情報･システム工学概論

情報を効率よく安全に伝送するための符号化技術

暗号理論

計算量的安全性に基づく暗号･情報セキュリティ符号化

コンピュータのモデル　　多項式時間の計算：容易

例：　公開鍵暗号など

情報理論

情報量的安全性に基づく暗号･情報セキュリティ符号化

コンピュータのモデル　　無限大の計算パワー

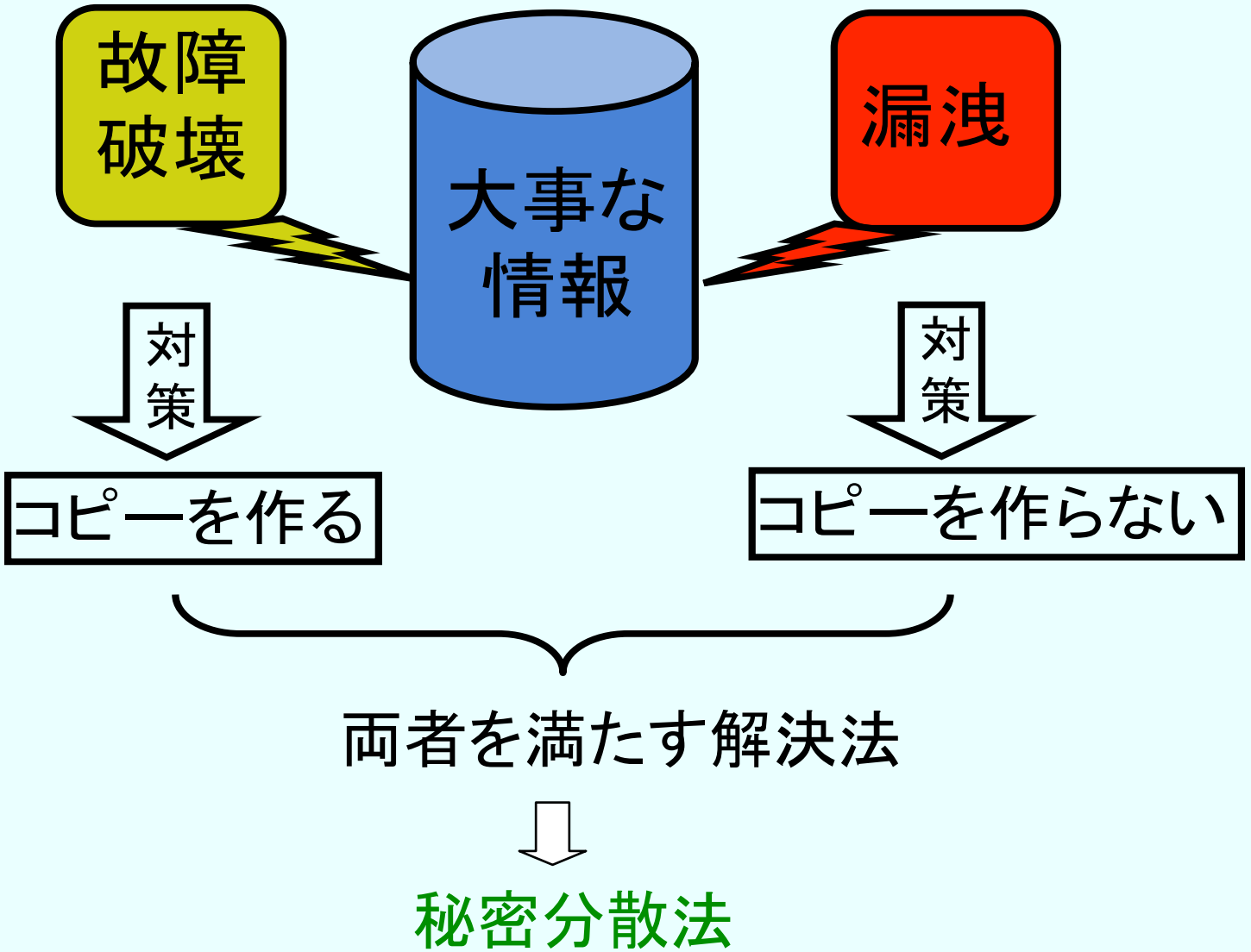
例：　秘密分散法など

秘密分散法

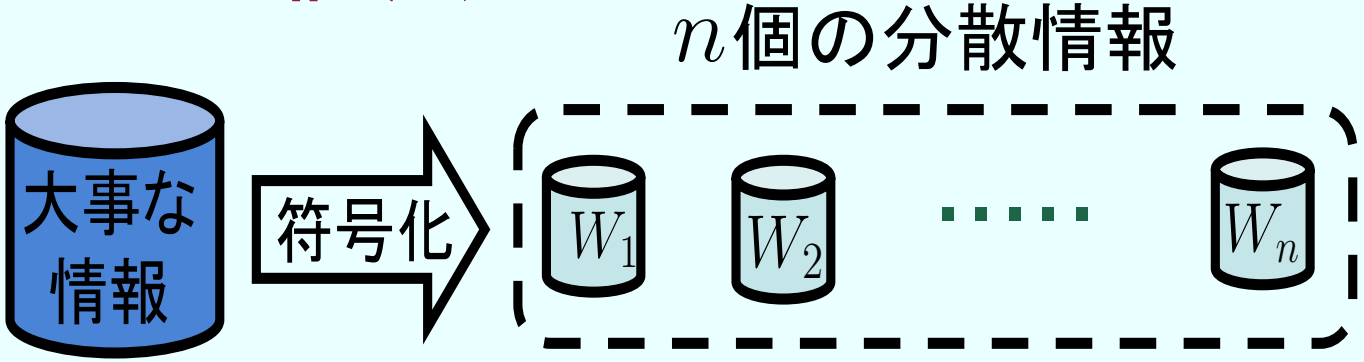
Secret Sharing Scheme

- しきい値法
- 一般アクセス構造
- ネットワーク符号化
- 視覚復号型秘密分散法
- etc.

秘密分散法（Secret Sharing Scheme）

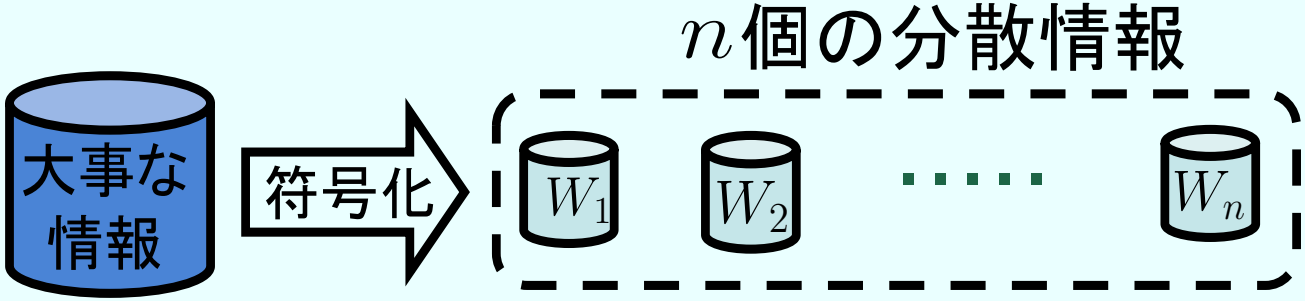


(k, n) しきい値法



- 任意の k 個の分散情報 ⇨ 元の情報を復元できる
  - $n-k$ 個まで故障/破壊されても安全
- 任意の $k-1$ 個の分散情報 ⇨ 元の情報が全く分からない
  - $k-1$ 個まで盗まれても安全

$(2, n)$ しきい値法

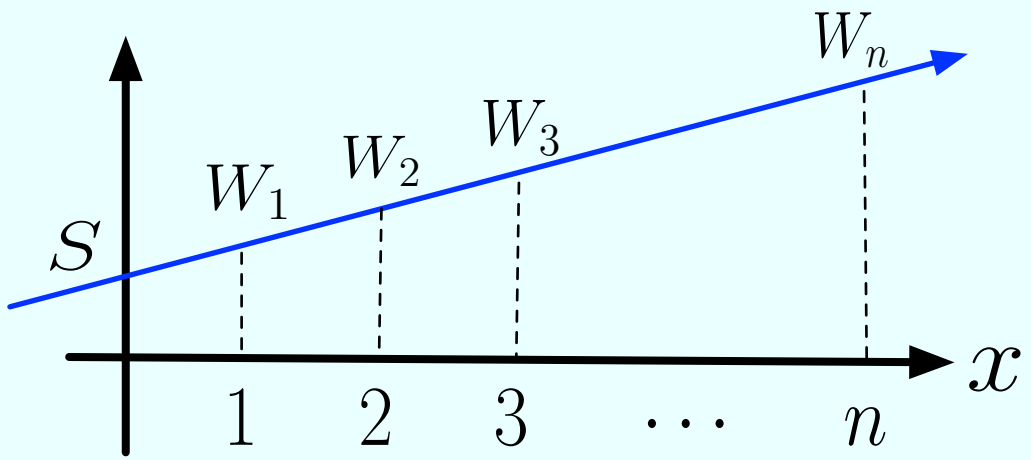


任意の 2 個の分散情報 ⇨ 元の情報を復元できる
$n-2$ 個まで故障/破壊されても安全
任意の 1 個の分散情報 ⇨ 元の情報が全く分からない
1 個まで盗まれても安全

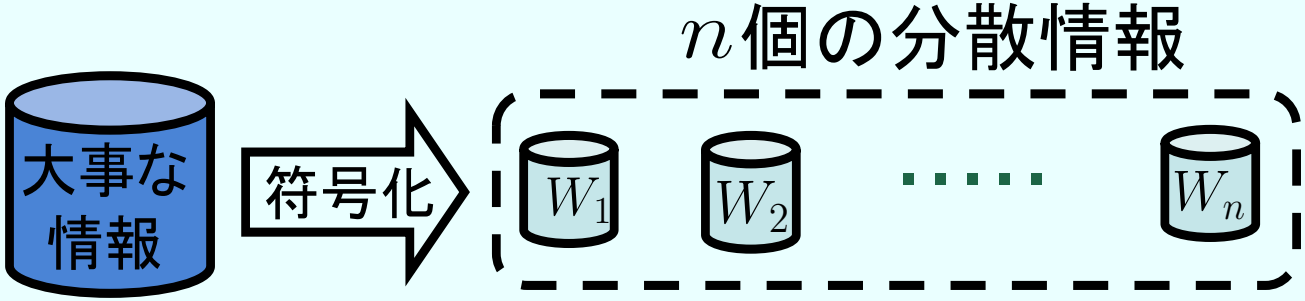
$$f(x) = S + Rx$$

S: 秘密情報　　R: 乱数

分散情報: $W_i = f(i)$



$(2, n)$ しきい値法

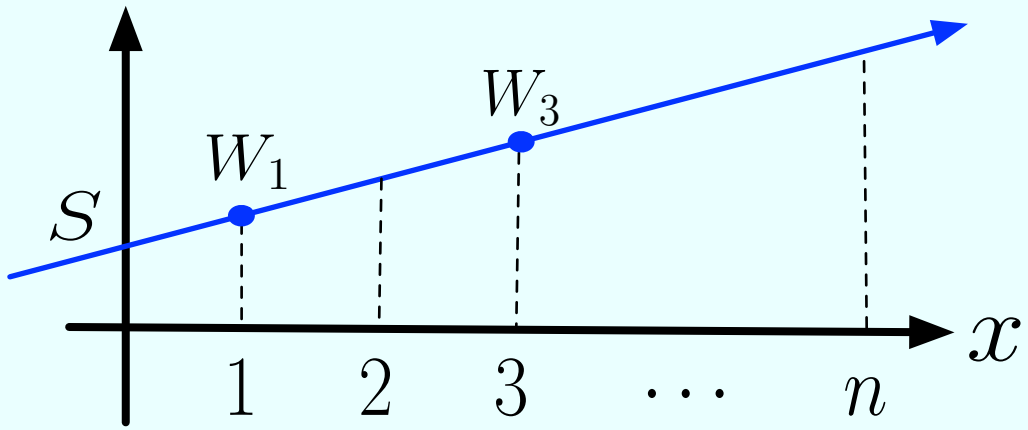


任意の 2 個の分散情報 ⇨ 元の情報を復元できる
$n-2$ 個まで故障/破壊されても安全
任意の$k-1$ 個の分散情報 ⇨ 元の情報が全く分からない
1 個まで盗まれても安全

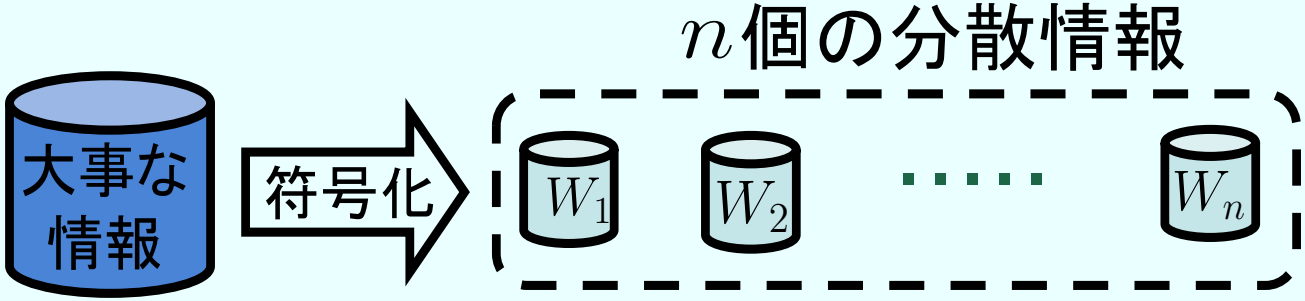
$$f(x) = S + Rx$$

S: 秘密情報　　R: 乱数

分散情報: $W_i = f(i)$



$(2, n)$ しきい値法

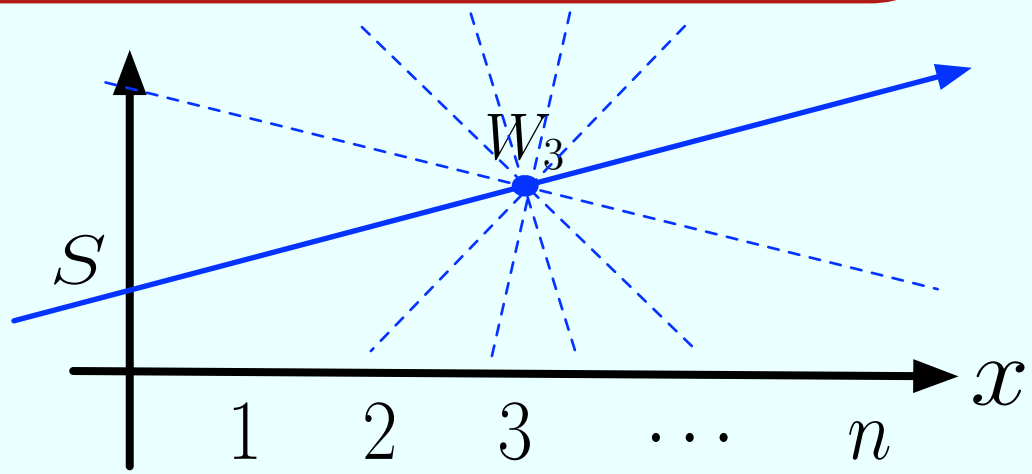


任意の 2 個の分散情報 ⇨ 元の情報を復元できる
$n-2$ 個まで故障/破壊されても安全
任意の$k-1$ 個の分散情報 ⇨ 元の情報が全く分からない
1 個まで盗まれても安全

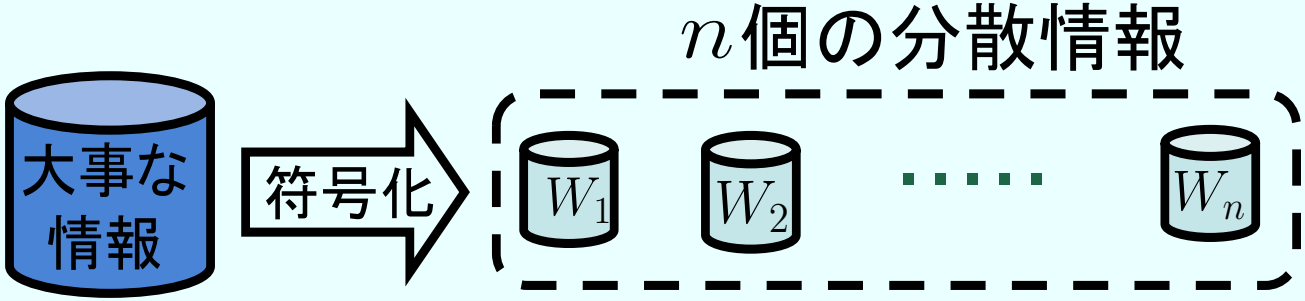
$$f(x) = S + Rx$$

S: 秘密情報　　R: 乱数

分散情報: $W_i = f(i)$



$(2, n)$ しきい値法

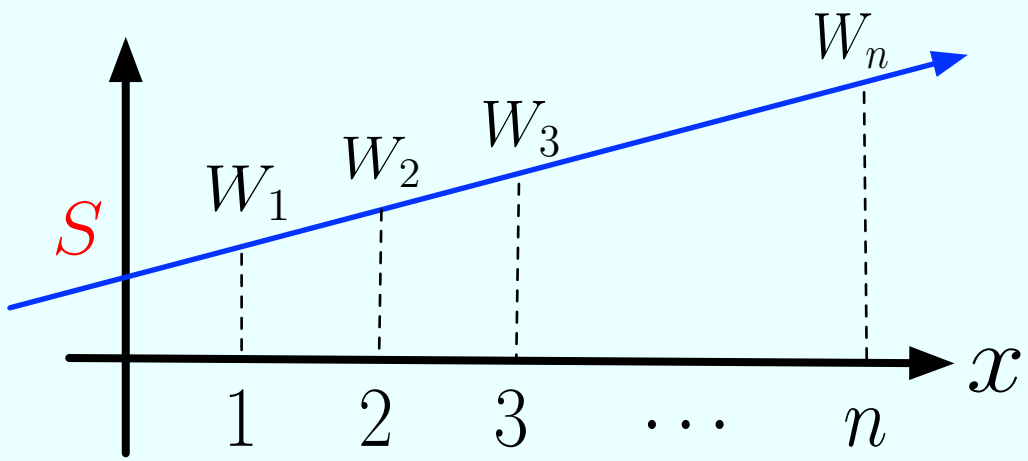


任意の 2 個の分散情報 ⇨ 元の情報を復元できる
$n-2$ 個まで故障/破壊されても安全
任意の$k-1$ 個の分散情報 ⇨ 元の情報が全く分からない
1 個まで盗まれても安全

$$f(x) = S + Rx \mod P$$

S: 秘密情報 $(0 \leq S < P)$　　R: 乱数 $(0 \leq R < P)$

分散情報: $W_i = f(i)$

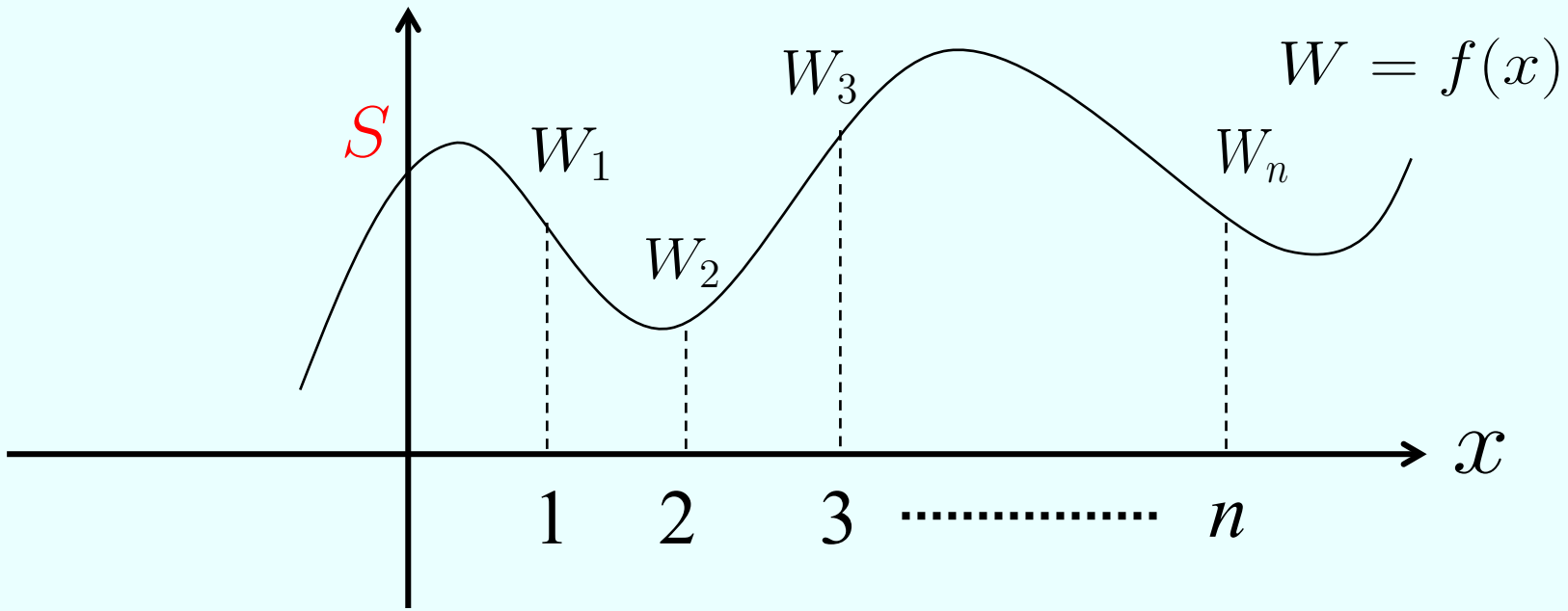


(k, n) しきい値法

Shamir のしきい値法 (1979)

$$W_i = f(i)\,, \quad i = 1, 2, \cdots, n$$

$$f(x) = S + R_1 x + R_2 x^2 + \cdots + R_{k-1} x^{k-1}$$



(k, n) しきい値法

Shamir のしきい値法 (1979)

$$W_i = f(i)\,, \quad i = 1, 2, \cdots, n$$

$$f(x) = S + R_1 x + R_2 x^2 + \cdots + R_{k-1} x^{k-1}$$

$$\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathrm{GF}(P) = \{0, 1, 2, \cdots, P-1\}$$

$$(W_1, W_2, W_3, \cdots, W_n) =$$

$$(S, R_1, R_2 \cdots, R_{k-1}) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

(k, n) しきい値法

$$(W_1, W_2, W_3, \cdots, W_n) = (S, R_1, R_2 \cdots, R_{k-1}) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

一般の行列に拡張

Karnin–Greene–Hellmanのしきい値法 (1983)

$$(S, W_1, W_2, \cdots, W_n) = (S, R_1, R_2, \cdots, R_{k-1})M$$

M : $(k+1) \times n$ 行列 (任意の k 列が線形独立)

(k, n) しきい値法

k 個で復号可能 ➡ $H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_k}) = 0$

$k-1$個で情報が漏れない ➡ $H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) = H(S)$

$$
\begin{aligned}
H(W_i) &\geq H(W_i|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) \\
&= H(W_i|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) - H(W_i|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}, S) \\
&= I(S; W_i|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) \\
&= H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) - H(S|W_i, W_{i_1}, W_{i_2}, \cdots, W_{i_{k-1}}) \\
&= H(S)
\end{aligned}
$$

$H(W_j) = H(S)$ ⇨ 符号化効率が悪い ⇨ ランプ型しきい値法

(k, l, n)ランプ型しきい値法

Blakey-Meadows ランプ型しきい値法 (1984)
Yamamotoランプ型しきい値法 (1985)

秘密情報: $S = (S_0, S_1, \cdots, S_{l-1})$

分散情報: $W_i = f(i), \quad i = 1, 2, \cdots, n$

$$f(x) = S_0 + S_1 x + \cdots + S_{l-1} x^{l-1} + R_l x^l + \cdots + R_{k-1} x^{k-1}$$

$$(S_0, \cdots, S_{l-1}, W_1, \cdots, W_n) = (S_0, \cdots, S_{l-1}, R_l, \cdots, R_{k-1}) M$$

ランプ型しきい値特性

$0 \leq b \leq l$

$$H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-b}}) = \frac{b}{l} H(S),$$

$$H(W_j) = \frac{1}{l} H(S) \Rightarrow$$ 符号化効率がよい

(k, l, n)ランプ型しき

Blakey-Meadows ランプ

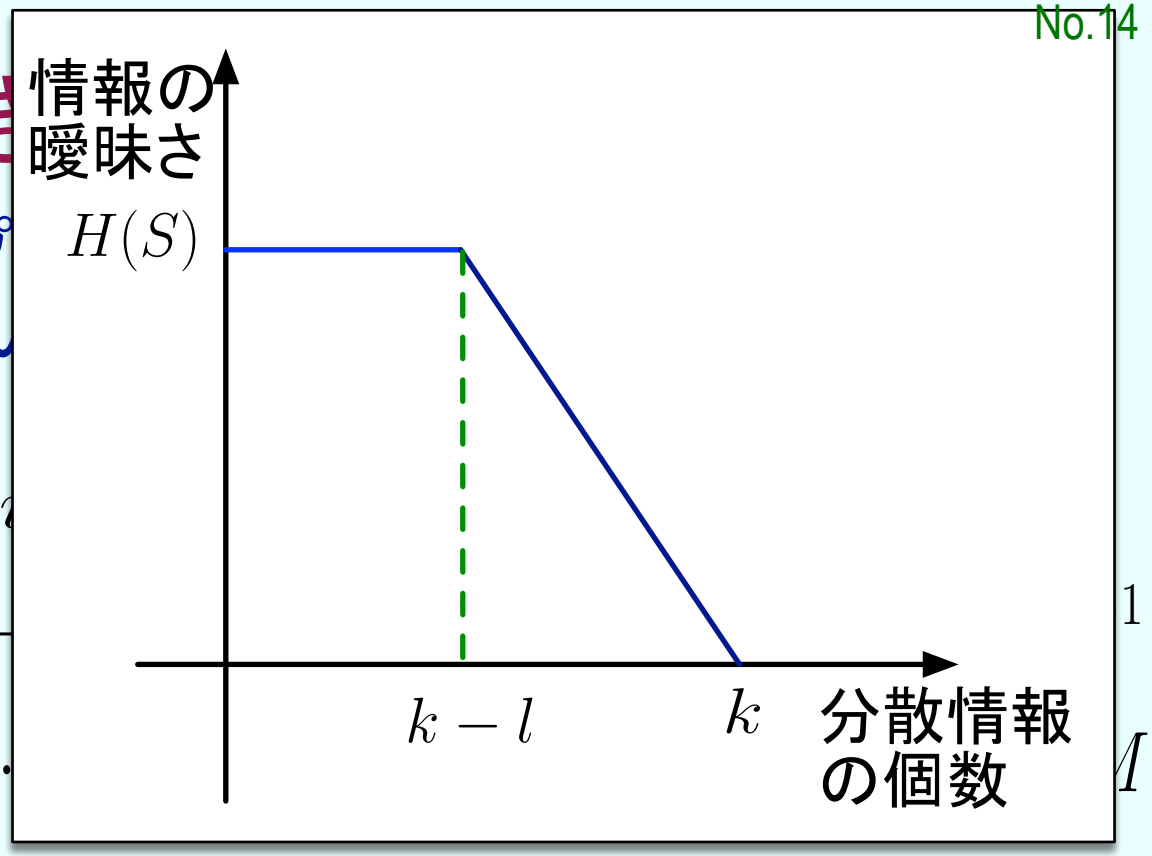
Yamamotoランプ型しきい

秘密情報: $S = (S_0,$

分散情報: $W_i = f($

$$f(x) = S_0 + S_1 x +$$

$$(S_0, \cdots, S_{l-1}, W_1, \cdots$$



1

M

ランプ型しきい値特性

$$0 \leq b \leq l$$

$$H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-b}}) = \frac{b}{l} H(S)\,,$$

$$H(W_j) = \frac{1}{l} H(S)$$ ⇨ 符号化効率がよい

(k, l, n)ランプ型しきい値法

Blakey–Meadows ランプ型しきい値法 (1984)
Yamamotoランプ型しきい値法 (1985)

秘密情報: $S = (S_0, S_1, \cdots, S_{l-1})$

分散情報: $W_i = f(i), \quad i = 1, 2, \cdots, n$

$$f(x) = S_0 + S_1 x + \cdots + S_{l-1} x^{l-1} + R_l x^l + \cdots + R_{k-1} x^{k-1}$$

$$(S_0, \cdots, S_{l-1}, W_1, \cdots, W_n) = (S_0, \cdots, S_{l-1}, R_l, \cdots, R_{k-1}) M$$

ランプ型しきい値特性

$$H(S|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-b}}) = \frac{b}{l} H(S), \quad 0 \le b \le l$$

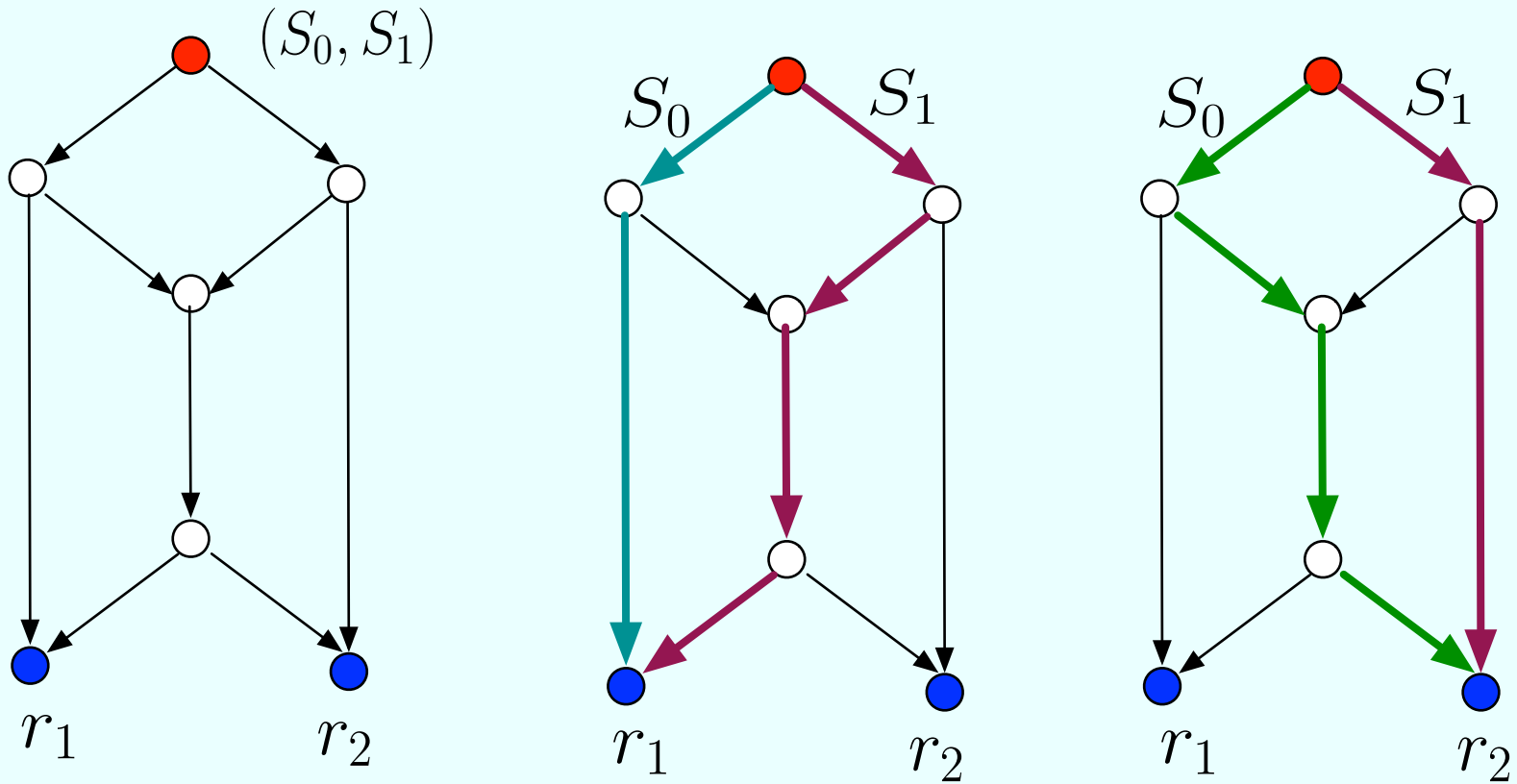
Strongly Secureなランプ型しきい値特性

$$H(S_{j_1}, S_{j_2}, \cdots, S_{j_b}|W_{i_1}, W_{i_2}, \cdots, W_{i_{k-b}}) = H(S_{j_1}, S_{j_2}, \cdots, S_{j_b})$$

$H(W_j) = \frac{1}{l} H(S)$ で実現可能

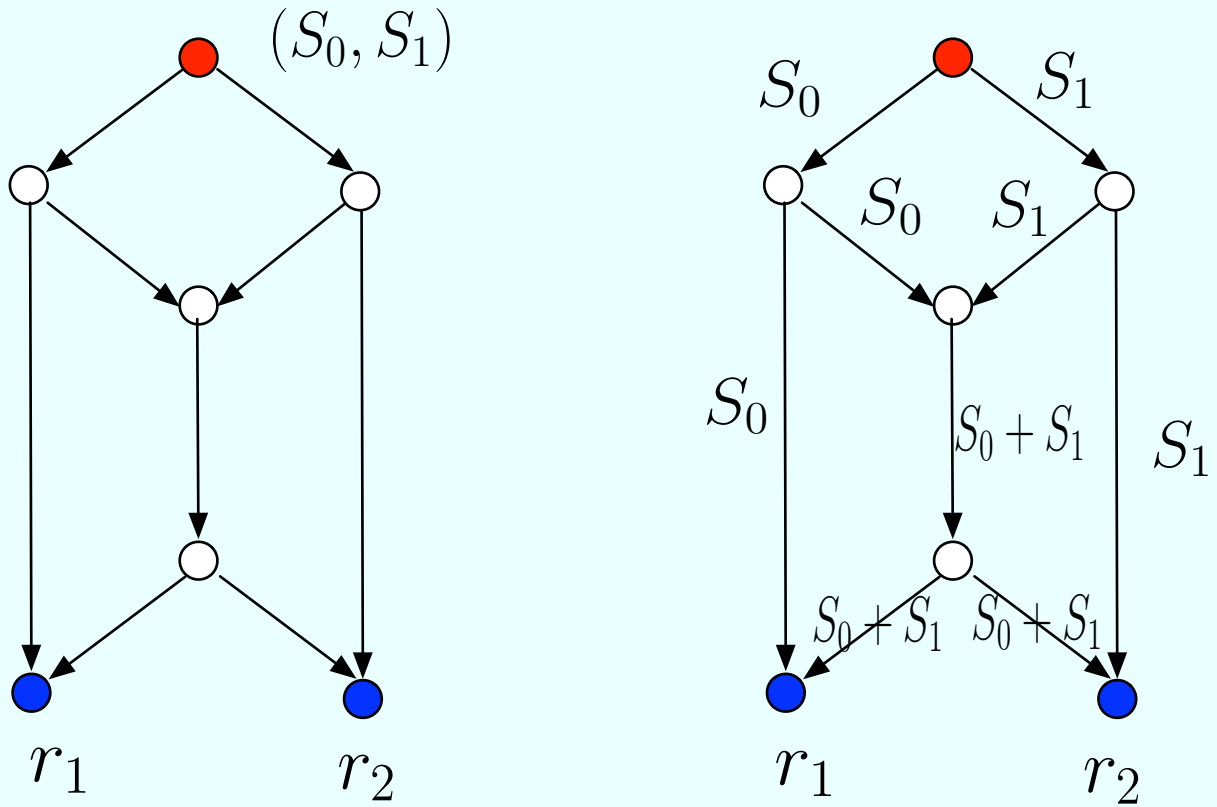
安全なネットワーク符号化(Secure Network Coding)

ネットワーク符号化 : Ahlswede–Cai–Li–Yeung (2000)



安全なネットワーク符号化(Secure Network Coding)

ネットワーク符号化 : Ahlswede–Cai–Li–Yeung (2000)

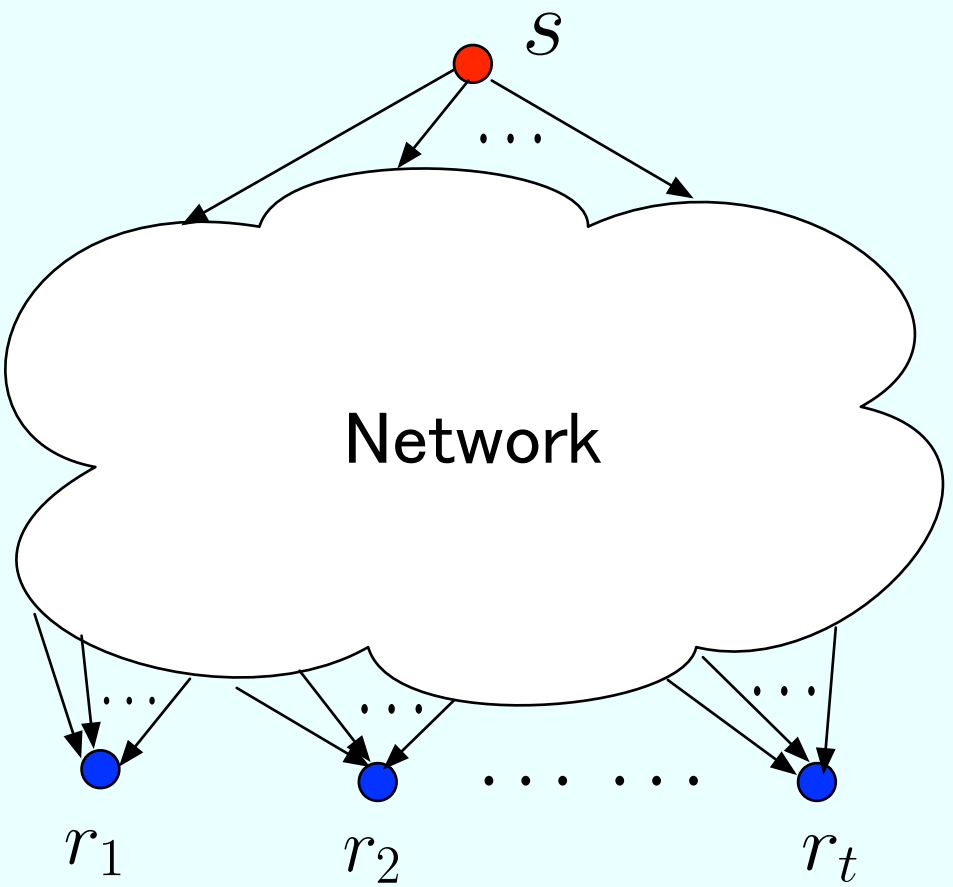


ネットワーク符号化の解説動画:

https://www.youtube.com/watch?v=B0ZcAWEvjCA

安全なネットワーク符号化(Secure Network Coding)

ネットワーク符号化：Ahlswede–Cai–Li–Yeung (2000)



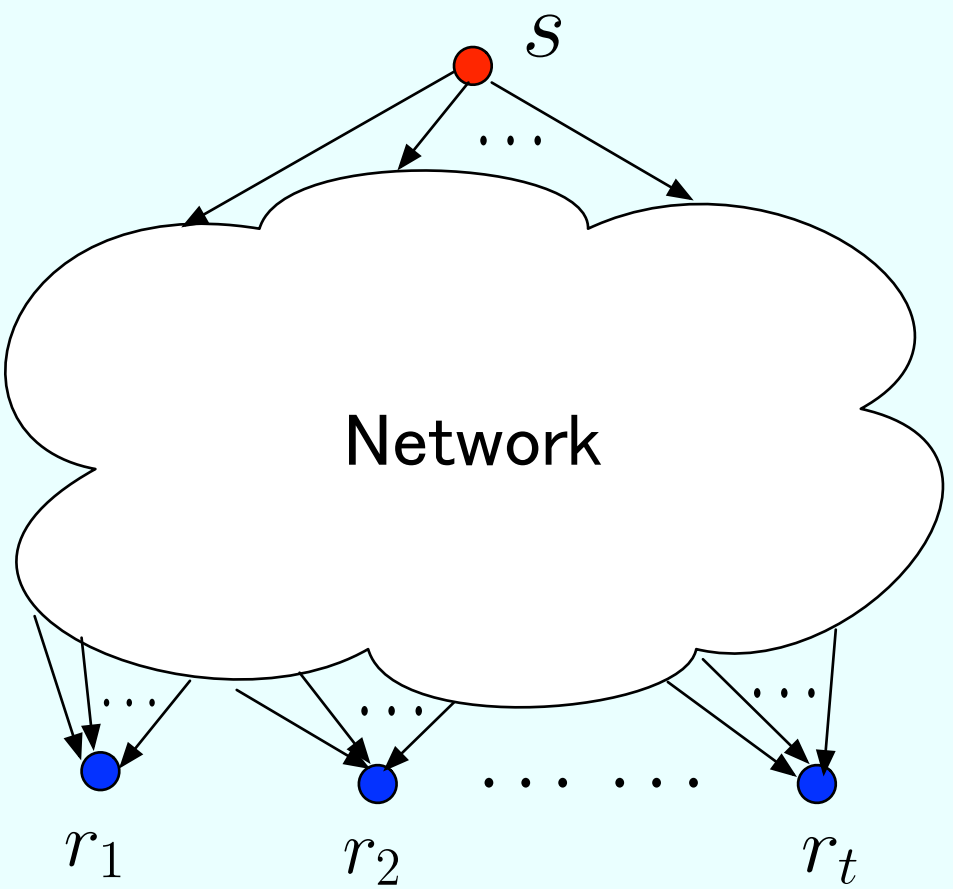
マルチキャスト容量

$$h = \min_r \mathrm{maxflow}(s, r)$$

線形ネットワーク符号化：Li–Yeung–Cai (2003)

安全なネットワーク符号化(Secure Network Coding)

t −secureネットワーク符号化： Cai−Yeung 2002



$t(t < h)$ 本の通信路で盗聴されても安全

マルチキャスト容量

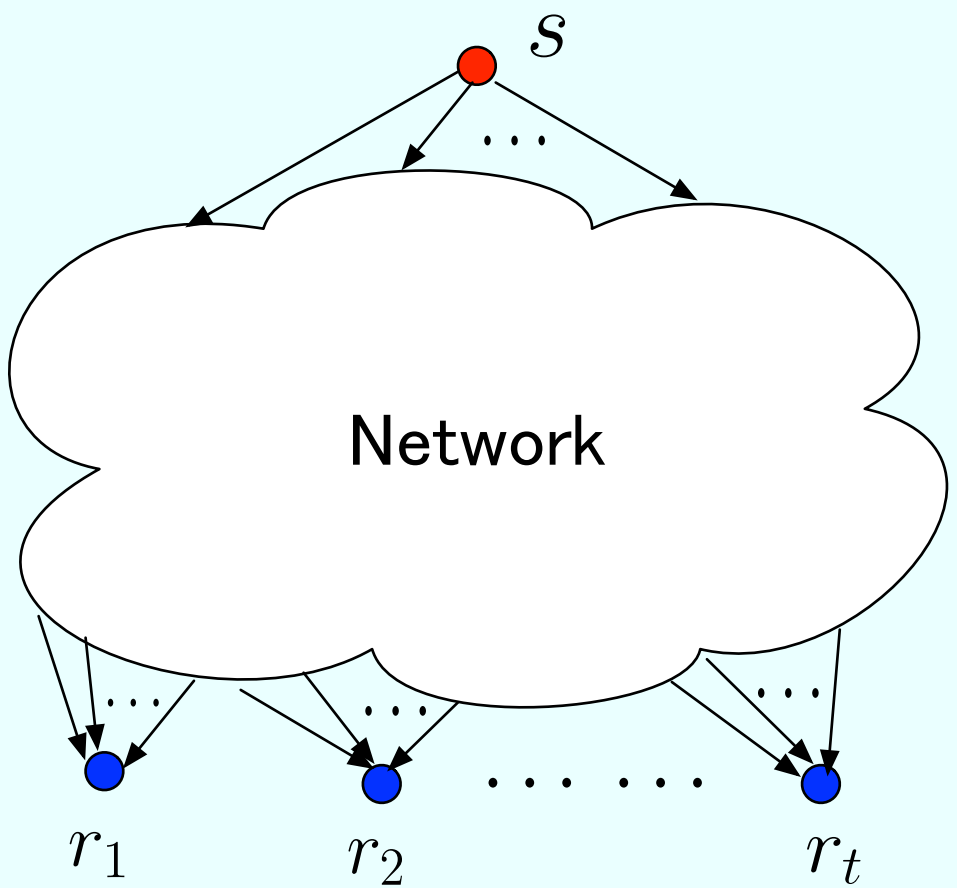
$$h = \min_r \mathrm{maxflow}(s, r)$$

送信可能な情報量 u

$$u \leq h - t$$

安全なネットワーク符号化(Secure Network Coding)

Strongly t−secureネットワーク符号化：Harada−Yamamoto 2002



$t(t < h)$ 本の通信路で盗聴されても安全

マルチキャスト容量

$$h = \min_{r} \mathrm{maxflow}(s, r)$$

送信可能な情報量 u

$$u \leq h - t$$

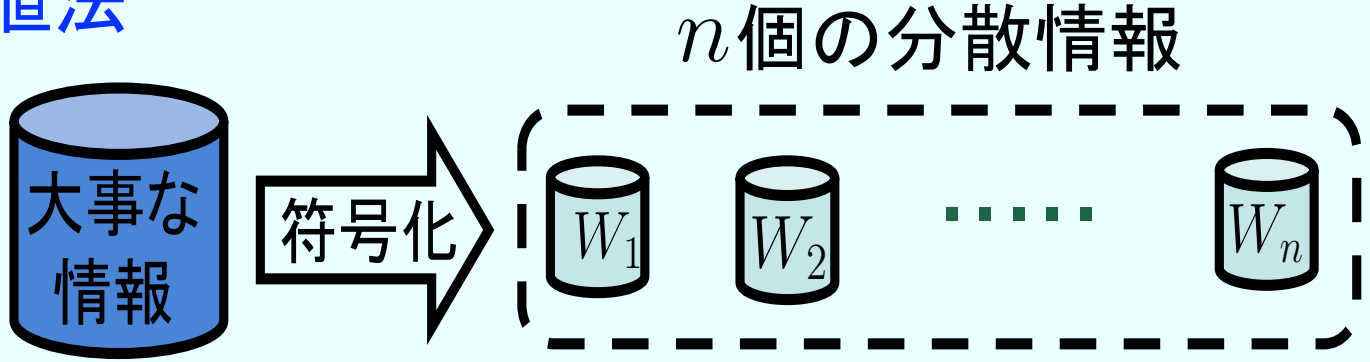
$(h, h-t, n)$ しきい値法

$(0 \leq b \leq h - t)$

$$H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-t-b}} | W_{i_1}, W_{i_2}, \cdots, W_{i_{t+b}}) = H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-t-b}})$$

一般アクセス構造

しきい値法



全ての分散情報は対等

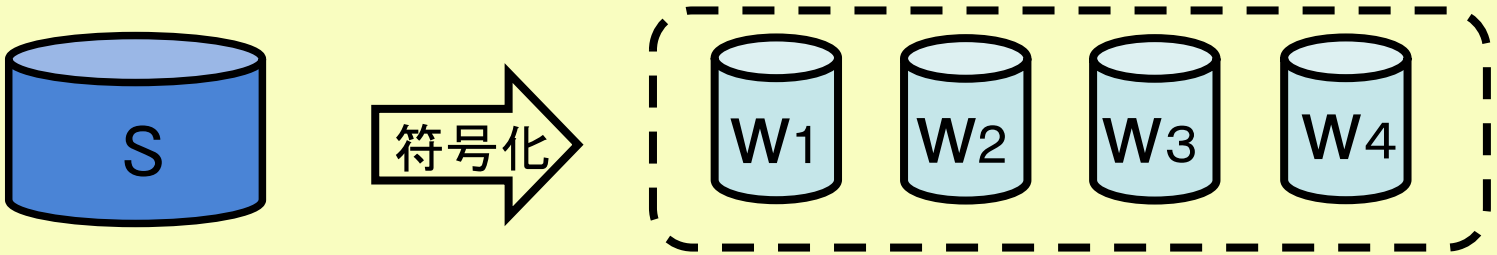
一般アクセス構造

分散情報の復号権限が対等でない

有資格集合：秘密情報を復号可能な分散情報の集合

禁止集合：秘密情報を復号できない分散情報の集合

一般アクセス構造の(n,n)しきい値法を用いた実現法



極小有資格集合族:

$$\Gamma = [\{w_1, w_2, w_3\}, \{w_1, w_4\}, \{w_2, w_4\}, \{w_3, w_4\}]$$

極大禁止集合族:

$$\overline{\Gamma} = [\{w_1, w_2\}, \{w_2, w_3\}, \{w_1, w_3\}, \{w_4\}]$$

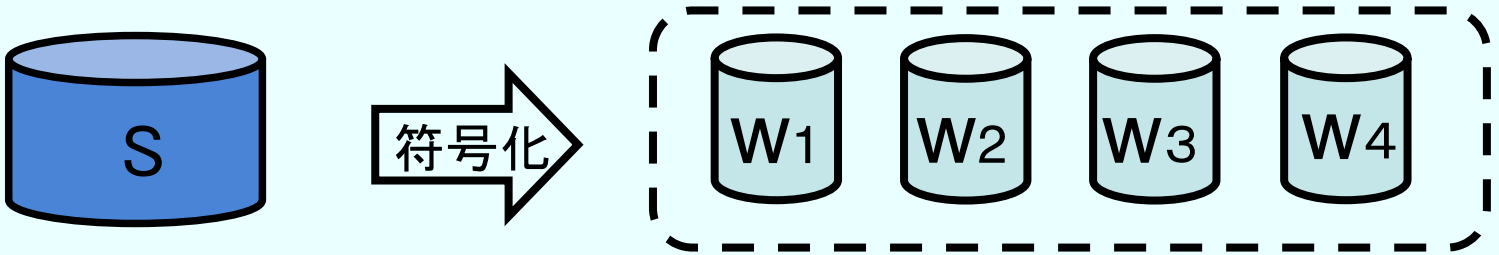
$S \Longrightarrow \quad v_1 \qquad v_2 \qquad v_3 \qquad v_4$

(4,4)しきい値法

$$w_1 : (v_2, v_4) \qquad w_3 : (v_1, v_4)$$

$$w_2 : (v_3, v_4) \qquad w_4 : (v_1, v_2, v_3)$$

一般アクセス構造の(n,n)しきい値法を用いた実現法



極小有資格集合族:

$$\Gamma = [\{w_1, w_2, w_3\}, \{w_1, w_4\}, \{w_2, w_4\}, \{w_3, w_4\}]$$

極大禁止集合族:

$$\overline{\Gamma} = [\{w_1, w_2\}, \{w_2, w_3\}, \{w_1, w_3\}, \{w_4\}]$$

効率のよい実現法

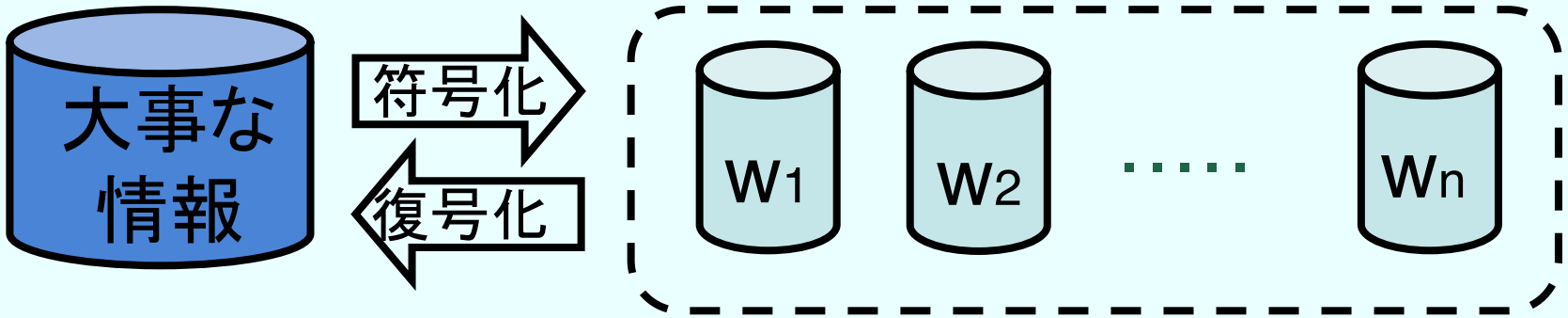
(k, n) しきい値法を利用

(Tochikubo-Uyematsu-Matsumoto, 2005)

整数計画法を利用(Iwamoto-Yamamoto-Ogawa, 2007)

視覚復号型秘密分散法(Visual Secret Sharing Scheme)

一般的な秘密分散法(計算機上で実現)

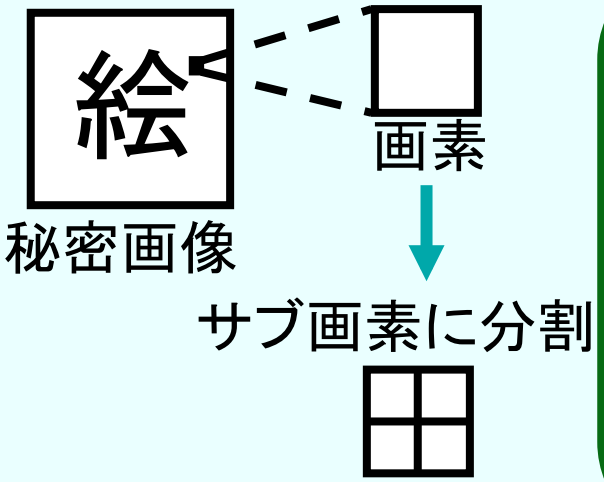


非常時(災害，テロ):電気や計算機が使えない

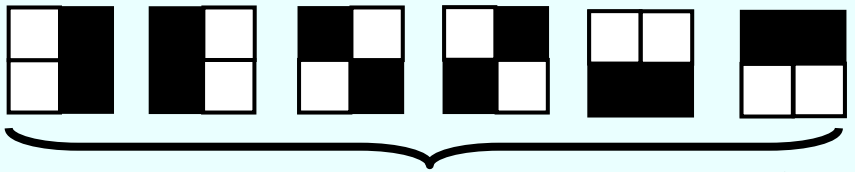
ビジュアル秘密分散法(視覚を使った暗号)

計算機がなくても，人間の視覚を使って秘密情報が復号できる

VSSS(白黒2値画像)（Naor-Shamir, 1994）



分散画像1の画素の作り方



6種類の画素を画面全体にランダムに配置

分散画像2の画素の作り方

白の画素：分散画像1の画素と同じ画素を使う

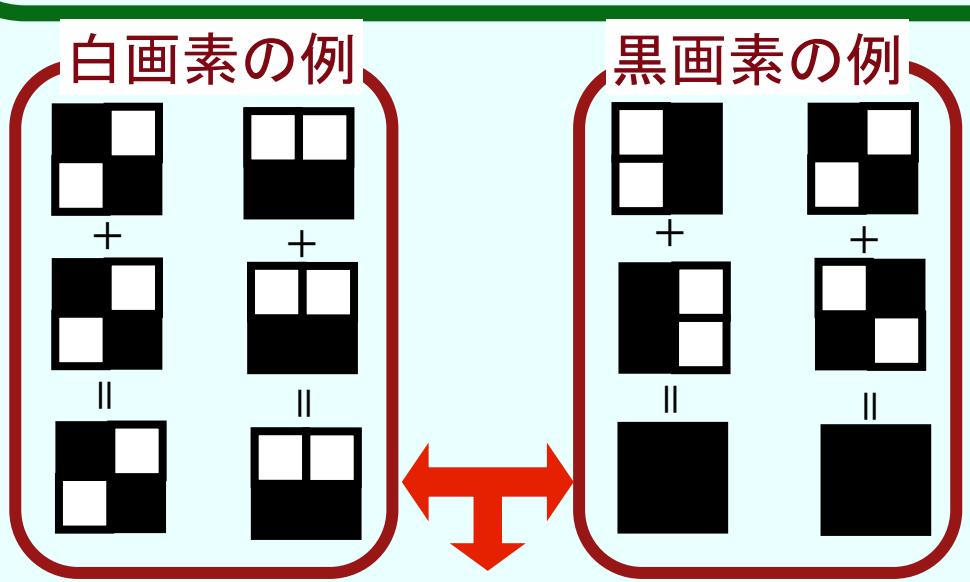
黒の画素：分散画像1の画素を反転した画素を使う

復号画素の例

分散画像1の画素→

分散画像2の画素→

重ねた画像の画素→

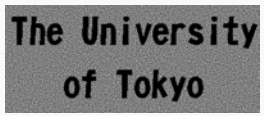


明暗の差で区別できる

(2,2)しきい値法の一般化

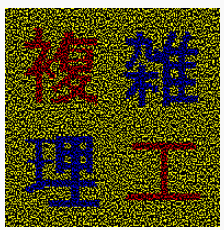
分散画像が3枚以上の場合 ➡ 数理的手法による構成法が必要
カラー・濃淡画像の場合

復号画像の例



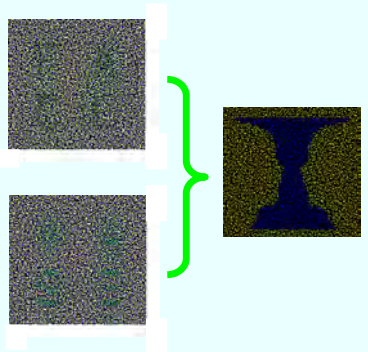
2値画像


濃淡画像

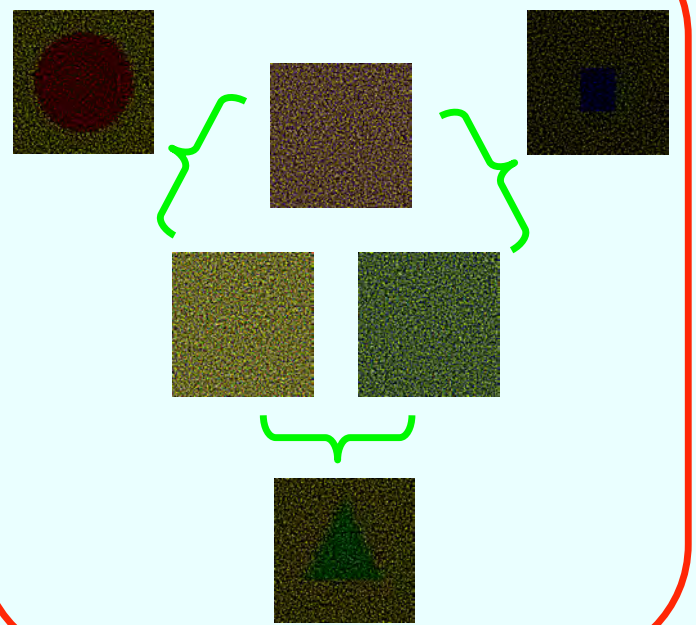


カラー画像

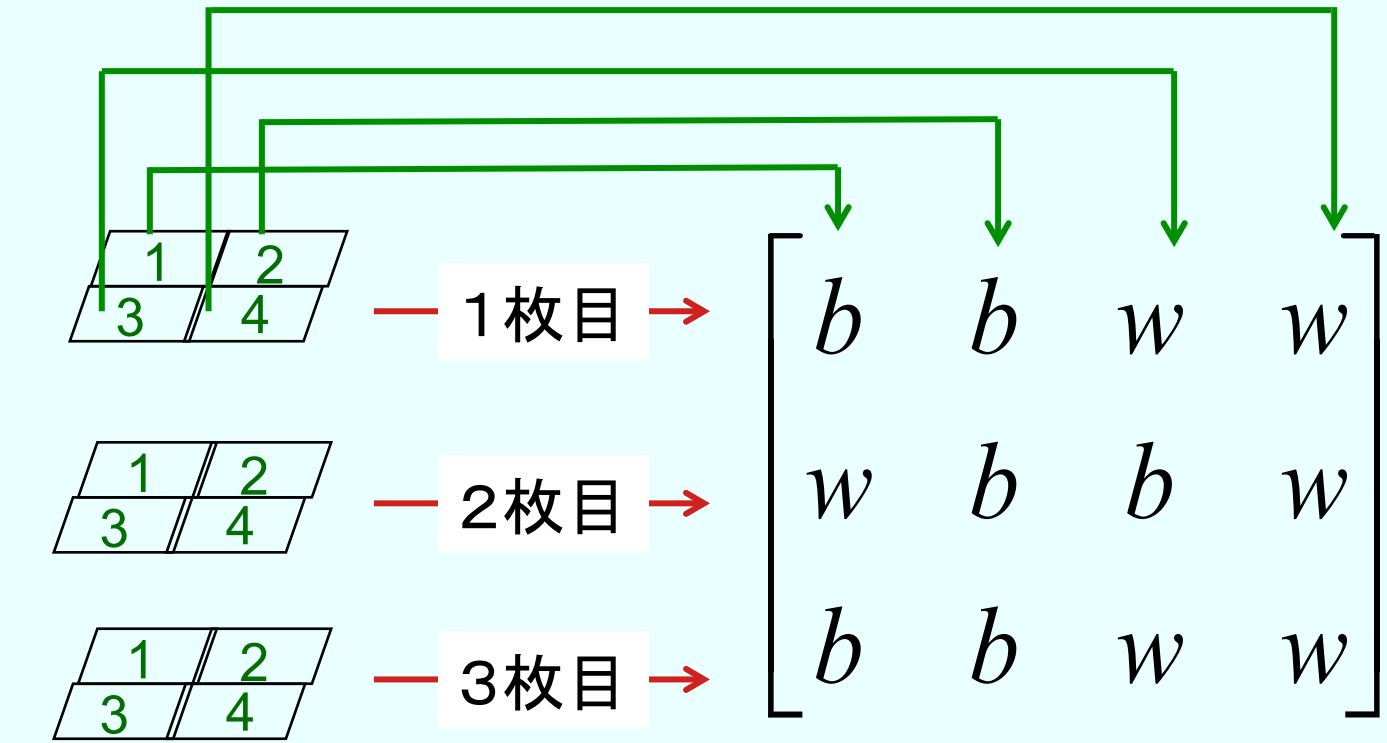
各分散画像に情報を書いた例



分散画像の組合せで秘密画像が異なる例



一般化のための数学的手法



一般化のための数学的手法

等重み行列の単項式表現

$$\begin{bmatrix} b & b & w \\ b & w & b \\ w & b & b \end{bmatrix} \quad \begin{bmatrix} b & w & w \\ w & b & w \\ w & w & b \end{bmatrix} \quad \begin{bmatrix} b \\ b \\ b \end{bmatrix}$$

$$\frac{wb^2}{2!} \qquad \frac{w^2b}{2!} \qquad \frac{b^3}{3!}$$

$$\left(\frac{wb^2}{1!\cdot 2!}\right) \qquad \left(\frac{w^2b}{2!\cdot 1!}\right) \qquad \left(\frac{w^0b^3}{0!\cdot 3!}\right)$$

$$\begin{cases} n! = n\times(n-1)\times\cdots\times 2\times 1 \\ 0! = 1 \end{cases}$$

等重み行列の接合と単項式の和表現

$$\left[\begin{array}{ccc:ccc:c} b & b & w & b & w & w & b \\ b & w & b & w & b & w & b \\ w & b & b & w & w & b & b \end{array}\right]$$

$$\frac{wb^2}{2!} + \frac{w^2b}{2!} + \frac{b^3}{3!}$$

一般化のための数学的手法

等重み行列の単項式表現

(Koga-Iwamoto-Yamamoto, 2001)

白画素

$$\begin{bmatrix} b & b & w & w \\ b & w & b & w \\ w & b & b & w \end{bmatrix}$$

1枚除く

$$\begin{bmatrix} b & b & w & w \\ b & w & b & w \end{bmatrix}$$

$$\frac{wb^2}{2!}+\frac{w^3}{3!} \xrightarrow{\left(\frac{\partial}{\partial w}+\frac{\partial}{\partial b}\right)} \frac{b^2}{2!}+wb+\frac{w^2}{2!}$$

黒画素

$$\begin{bmatrix} b & w & w & b \\ w & b & w & b \\ w & w & b & b \end{bmatrix}$$

1枚除く

$$\begin{bmatrix} b & w & w & b \\ w & b & w & b \end{bmatrix}$$

$$\frac{w^2b}{2!}+\frac{b^3}{3!} \xrightarrow{\left(\frac{\partial}{\partial w}+\frac{\partial}{\partial b}\right)} wb+\frac{w^2}{2!}+\frac{b^2}{2!}$$

同じ

↓

区別が付かない

秘密分散法のその他の話題

- 復号の高速化

  XOR演算のみ利用

  （Kurihara-Kiyomoto-Fukushima-Tanaka, 2007）

- 量子秘密分散法

  量子状態の秘密分散法

  （Ogawa-Sakai-Iwamoto-Yamamoto, 2005）