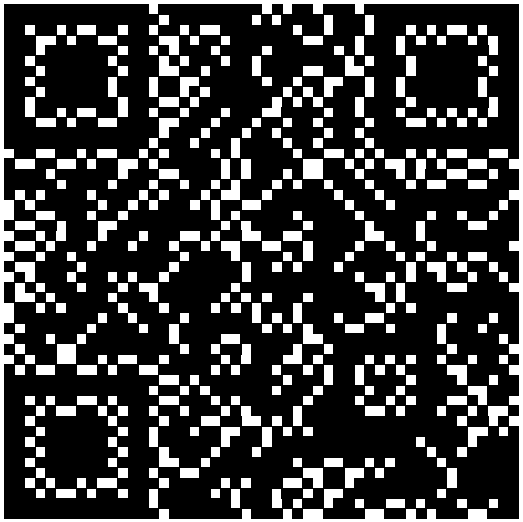


(2,2)しきい値型視覚暗号

秘密画像を暗号化した
透明なシート

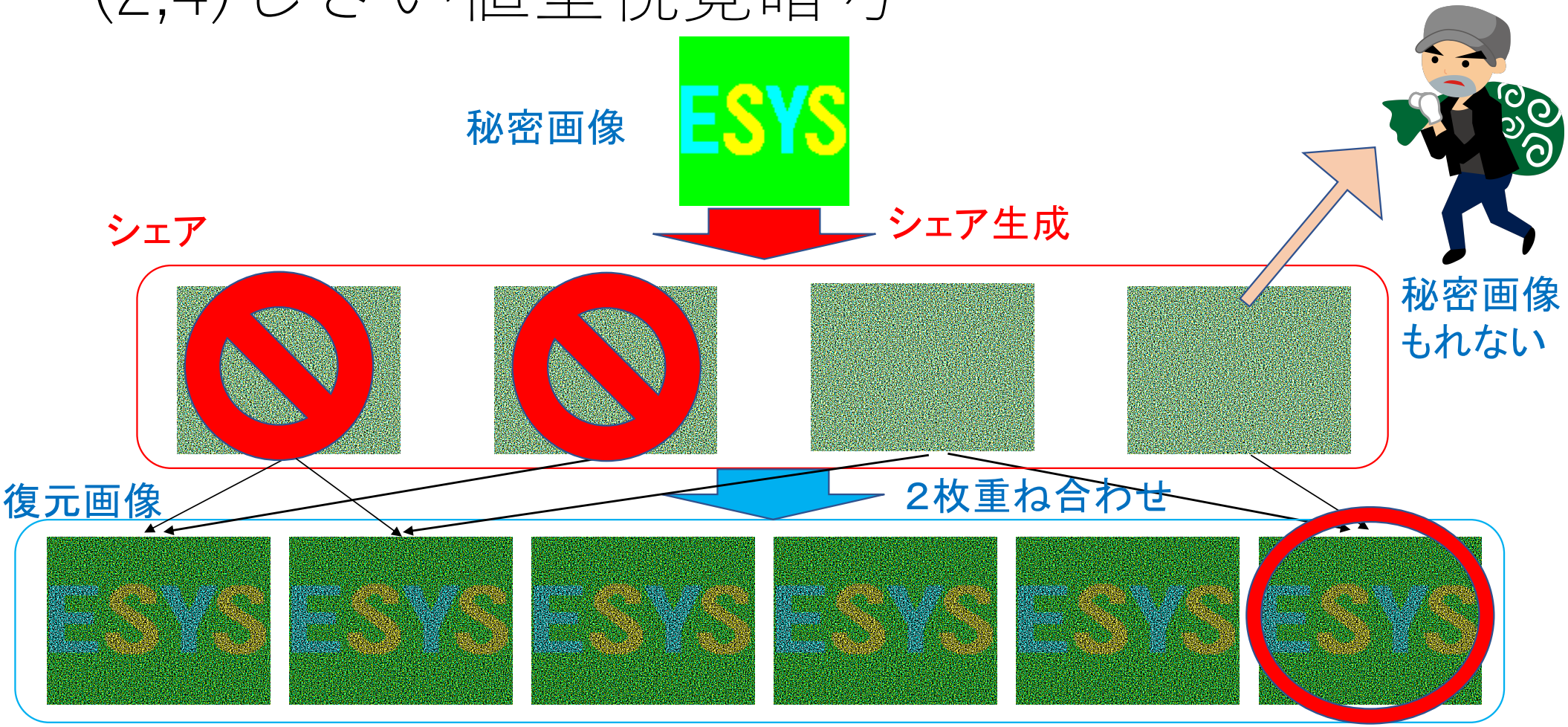
それぞれのシートからは
元の画像を推測できない

安全性が保証
されている！

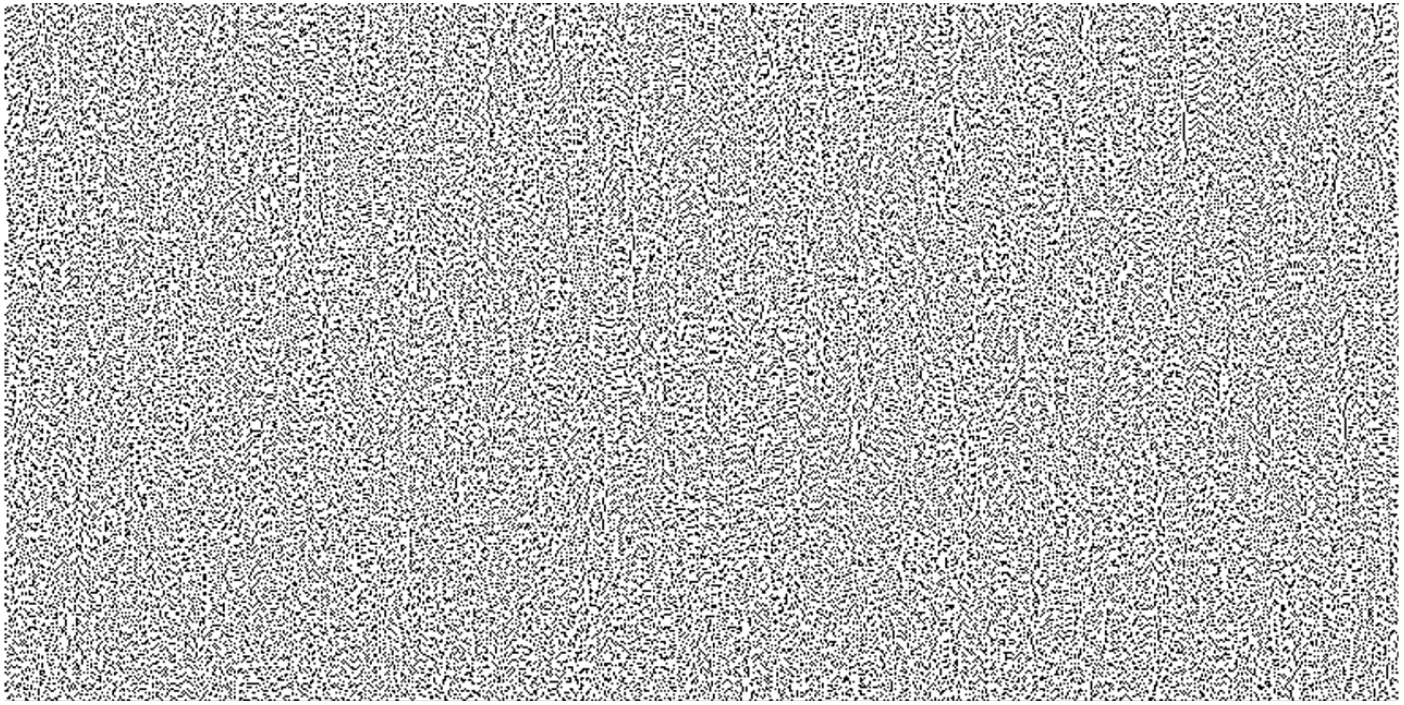


分散したシートを
重ね合わせることで
秘密画像が復元！！

(2,4)しきい値型視覚暗号



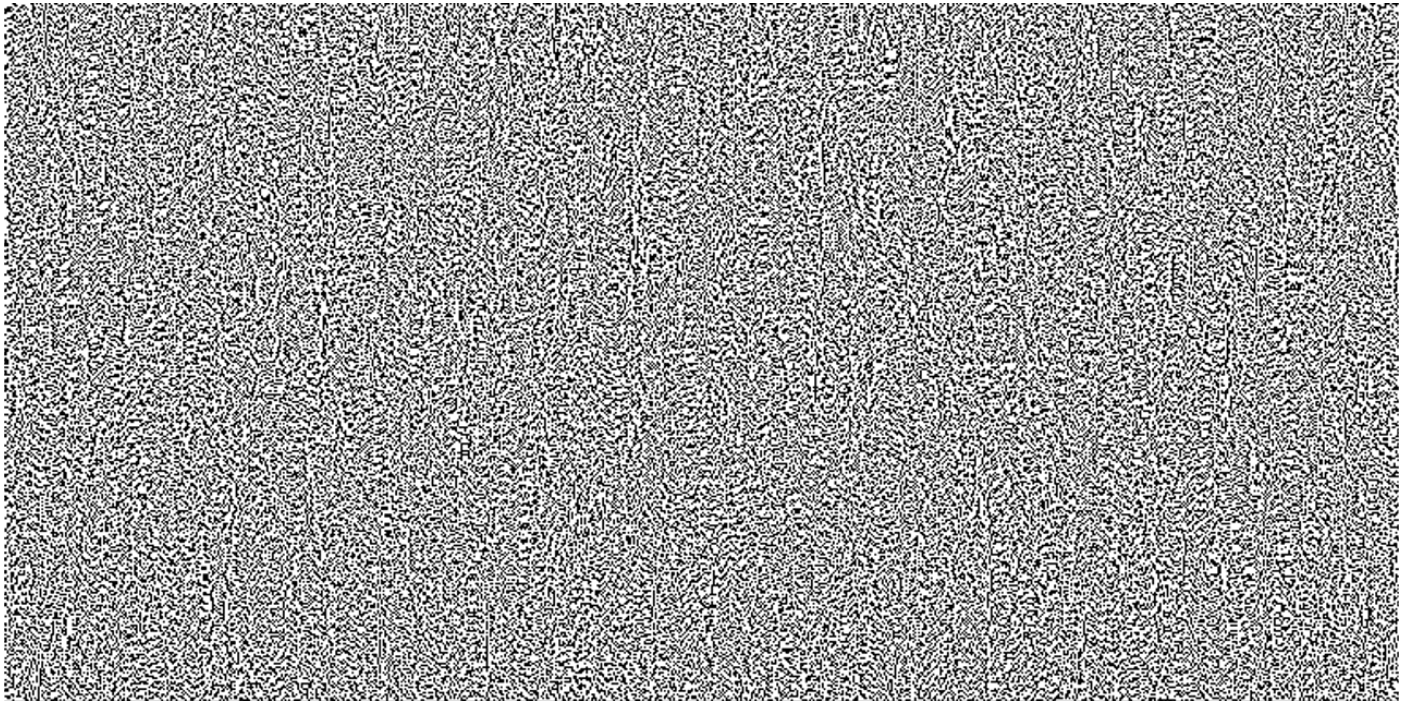
(3,7)プログレッシブ型視覚暗号



シェア単体

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

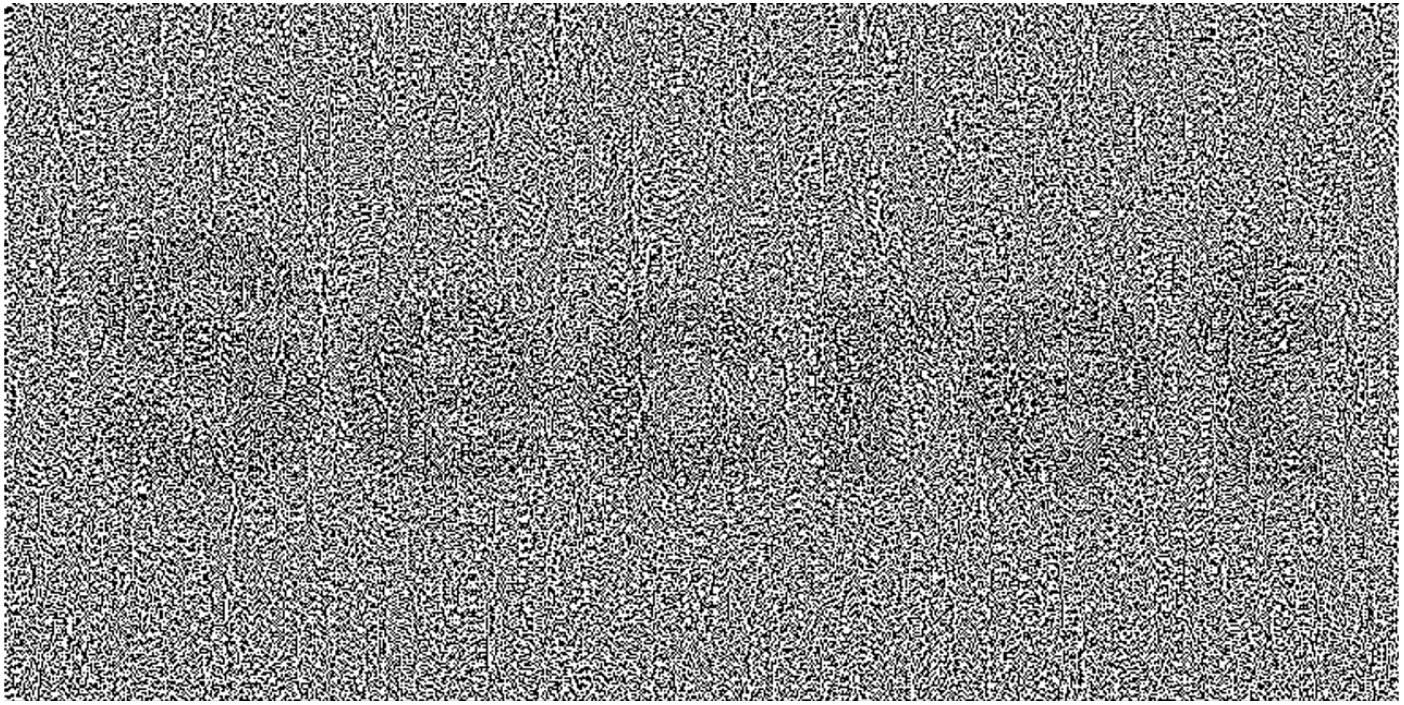
(3,7)プログレッシブ型視覚暗号



２枚重ね

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

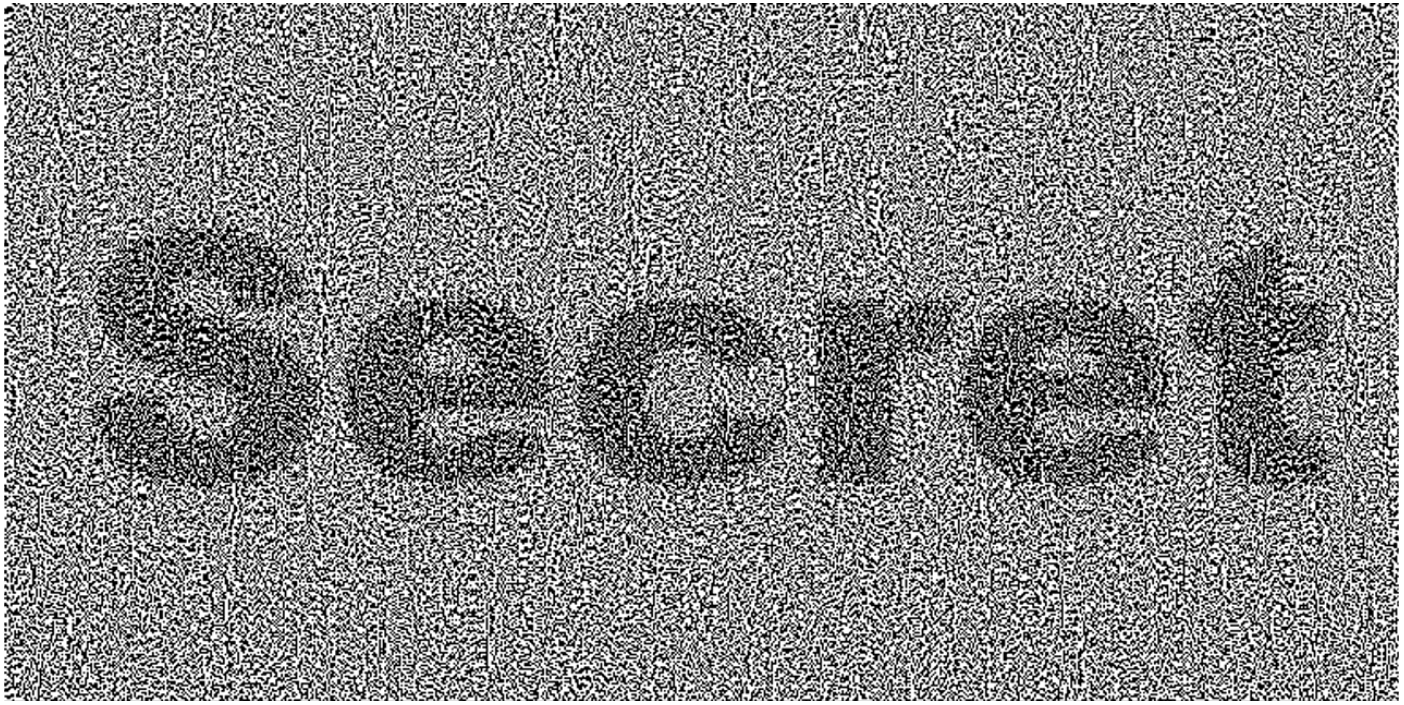
(3,7)プログレッシブ型視覚暗号



3 枚重ね

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

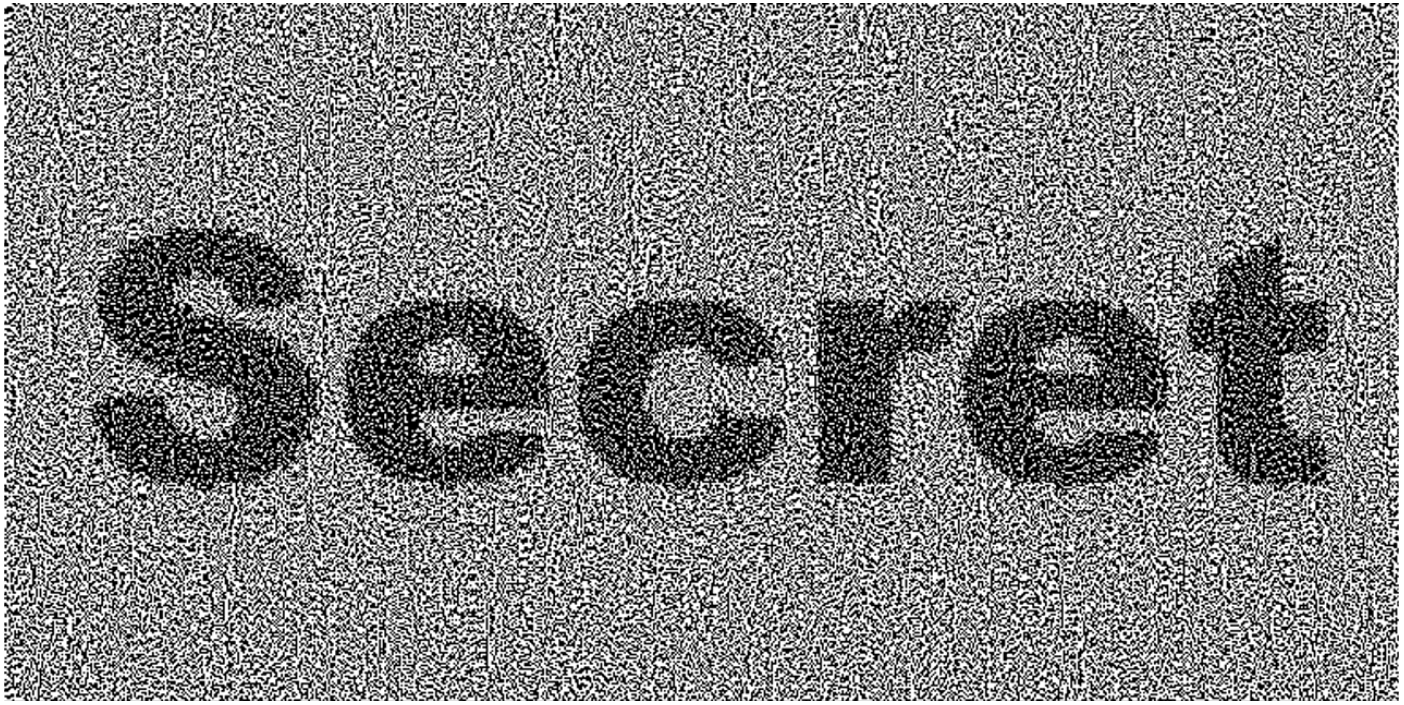
(3,7)プログレッシブ型視覚暗号



4 枚重ね

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

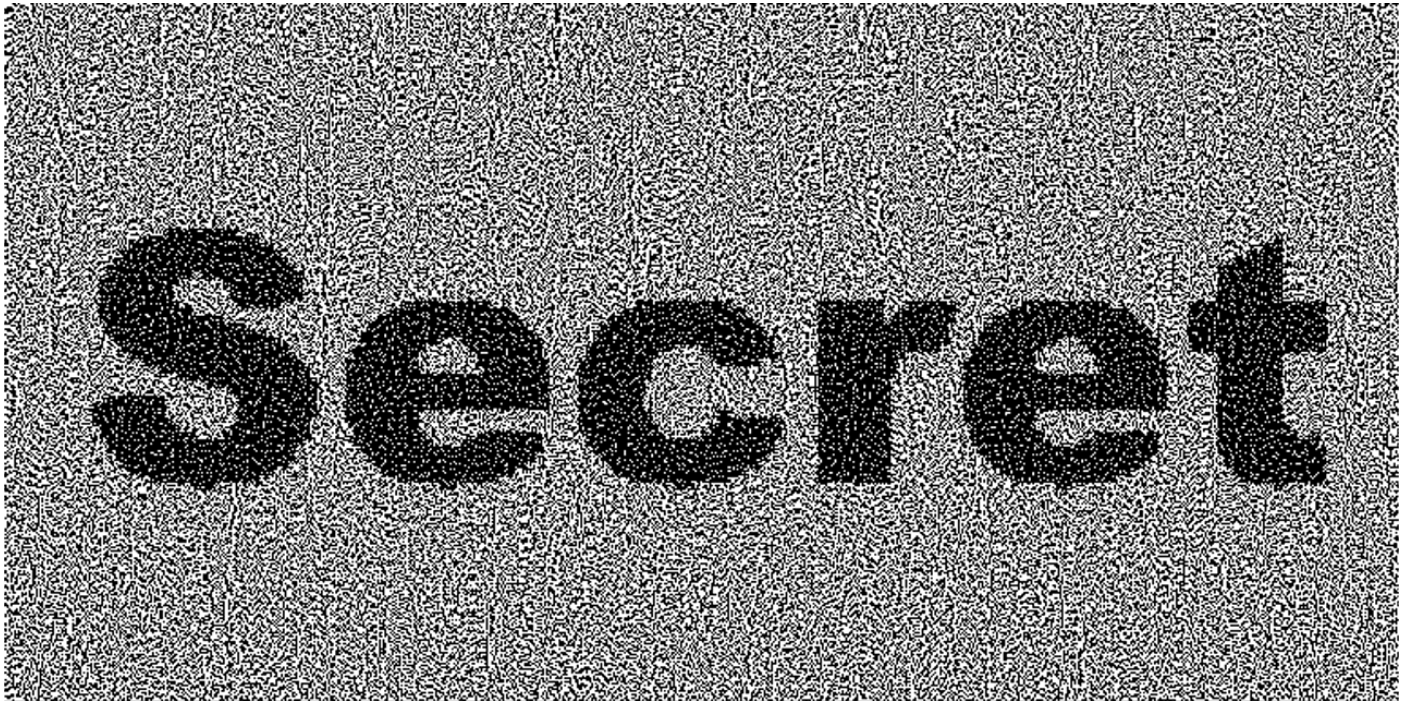
(3,7)プログレッシブ型視覚暗号



5 枚重ね

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

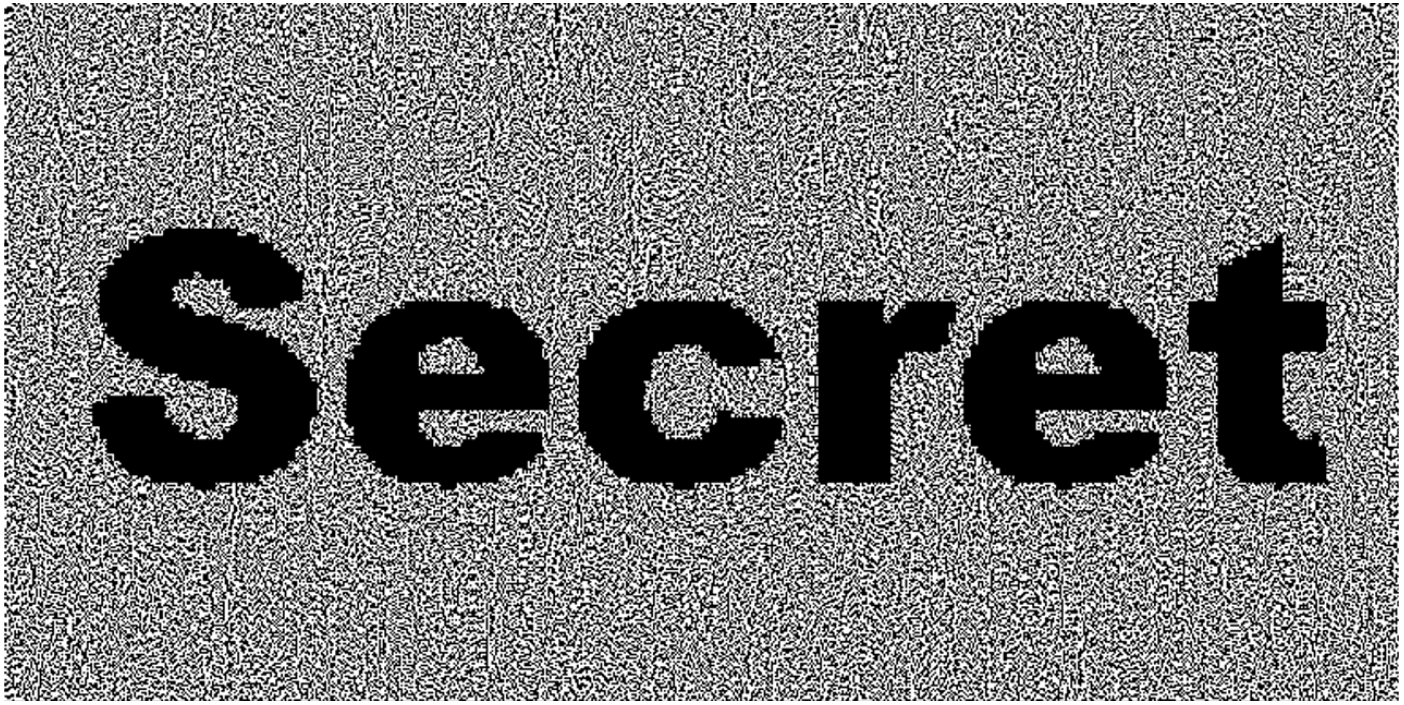
(3,7)プログレッシブ型視覚暗号



6 枚重ね

- 2枚重ねても情報が漏れない.
- 3枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

(3,7)プログレッシブ型視覚暗号



7 枚重ね

- ２枚重ねても情報が漏れない.
- ３枚重ねて初めて秘密画像が復元.
- 重ねる枚数が増えるごとに，秘密画像が鮮明に復元.

概要

1. 視覚暗号の定義
2. 過去の研究の紹介（少しだけ）
3. 画素拡大および相対差の最適化
4. BIBDを用いた(3,n)しきい値型の視覚暗号の構成
5. 最適化によるEVCSの構成と新しい安全性
6. まとめ

参加者集合とアクセス構造

- 秘密画像 (SI)は白黒２値の画像であることを仮定.

- 参加者集合　$\mathcal{P} = \{1, 2, \ldots, n\}$　　（べき集合を$2^{\mathcal{P}}$）
- 有資格集合 (qualified set)　$\Gamma_Q \subset 2^{\mathcal{P}}$
  - シェアの重ね合わせによって SI を復元できる参加者集合の集合
  - 単調増加性 $(A \in \Gamma_Q, A \subset B \Rightarrow B \in \Gamma_Q)$ を仮定.
  - 極小有資格集合を$\Gamma_Q^* = \{ A \in \Gamma_Q : B \notin \Gamma_Q , \forall B \subsetneq A \}$

- 禁止集合 (forbidden set)　　$\Gamma_F \subset 2^{\mathcal{P}}$
  - シェアから SI に関する一切の情報を得られない集合.
  - 単調減少性 $(A \in \Gamma_F, B \subset A \Rightarrow B \in \Gamma_F)$ を仮定.
  - 極大禁止集合を$\Gamma_F^* = \{ A \in \Gamma_F : B \notin \Gamma_Q , \forall A \subsetneq B \}$

$\Gamma_Q \cup \Gamma_F = 2^{\mathcal{P}}$
$\Gamma_Q \cap \Gamma_F = \emptyset$
を仮定.

$\Gamma = (\Gamma_Q, \Gamma_F)$ を
アクセス構造
という.

(t, n)しきい値型のアクセス構造

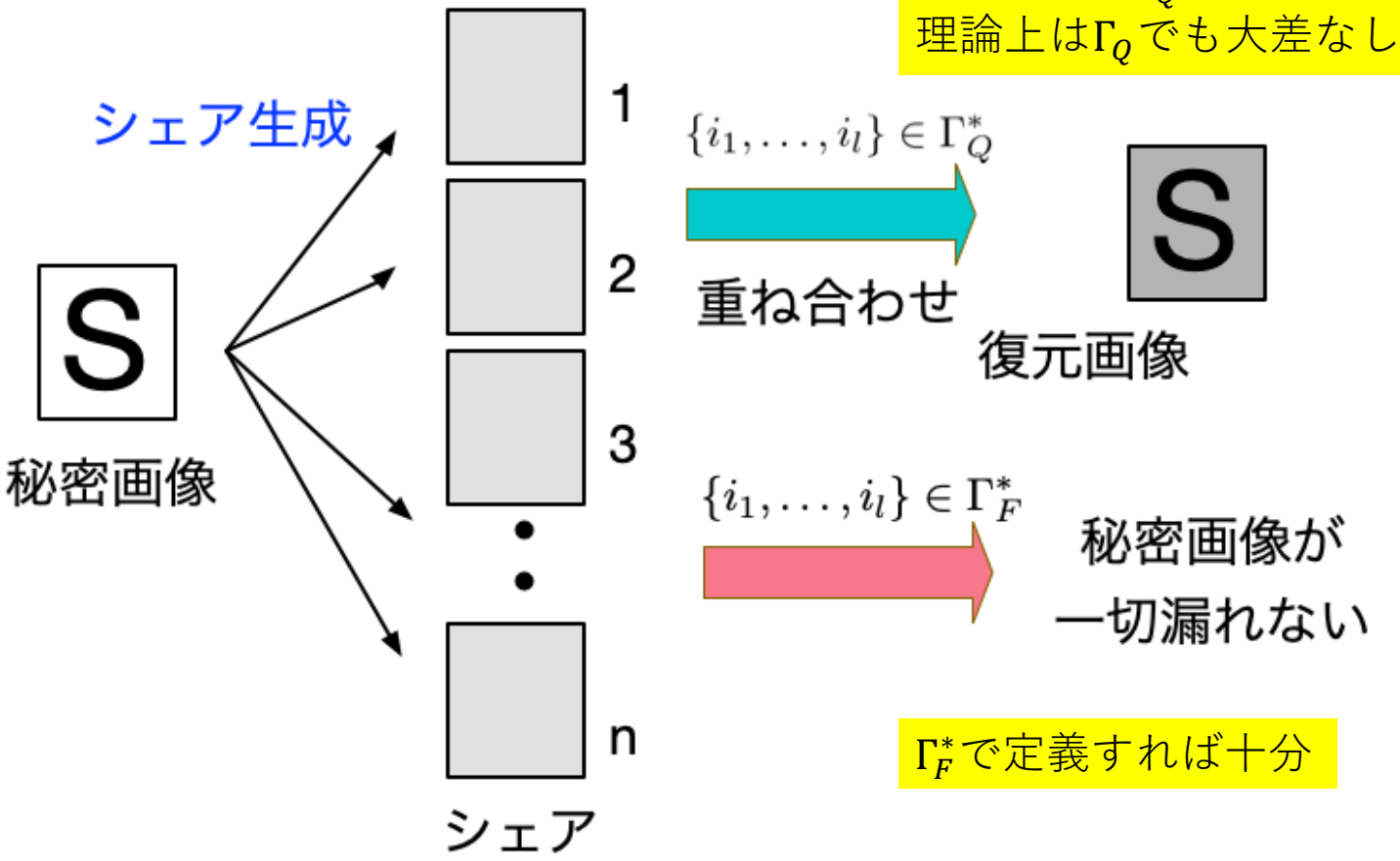
- t をしきい値とする．$(2 \leq t \leq n)$

- 任意のt 枚のシェアから秘密画像 SI を復元できるので,
  $\Gamma_Q = \{ A \in 2^{\mathcal{P}} : |A| \geq t \}$. このとき$\Gamma_Q^* = \{ A \in 2^{\mathcal{P}} : |A| = t \}$.

- どんな$t-1$ 枚以下のシェアからもSI の情報が一切もれないので
  $\Gamma_F = \{ A \in 2^{\mathcal{P}} : |A| \leq t-1 \}$. $\Gamma_F^* = \{ A \in 2^{\mathcal{P}} : |A| = t-1 \}$.

- (t, n)しきい値型のアクセス構造に対する視覚暗号を(t, n)-VCS

本発表の視覚暗号


本発表ではΓ_Q^*に限定するが
理論上はΓ_Qでも大差なし
シェア生成
S
秘密画像
1
2
3
n
シェア
$\{i_1, \ldots, i_l\} \in \Gamma_Q^*$
重ね合わせ
S
復元画像
$\{i_1, \ldots, i_l\} \in \Gamma_F^*$
秘密画像が
一切漏れない
Γ_F^*で定義すれば十分

基本行列の定義

定義 1 (Naor-Shamir (1994), Ateniese et al. (1996))
$\Gamma = (\Gamma_Q, \Gamma_F)$: 参加者集合$\mathcal{P} = \{1, 2, \ldots, n\}$ 上のアクセス構造.

$n \times m$ ブール行列の組(X_0, X_1) は以下の 2 条件を満たすとき，アクセス構造Γを実現する基本行列(basis matrices)という.

1. すべての$S \in \Gamma_Q^*$ に対してある定数$\alpha = \alpha_S > 0$が存在して,

$$HW\big(OR(X_0[S])\big) + \alpha_S m \leq HW\big(OR(X_1[S])\big)$$

SIが復元できる条件

$X_b[S]$ はX_bの行をS に制限して得られる行列,
OR は列ごとのOR操作, HWはハミング重み.

2. すべての$S \in \Gamma_F^*$ に対して, $X_0[S]$と$X_1[S]$ は適当な列の並べ替えで等しくできる.

安全性条件

基本行列の例　～(2,2)-VCSの場合～

$\Gamma_Q^* = \{\{1,2\}\}, \quad \Gamma_F^* = \{\{1\},\{2\}\}$

$$X_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

基本行列の例　～(2,2)-VCSの場合～

$\Gamma_Q^* = \{\{1,2\}\}, \quad \Gamma_F^* = \{\{1\},\{2\}\}$

$$X_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

列ごとのOR ⬇

$$\begin{bmatrix} 0 & 1 \end{bmatrix}$$

ハミング重み1

$$X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

列ごとのOR ⬇

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

ハミング重み2

この場合

$$\alpha_S = \frac{(2-1)}{2} = \frac{1}{2}$$

＜

基本行列の例　～(2,2)-VCSの場合～

$\Gamma_Q^* = \{\{1,2\}\}$,　$\Gamma_F^* = \{\{1\},\{2\}\}$

列の並べ替えで一致

$X_0[\{1\}]$ ⟷ $X_1[\{1\}]$

$$X_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$X_0[\{2\}]$ ⟷ $X_1[\{2\}]$

列の並べ替えで一致

基本行列の例　　～(3,4)-VCSの場合～

$$X_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

基本行列の例　～(3,4)-VCSの場合～

$$X_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

任意の3行のOR

$$[1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0]$$

ハミング重み４

$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

任意の3行のOR

$$[1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1]$$

ハミング重み５＞４

$$\alpha_S = \frac{(5-4)}{6} = \frac{1}{6}$$

基本行列の例　～(3,4)-VCSの場合～

$$X_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

任意の2行

の内訳

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

2列　1列　1列　2列

$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

任意の2行

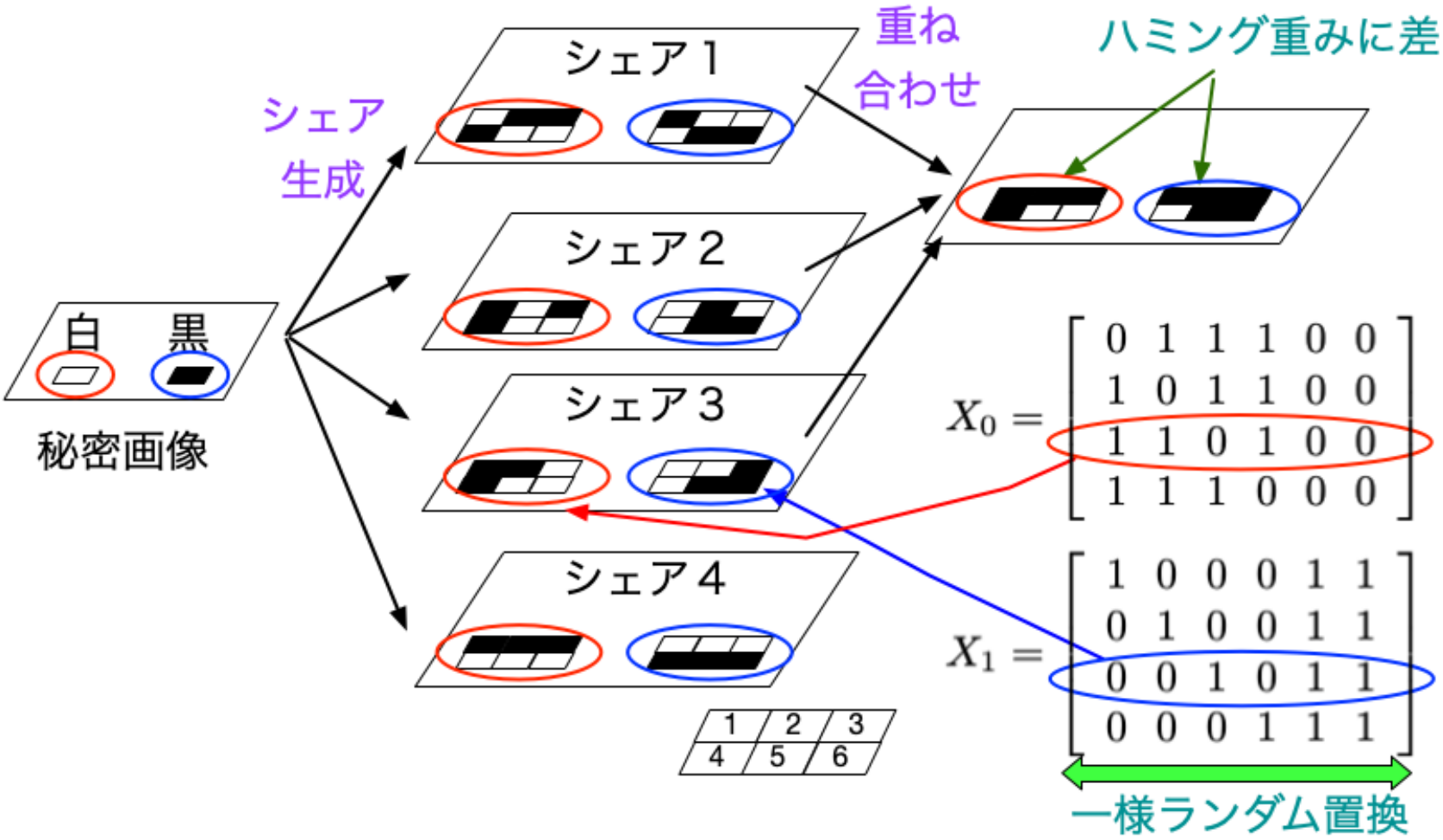
の内訳

頻度が完全に一致

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

2列　1列　1列　2列

基本行列によるシェアの生成　～(3,4)-VCS～



基本行列のパラメータ

- 画素拡大 (pixel expansion) m
  - 基本行列の列数のこと
  - 各シェアの大きさは秘密画像SI の大きさの m 倍になる.
  - 一般には，小さければ小さいほどよい　⇒　最小化問題

- 相対差 (relative difference) α
  - (黒画素のHW – 白画素のHW) / 画素拡大　の$S \in \Gamma_Q^*$ に関する最小値

$$\alpha = \min_{S \in \Gamma_Q^*} \frac{HW\left(OR(X_1[S])\right) - HW\left(OR(X_0[S])\right)}{m}$$

  - 一般に大きいほど，復元されるSIの視認性が上がる．⇒　最大化問題

従来研究

- 1990年代後半～2000年代に様々な議論がなされている.
  - Droste (1996), 加藤 & 今井 (1996)
  - Blundo, De Bonis & De Santis (1999)
  - Eisen & Stinson (2002), K. (2002)
  - Blundo, D'Arco, De Santis & Stinson (2003), など.

行列のクラスに関する仮定のもとでも，(t, n)-VCS $(t \geq 4)$の最適な基本行列を閉じた形で求めるのは難しい.

- 2012年に１つのブレイクスルー
  - Iwamoto (2012) , Shyu & Chen (2012)

行列のクラスに関する仮定なしで，画素拡大を最小にする基本行列が整数計画法で定式化でき，実用的な範囲で解ける.

従来型の基本行列の構成　（その１）

(3,4)-VCS の基本行列（再掲）

$$X_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ の相異なる並べ替え

でできる行列

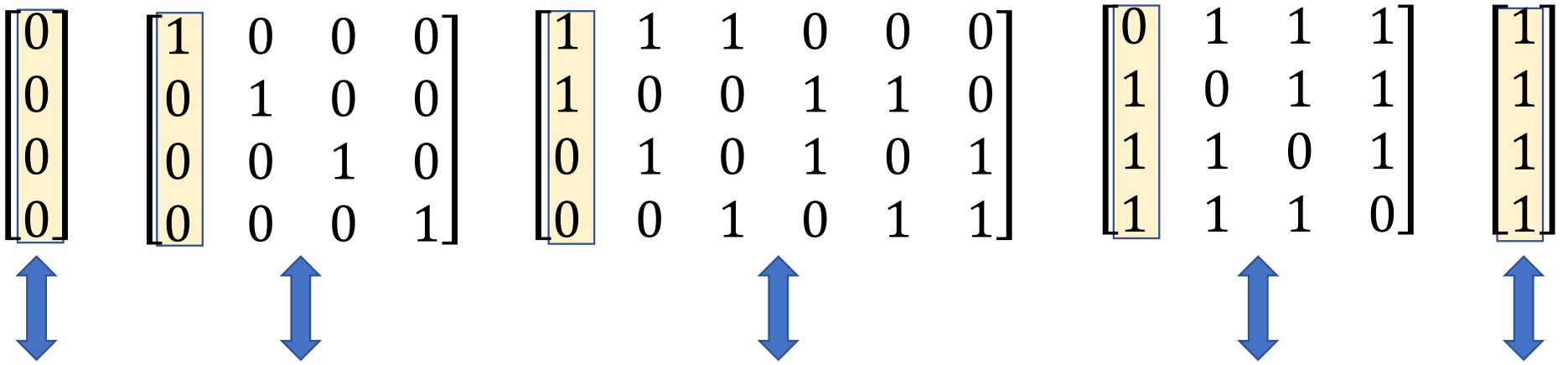
$$X_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ の相異なる並べ替え

でできる行列

従来型の基本行列の構成　（その２）

以下の行列の連接で基本行列を構成.



それぞれ単項式と対応させる（連接の場合は多項式）になる.

従来型の基本行列の構成　（その３）

次の形の多項式を代数的に処理する (K. (2002)).

$$f = \beta_0\, a\,(a-z)^3 + \beta_1\, z\,(a-z)^3 \qquad (\beta_0, \beta_1 \text{は整数}, \beta_0 + \beta_1 > 0)$$

$\beta_0 = \beta_1 = 1$とおいて展開すると

ある２次元の線形空間の基底になっている
(t,n)-VCSなら$a^{n-t-i}z^i(a-z)^t, i = 0,1,\ldots,n-t$

別のβ_0, β_1からは
別の基本行列が
導かれる

$$f = a^4 - 2a^3z + 2az^3 - z^4$$

$$= 2 \cdot 3!\left[\left(2\frac{a^4}{4!} + \frac{az^3}{1!\,3!}\right) - \left(2\frac{z^4}{4!} + \frac{a^3z}{1!\,3!}\right)\right]$$

$$X_0 = \left[\begin{array}{cccc|c|c} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{array}\right] \quad X_1 = \left[\begin{array}{cccc|c|c} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

基本行列の定義（再掲）

定義 1（Naor-Shamir (1994), Ateniese et al. (1996)）
$\Gamma = (\Gamma_Q, \Gamma_F)$：参加者集合$\mathcal{P} = \{1, 2, \ldots, n\}$ 上のアクセス構造.

$n \times m$ ブール行列の組(X_0, X_1) は以下の 2 条件を満たすとき，アクセス構造Γを実現する基本行列(basis matrices)という.

1. すべての$S \in \Gamma_Q^*$ に対してある定数$\alpha = \alpha_S > 0$が存在して,

$$HW\big(OR(X_0[S])\big) + \alpha_S m \leq HW\big(OR(X_1[S])\big)$$

SIが復元できる条件

$X_b[S]$ はX_bの行をS に制限して得られる行列,
OR は列ごとのOR操作，HWはハミング重み.

2. すべての$S \in \Gamma_F^*$ に対して，$X_0[S]$と$X_1[S]$ は適当な列の並べ替えで等しくできる.

安全性条件

同値な安全性条件

補題(Iwamoto (2012), Shyu & Chen (2012))
X, Yを$n \times m$のブール行列とする．次の２つの命題は同値．

1. X, Yは列の適当な並べ替えで等しくできる．
2. $HW(OR(X[S])) = HW\big(OR(Y[S])\big),\ \forall S \subset \{1, 2, \ldots, n\}$.

基本行列の安全性条件版
1. すべての$S \in \Gamma_F^*$ に対して，$X_0[S]$と$X_1[S]$ は適当な列の並べ替えで等しくできる．
2. $HW(OR(X_0[S])) = HW\big(OR(X_1[S])\big),\ \forall S \in \Gamma_F$.

この２つの命題は同値．２は線形制約の形で書ける．

同値性の直観的な理解　（その１）

$$X = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

任意の2行

の内訳

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

2列　1列　1列　2列

頻度が完全に一致

$$Y = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

任意の2行

の内訳

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

2列　1列　1列　2列

同値性の直観的な理解　（その２）

$$X = \begin{matrix} 1 & 2 & \cdots & \cdots & m \end{matrix}\begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \cdots & \cdots & 0 \end{bmatrix}$$

$$Y = \begin{matrix} 1 & 2 & \cdots & \cdots & m \end{matrix}\begin{bmatrix} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 1 \end{bmatrix}$$

A_X, A_Y: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ に等しい列の添字集合

B_X, B_Y: $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ に等しい列の添字集合

C_X, C_Y: $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ に等しい列の添字集合

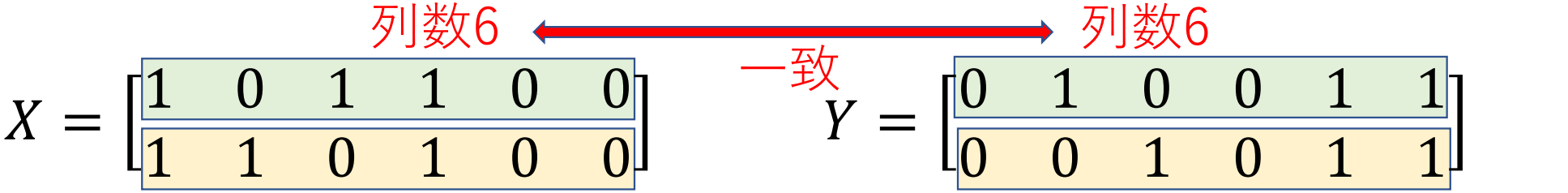
D_X, D_Y: $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ に等しい列の添字集合

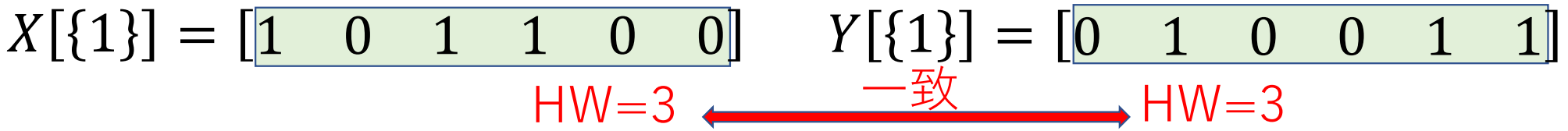
XとYが列の並べ替えで等しい

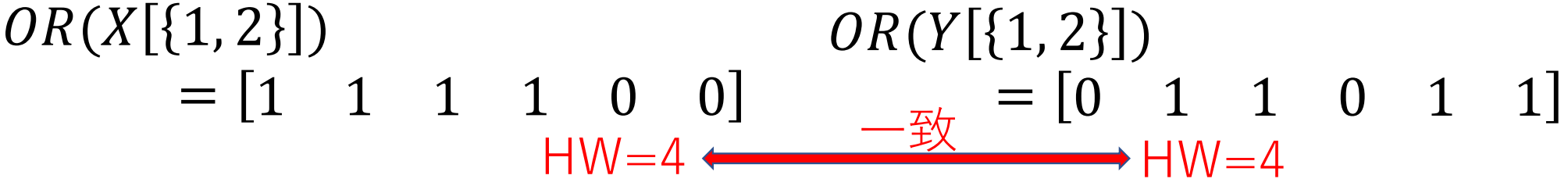
$$\Leftrightarrow$$

$$|A_X| = |A_Y|, |B_X| = |B_Y|,$$
$$|C_X| = |C_Y|, |D_X| = |D_Y|$$

同値性の直観的な理解　（その３）







同値性の直観的な理解　（その４）

$$X = \begin{matrix} 1 & 2 & \cdots & \cdots & m \end{matrix}\begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \cdots & \cdots & 0 \end{bmatrix} \qquad Y = \begin{matrix} 1 & 2 & \cdots & \cdots & m \end{matrix}\begin{bmatrix} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 1 \end{bmatrix}$$

$\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}$に等しい列の添字集合を$A, B, C, D$

$HW(X[\{1\}]) = HW(Y[\{1\}])$ ⟷ $|C_X| + |D_X| = |C_Y| + |D_Y|$

$HW(X[\{2\}]) = HW(Y[\{2\}])$ ⟷ $|B_X| + |D_X| = |B_Y| + |D_Y|$

$HW\big(OR(X[\{1,2\}])\big) = HW(OR(Y[\{1,2\}]))$

⟷ $|B_X| + |C_X| + |D_X| = |B_Y| + |C_Y| + |D_Y|$

列数が等しい ⟷ $|A_X| + |B_X| + |C_X| + |D_X| = |A_Y| + |B_Y| + |C_Y| + |D_Y|$

最適化の準備

- 参加者集合 $\mathcal{P} = \{1, 2, \dots, n\}$, $N = 2^n$.
- $j = 0, 1, \dots, N-1$ の２進数表記 $j = b_0 + b_1 2 + \cdots + b_{n-1} 2^{n-1}$ に対して $E_j = [b_0 \ b_1 \cdots b_{n-1}]^T$ とおく.
- $n = 3$のとき

$$E_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, E_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, E_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, E_3 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \cdots, E_6 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, E_7 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

- ブール行列X_bの列の中で, E_jに等しい列の個数をx_{bj}とする. $x_{bj} (b \in \{0,1\}, j = 0, 1, \dots, N-1)$は非負整数.

(3,4)-VCSの基本行列とE_j, x_{bj}

$$X_0 = \begin{matrix} E_{14} & E_{13} & E_{11} & E_7 & E_0 & E_0 \end{matrix}\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$x_{0,0} = 2$$

$$x_{0,7} = x_{0,11} = x_{0,13} = x_{0,14} = 1$$

$$x_{0,j} = 0 \quad (j \neq 0, 7, 11, 13, 14)$$

$$X_1 = \begin{matrix} E_1 & E_2 & E_4 & E_8 & E_{15} & E_{15} \end{matrix}\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$x_{1,15} = 2$$

$$x_{1,1} = x_{1,2} = x_{1,4} = x_{1,8} = 1$$

$$x_{1,j} = 0 \quad (j \neq 1, 2, 4, 8, 15)$$

画素拡大の最小化

Iwamoto (2012)
Shyu&Chen (2012)

目的関数 $\sum_{j=0}^{N-1} x_{0j} \rightarrow \min$

X_0 の列数を最小化

制約条件 $\sum_{j=0}^{N-1} x_{0j} = \sum_{j=0}^{N-1} x_{1j}$

X_0 の列数= X_1 の列数

$$\sum_{j=0}^{N-1} x_{0j}\, OR\big(E_j[S]\big) + 1 \leq \sum_{j=0}^{N-1} x_{1j}\, OR\big(E_j[S]\big), \quad \forall S \in \Gamma_Q^*$$

($HW(X_0[S])$, $HW(X_1[S])$)

SIが復元できる条件

$$\sum_{j=0}^{N-1} x_{0j}\, OR\big(E_j[S]\big) = \sum_{j=0}^{N-1} x_{1j}\, OR\big(E_j[S]\big), \quad \forall S \in \Gamma_F$$

($HW(X_0[S])$, $HW(X_1[S])$)

安全性条件

$x_{0j}, x_{1j}\ (j = 0, 1, \ldots, N-1)$ は非負整数

相対差の最大化の考え方

相対差 $$\alpha = \min_{S \in \Gamma_Q^*} \frac{HW\left(OR(X_1[S])\right) - HW\left(OR(X_0[S])\right)}{m}$$

$$= \min_{S \in \Gamma_Q^*} \frac{\sum_{j=0}^{N-1} x_{1j} OR(E_j[S]) - \sum_{j=0}^{N-1} x_{0j} OR(E_j[S])}{\sum_{j=0}^{N-1} x_{0j}} \to \max$$

この値は $\sum_{j=0}^{N-1} x_{0j} = \sum_{j=0}^{N-1} x_{1j}$ の値によらない.

$\sum_{j=0}^{N-1} x_{0j} = \sum_{j=0}^{N-1} x_{1j} = 1$ とおいて線形計画法で解く.

最小値の最大化のための変数zを用意する.

相対差の最大化

古賀 (2016)
Okada-K. (2017)

目的関数　$z \to \max$

制約条件　$\sum_{j=0}^{N-1} x_{0j} = \sum_{j=0}^{N-1} x_{1j} = 1$　　X_0 の列数= X_1 の列数

$$\underbrace{\sum_{j=0}^{N-1} x_{1j}\, OR(E_j[S])}_{HW(X_1[S])} - \underbrace{\sum_{j=0}^{N-1} x_{0j}\, OR(E_j[S])}_{HW(X_0[S])} \geq z, \qquad \forall S \in \Gamma_Q^*$$

SIが復元できる条件

$$\underbrace{\sum_{j=0}^{N-1} x_{0j}\, OR(E_j[S])}_{HW(X_0[S])} = \underbrace{\sum_{j=0}^{N-1} x_{1j}\, OR(E_j[S])}_{HW(X_1[S])}, \qquad \forall S \in \Gamma_F$$

安全性条件

$x_{0j}, x_{1j}\ (j = 0, 1, \ldots, N-1)$ は非負実数

数値結果

- MacBook Pro メモリ32M, CPU 2.4GHz 8コア Intel Core i9
- Mathematica 12 上で最適化
- (t,n)-VCSにおけるK. (2002) の準最適な結果と比較.

- $2 \leq n \leq 9$ の範囲で最適解を出力.　$n = 9$ で 1時間程度で終了.
- αの値は基本的に等しい（ $(5,9)$-VCSのみ例外）
- $(5,9)$-VCSで $\alpha = \frac{3}{200}, m = 200$ の最適解を出力. 既存手法では $\alpha = \frac{13}{896}, m = 8064.$
- $(6,9)$-VCSで$\alpha = \frac{1}{147}, m = 441$ の最適解を出力. 既存手法では $\alpha = \frac{1}{147}, m = 1764.$

これからの問題意識

- 最適解は$n \leq 10$程度なら現実的な時間で求まることを確認済み.
- 最適解が求まればそれで終わりなのか？

- 最適解の特徴づけを行えるか？たとえば固定したt に対する(t, n)-VCSの最適な基本行列の形は見つかるか？

- 最適化ソルバーは最適解を１つ見つけ出して終了するケースがほとんど．いい最適解が見つかればよいが・・・

すべてのシェアを重ねたときの相対差

- (t,n)-VCSでは，t枚のシェアを重ねれば，秘密画像SI が復元される．
- t枚以上のシェアを重ねることにより，視認性をさらに上げることが可能．
- n枚すべてのシェアを重ねたときの相対差

$$\alpha_{all} = \frac{HW\left(OR(X_1)\right) - HW\left(OR(X_0)\right)}{m}$$

- この値は，線形計画法で最適化できる．

α_{all}の最適化の結果（$t = 3$の場合）

Okada-K. (2017)

n	3	4	5	6	7	8	9	10	11
α^*_{all}	1/4	1/3	4/9	1/2	9/16	3/5	16/25	2/3	25/36

$$\alpha^*_{all} = \begin{cases} \left(\dfrac{n-1}{n+1}\right)^2 & (n\text{が奇数のとき}) \\ \dfrac{n-2}{n+2} & (n\text{が偶数のとき}) \end{cases}$$

と推定される（$3 \leq n \leq 11$ では真に最適）．この値を達成する基本行列を構成したい．

BIBD (Balanced Incomplete Block Design)

$Y = \{y_1, y_2, \ldots, y_v\}$: v個の要素からなる集合． Yの各要素を点.

$\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$: $B_i \subset Y$. $\mathcal{B}$の各要素をブロック． $|\mathcal{B}| = b$.

定義 2

v, k, λ を$v > k \geq 2$かつ$\lambda \geq 1$を満たす整数とする.

組$(Y, \mathcal{B})$が以下の 3 条件を満たすとき，(v, k, λ)-BIBDという.

1. $|Y| = v$.
2. $\mathcal{B}$ に属する各ブロックは，ちょうどk個の点を要素にもつ.
3. 任意の$y, y' \in Y, y \neq y'$に対して， $\{y, y'\} \subset B$を満たす$B \in \mathcal{B}$は ちょうど λ 個である.

(v, k, λ)-BIBDの例と補デザイン

$Y = \{1, 2, 3, 4, 5, 6, 7\}$

$v = |Y| = 7$

$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}$

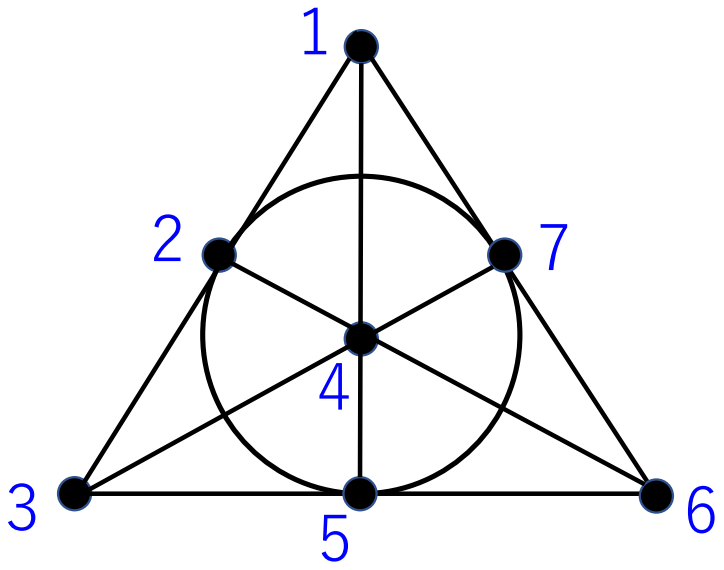
$k = |B| = 3, B \in \mathcal{B}$

とすると，$(Y, \mathcal{B})$は$(7, 3, 1)$-BIBD である．

$\overline{\mathcal{B}} = \{Y \setminus B : B \in \mathcal{B}\}$とすると，

$(Y, \overline{\mathcal{B}})$は$(7, 4, 2)$-BIBD である．

$(Y, \overline{\mathcal{B}})$を$(Y, \mathcal{B})$の補デザイン



Fano平面

接続行列

$(Y, \mathcal{B})$を(v, k, λ)-BIBDとするとき，接続行列$M = (m_{ij})$が定まる．

$$m_{ij} = \begin{cases} 1, & y_i \in B_j \text{のとき} \\ 0, & \text{それ以外のとき} \end{cases}$$

$Y = \{1, 2, 3, 4, 5, 6, 7\}$

$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}$

の場合の接続行列Mは右の通り．

$$M = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \left[\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] \end{array}$$

r（B_1〜B_3）

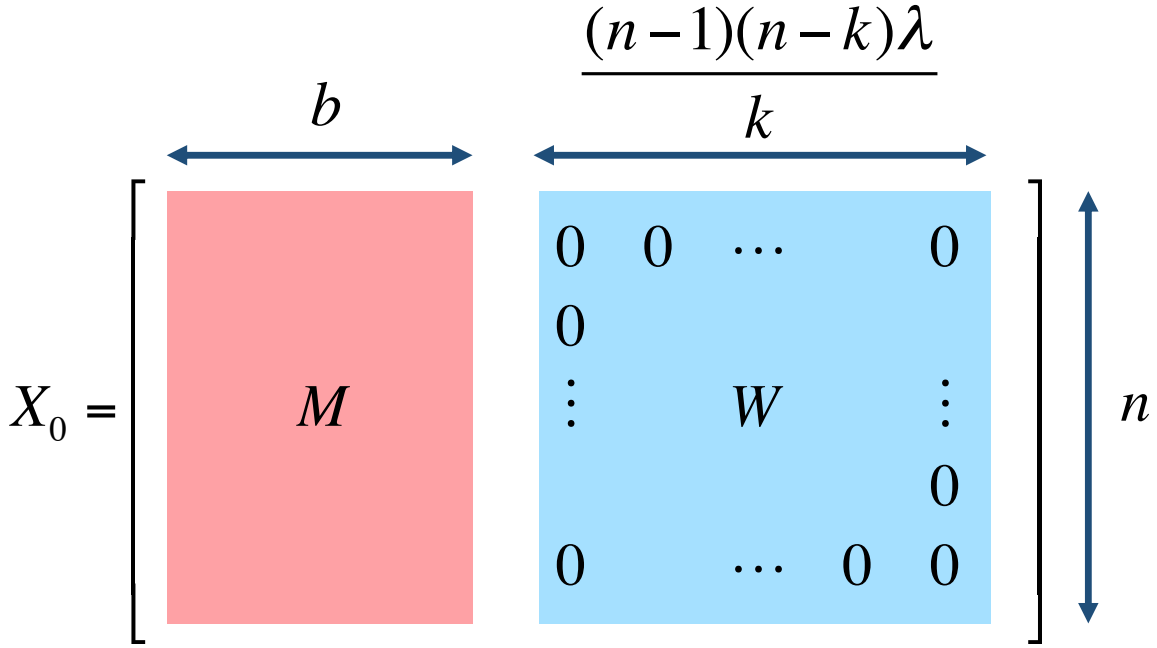
v（行）

b（列）

$b = |\mathcal{B}|, r = |\{B \in \mathcal{B} : y \in B\}|$ と定める．rの値は$y \in Y$によらない．

BIBDを用いた基本行列の構成（その１）

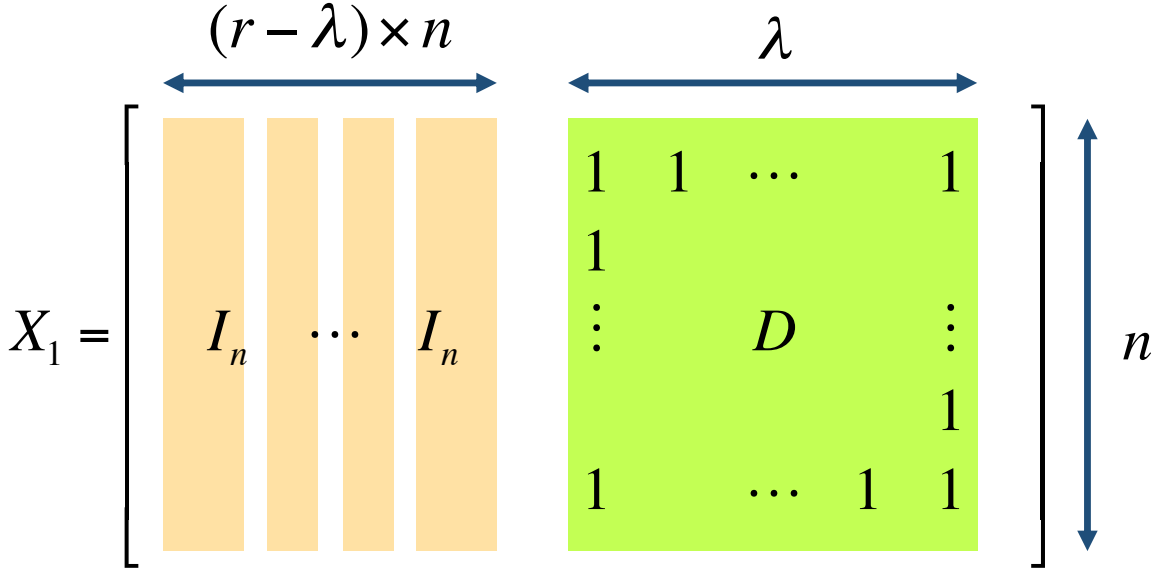
X_0を，(n,k,λ)-BIBDの接続行列をMと，
大きさ$n\times\frac{(n-1)(n-k)\lambda}{k}$で要素がすべて0の行列$W$の連接と定義.



1 行のHW
r
2 行のORのHW
$2r-\lambda$

BIBDを用いた基本行列の構成（その２）

X_1を，$(r-\lambda)$個のn次単位行列I_nと，
大きさ$n \times \lambda$で要素がすべて1の行列Dの連接と定義.



1 行のHW
r
2 行のORのHW
$2r-\lambda$

X_0と一致！

構成した基本行列の性質 1

定理 1 (Okada & K. (2017))
(n, k, λ)-BIBDが$n < 2k + 1$を満たすとき，先に構成した(X_0, X_1)は$(3, n)$-VCS の基本行列になる．このときの画素拡大mとn枚すべてのシェアを重ねたときの相対差α_{all}は

$$m = \frac{(n-1)(n-k+1)\lambda}{k-1} = r(n-k+1)$$

$$\alpha_{all} = \frac{(n-k)(k-1)\lambda}{(n-k+1)k}$$

を満たす.

構成した基本行列の性質 2

定理 1 より， n枚すべてのシェアを重ねたときの相対差α_{all}は

$$\alpha_{all} = \frac{(n-k)(k-1)\lambda}{(n-k+1)k}$$

であった． α_{all}をnを固定してkについて最大化すると，

nが奇数$(n \geq 5)$のとき， $k = \frac{n+1}{2}$で最大， $\alpha^*_{all} = \left(\frac{n-1}{n+1}\right)^2$

nが偶数$(n \geq 4)$のとき， $k = \frac{n}{2}, \frac{n+2}{2}$で最大， $\alpha^*_{all} = \frac{n-2}{n+2}$

であることがわかる．

最適なBIBD

- n が5以上の奇数のとき，$k = \frac{n+1}{2}$ でα_{all}は最大値をとる．一般に $r = \frac{(n-1)\lambda}{k-1}$ だから，このとき$r = 2\lambda$.
- ブロック数 b は一般に$b = \frac{nr}{k}$ を満たすから，

$$b = \frac{4n\lambda}{n+1} = 4\lambda - \frac{4\lambda}{n+1}$$

がいえる．bは整数だから，$4\lambda \equiv 0 \pmod{n+1}$.

- よって $n = 4p - 1$ ($p \geq 2$は整数)のときは，$(4p-1, 2p, p)$-BIBDで最適になる．

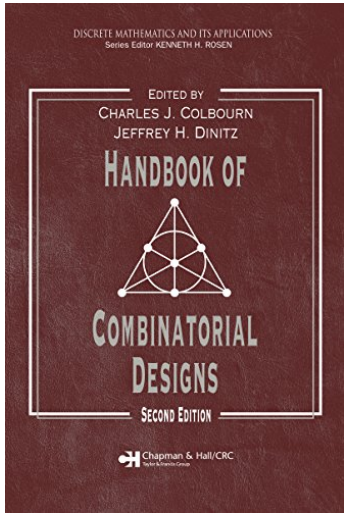
アダマール行列との関係

- そもそも，$(4p-1, 2p, p)$-BIBD は存在するか？　または，その補デザインである $(4p-1, 2p-1, p-1)$-BIBDは存在するか？

- $4p$ 次のアダマール行列H から，すべて 1 の行と列を除いてできる行列で$-1 \to 0$ としたものを接続行列にもつ BIBDは$(4p-1, 2p-1, p-1)$-BIBD になる．なおn次のアダマール行列は$HH^T = nI_n$ を満たす成分が± 1の行列と定義する．

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

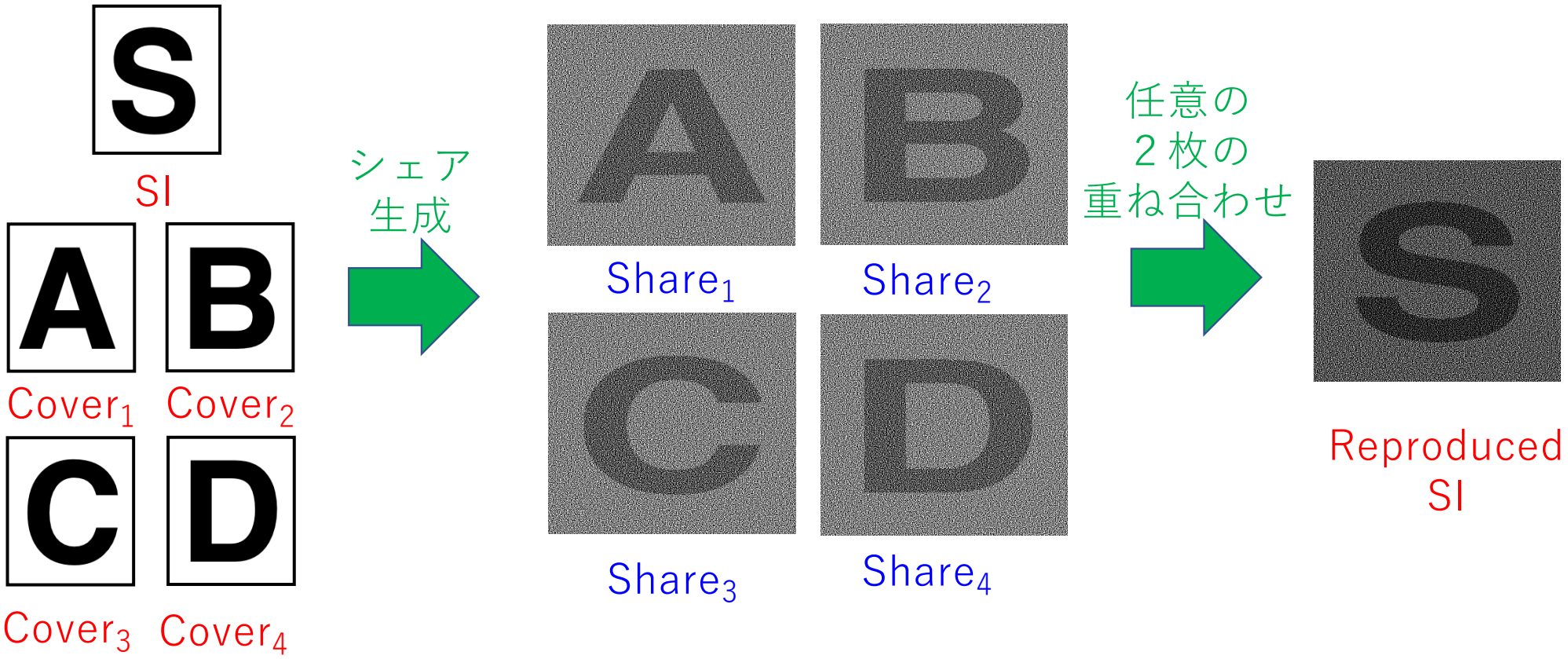
- $4p$次のアダマール行列は $4p < 668$ で存在する．



EVCS (Extended VCS)

- 2001年にAtenieseらにより提案.　（原型はDroste (1996)にも）
- 1枚の秘密画像(SI)の他，n 枚のカバー画像 (Cover_i) を用いて，n 枚のシェアを生成.
- シェア i 上では Cover_i が視認できる.
- この他の機能はVCSと同じ.
- 復号時に視認できるのはSIのみ.

EVCSの例　～(2,4)-EVCS～



EVCSの基本行列の定義

定義 2（Ateniese et al. (2001), Shyu(2014), Sekine & K. (2020)）

$\Gamma = (\Gamma_Q, \Gamma_F)$：参加者集合$\mathcal{P} = \{1, 2, \dots, n\}$ 上のアクセス構造.

2^n個の$n \times m$ ブール行列の組$\left\{\left(X_0^{c_1 \cdots c_n}, X_1^{c_1 \cdots c_n}\right)\right\}_{c_1,\dots,c_n \in \{0,1\}}$ は以下の 3 条件を満たすとき，アクセス構造Γを実現する基本行列という.

1. すべての$S \in \Gamma_Q^*$ に対して$0 \le l_S < h_S \le m$を満たす整数l_S, h_Sが存在して

SIの復元条件

$$HW\left(OR\left(X_0^{c_1 \cdots c_n}[S]\right)\right) = l_S, HW\left(OR\left(X_1^{c_1 \cdots c_n}[S]\right)\right) = h_S, \qquad \forall c_1, \dots, c_n \in \{0,1\}$$

2. すべての$S \in \Gamma_F$ と$c_1, \dots, c_n \in \{0,1\}$に対して

$$HW\left(OR\left(X_0^{c_1,\dots,c_n}[S]\right)\right) = HW\left(OR\left(X_1^{c_1,\dots,c_n}[S]\right)\right)$$

SIの安全性条件

3. すべての$i = 1,2, \dots, n$ に対して，$0 \le l_i < h_i \le m$を満たす整数l_i, h_iが存在し

$$HW\left(OR\left(X_b^{c_1 \cdots c_{i-1} 0 c_{i+1} \cdots c_n}[\{i\}]\right)\right) = l_i, HW\left(OR\left(X_b^{c_1 \cdots c_{i-1} 1 c_{i+1} \cdots c_n}[\{i\}]\right)\right) = h_i,$$

$$\forall b, c_1, \dots, c_{i-1}, c_{i+1}, \cdots c_n \in \{0,1\}$$

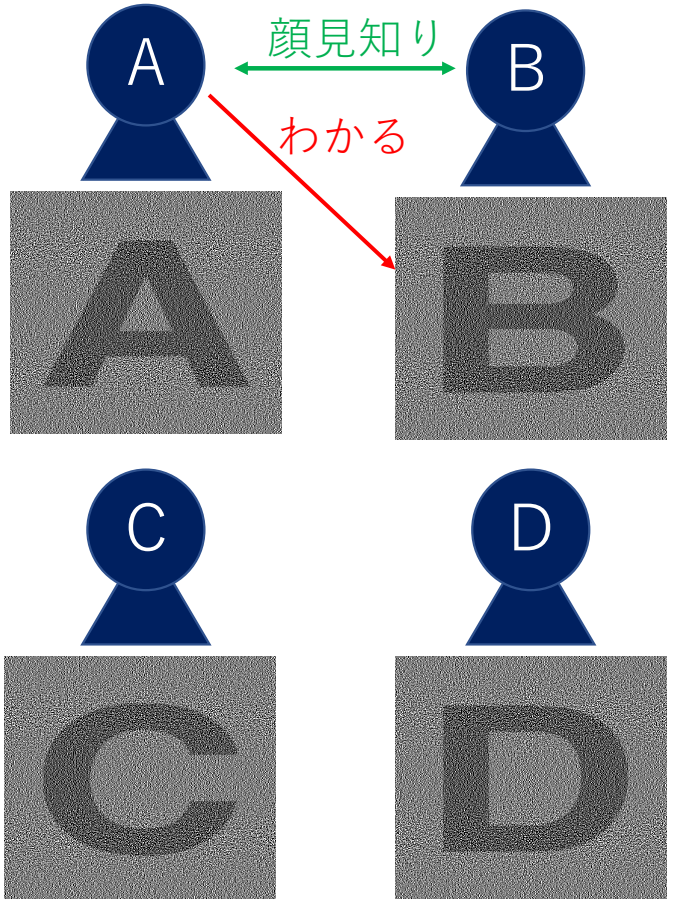
Cover$_i$の視認条件

最適なEVCSの基本行列

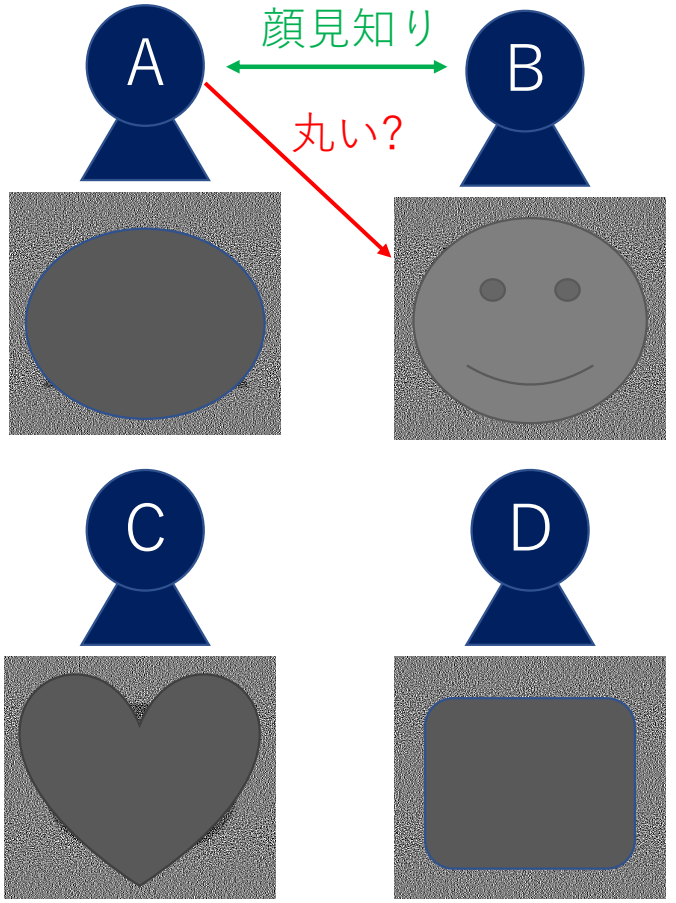
- 整数計画法を用いることで，EVCSの画素拡大mを最小化できる．
- 変数の数は2^{2n+1}個（nは参加者数）．大きなnでは現実時間では解けない．
- $(2,4)$-EVCS, $(2,5)$-EVCSなどでは，既存方法より小さい画素拡大の基本行列を構成できることを示した．（ISITA2020で報告ずみ）

EVCSの用い方

カバー画像に参加者名が記載



他の参加者のカバー画像が不明



カバー画像の安全性

- 定義２を満たすEVCSについて，次を示すことができる．

$(B, C_1, \ldots, C_n)$の同時分布を$P_{BC_1 \cdots C_n}$，シェア i の画素拡大のパターンをM_iと表す．定義２の条件３が満たされるとき，任意の$P_{BC_1 \cdots C_n}$に対して $I(M_i; BC_1 \cdots C_{i-1}C_{i+1} \cdots C_n | C_i) = 0$ が成り立つ．

- つまり，参加者iがどんなにシェアパターンM_iを解析しても，$BC_1 \cdots C_{i-1}C_{i+1} \cdots C_n$に関する情報は，$C_i$ からわかる以上に得ることができない．

3. すべての$i = 1,2, \ldots, n$ に対して，$0 \leq l_i < h_i \leq m$を満たす整数l_i, h_iが存在し

$$HW\left(OR\left(X_b^{c_1 \cdots c_{i-1} 0 c_{i+1} \cdots c_n}[\{i\}]\right)\right) = l_i, HW\left(OR\left(X_b^{c_1 \cdots c_{i-1} 1 c_{i+1} \cdots c_n}[\{i\}]\right)\right) = h_i,$$

$$\forall b, c_1, \ldots, c_{i-1}, c_{i+1}, \cdots c_n \in \{0,1\}$$

Cover$_i$の視認条件

まとめ

- 視覚暗号の最適化の手法（画素拡大，相対差）について説明しました.
  - 画素拡大は整数計画法で最小化できる.
  - 相対差は線形計画法で最大化できる.

- 講演者の最近の研究についてもお話ししました.
  - BIBDを用いた$(3, n)$-VCSの構成
  - EVCSにおけるカバー画像の安全性

- 「最適解の特徴づけ」は今後の研究課題の１つ.