秘密情報の符号化

山本博資

東京大学

明治大学　中央大学

講演を始める前に

SITA特別講演の歴史

を振り返ってみよう

1978(神戸): 特別講演無し

1979(京都): 特別講演無し

1980(箱根): 特別講演無し(夜のワークショップが始まる)

1981(賢島): (講演題目不明)
(R.R. Varshamov, Academy of Sciences of the Armenian SSR)

1982(八幡平): 特別講演無し

1983(松山): IEEE特別講演(詳細不明)

1984(鬼怒川):
素数と素因数分解 -暗号理論と関連して-(廣瀬健, 早稲田大学)
情報資源とその流通(平山博, 早稲田大学)
Coding on Multi-User Channels(Shu Lin, University of Hawaii)
(情報理論研究会のチュートリアルセッションが始まる)

1985(奈良):
計算幾何学(伊里正夫, 東京大学)
Combined Modulation/Coding System (Jack K. Wolf, Univ. of California)
Cascade Coding Schemes for Error Control in Satellite and Space Communications (Shu Lin, University of Hawaii)

1986(赤倉):
情報幾何学(甘利俊一, 東京大学)
情報理論の思い出(喜安善市, 東北大学)
ブラックホールプロセッサ構成論 -知的謀反のすすめ-(川上正光)

1987(江ノ島): Contextual Information Processing in Japanese Dialogue System(安西祐一郎, 北海道大学)

1988(別府): マシーンインテリジェンスと情報理論(有本卓, 東京大学)

1989(犬山): 情報理論研究の歩みと将来(本多波雄, 豊橋技術科学大学)
(講演題目不明)(I. Csiszár, Hangarian Academy of Sciences)
大脳の神経情報処理(久保田競, 京都大学霊長類研究所)

1990 (1991年1月) (蓼科):
ホワイトノイズ(飛田武幸, 名古屋大学)
(Thomas Ericsson, Linköpings Univ.) ←中止(湾岸戦争, リトアニア情勢)

(ISITAが始まる)

1991(指宿): 海洋と気候(前田明夫, 鹿児島大学)
Performance Limits of Code Division Multiple Access
(Sergio Verdu, Princeton University)

1992(水上):
広帯域ネットワークの展開 – VI&Pサービスの実現を目指して–
(三木哲也, NTT伝送システム研究所長)
Asymptotic Expansions in Signal Detection
(Marat Burnashev, Inst. for Problems of Information Transmission)

1993(金沢):
Approximation theory of output statistics (韓太舜, 電気通信大学)
神経網膜における情報処理機構(加藤聖, 金沢大学)
Online algorithms (Manus Halldorosson, 北陸先端大学院大学)

1994(広島): 角筆文献と情報提供(位藤邦生, 広島大学)
マルチメディアにおけるCGの役割(中前栄八郎, 広島県立大学)

1995(花巻): 宮澤賢治とエコロジー思想(吉見正信, 文芸評論家)
インターネット – 技術の現状と将来展望– (村井純, 慶應大学)

1996(箱根): 情報と制御の数理科学的側面 (有本卓, 東京大学)

1997(松山):
Some New Signal Processing Ideas for Present and Future Magnetic Recoding (Desmond J. Mapps, Univ.of Plymouth)
四国は死国にされた (大杉博, 倭国研究所)
SITA20年を振り返って (堀内和夫, 早稲田大学)

1998(岐阜): (3件, 詳細不明)

1999(湯沢): モデル海底熱水噴出環境でのオリゴペプリド生成
(松野孝一郎, 長岡技術科学大学)

2000(阿蘇): 符号理論研究における挿話(嵩忠雄, 広島市立大学)

2001(神戸): 電子社会と情報セキュリティ(辻井重男, 中央大学)

2002(伊香保): 温泉を科学する(久保田一雄, 群馬温泉医学研究所)

2003(淡路): 最近のコンピュータ・ウィルスの動向について
(星沢裕二, 株式会社シマンテック)

2004(下呂): 2005年国際博覧会とIT
(川瀬洋一, 財団法人2005年日本国際博覧会協会調査役)

2005(沖縄): 八重山民謡に見るスローライフ(山里純一, 琉球大学)

2006(函館): 日本の開国と箱館(紺野哲也, 函館市史編さん室参事)

2007(賢島): 1977年に何が望まれたか, そして2007年の今何が望まれているか - 我が国のコミュニケーション技術の将来を考える
(笠原正雄, 大阪学院大学教授)

2008(鬼怒川): 学会活動雑 - 学会化の頃のお話と私の最近の研究テーマ
(平澤茂一, 早稲田大学)

2009(山口湯田): 山口の歴史と風土(福山百合子, 中原中也記念館前館長)

2010(信州松代): パワースポット　善光寺(福島貴和, 善光寺玄証住職)

2011(鶯宿): 宮澤賢治 -「いのち」への思い
(佐々木民夫, 岩手県立大学副学長)

2012(大分):(特別講演無し)

2013(伊東): 過去と現代を対比し巨大地震を克災する
(福和伸夫, 名古屋大学減災連携研究センター長)

2014(富山宇奈月):基調講演
MDL原理入門(竹内純一, 九州大学)
情報スペクトル理論の記憶のある情報通信システムへの展開
(大濱靖匡, 電気通信大学)

2015(倉敷):「文化の力」を考える - 大原美術館の85年 -
(大原謙一郎, 大原美術館理事長)

2016(高山): 忍者の修行と活動＆忍術の活用
(川上仁一, 甲賀流伴党21代宗家, 三重大学特任教授)

2017(新発田月岡): 脳内情報処理機構とその多様性, 脆弱性:ドラえもんは作れるか？(那波宏之, 新潟大学脳研究所所長)

最近の私の研究テーマ

準瞬時符号 (AIFV Code)
(Almost Instantaneous Fixed-to-Variable Code)

複数の符号木を使用
若干の復号遅延を許す

Huffman符号：
1個の符号木
ゼロ復号遅延

一意復号可能で，Huffman符号より短い平均符号長を達成可能

SITA2017 情報理論研究会（若手研究者のための講演会）
山本博資，準瞬時FV符号とその拡張符号，
電子通信学会技術報告，IT2017-54, pp.19-26, 2017

AEW10 (2017), Beyond iid in Information Theory (2017)

秘密情報の符号化

情報量的安全性に基づく符号化システム

Shannon暗号システム，秘密分散通信システム，
秘密分散法，ネットワーク符号化，盗聴通信路符号化

不完全秘匿と情報の強安全な多重符号化

CMRR, UC San Diego

EECS, MIT

Shannonのドキュメンタリー映画

The Bit Player

監督，脚本：Mark Levinson

俳優：Claude Shannon: John Hutton
Betty Shannon: Judith Ivey
The Interviewer: Kaliswa Brewster

配信：IMDb

予告編 (https://vimeo.com/288625027)

「Oral-History: Claude E. Shannon」を映画化したもの

1982年7月28日に行われたRobert PriceによるShannonのインタビュー

(https://ethw.org/Oral-History:Claude_E._Shannon)

Shannonの暗号システム

C.E.Shannon,
"A Mathematical Theory of Communications"
B.S.T.J., vol.27, pp.379-423, 623-656, July and October 1948

C.E.Shannon,
"Communication Theory of Secrecy Systems"
B.S.T.J., vol.28, pp.656-715, October 1949

C.Shannon, "A Mathematical Theory of Cryptography,"
Technical Memoranda (Confidential), September 1, 1945

IACR Museum of Historic Papers in Cryptology
https://www.iacr.org/museum/index.html

IACR's Presentation of Shannon's 1945 A Mathematical Theory of Cryptograpny
https://www.iacr.org/museum/shannon45.html

Shannonの暗号システム

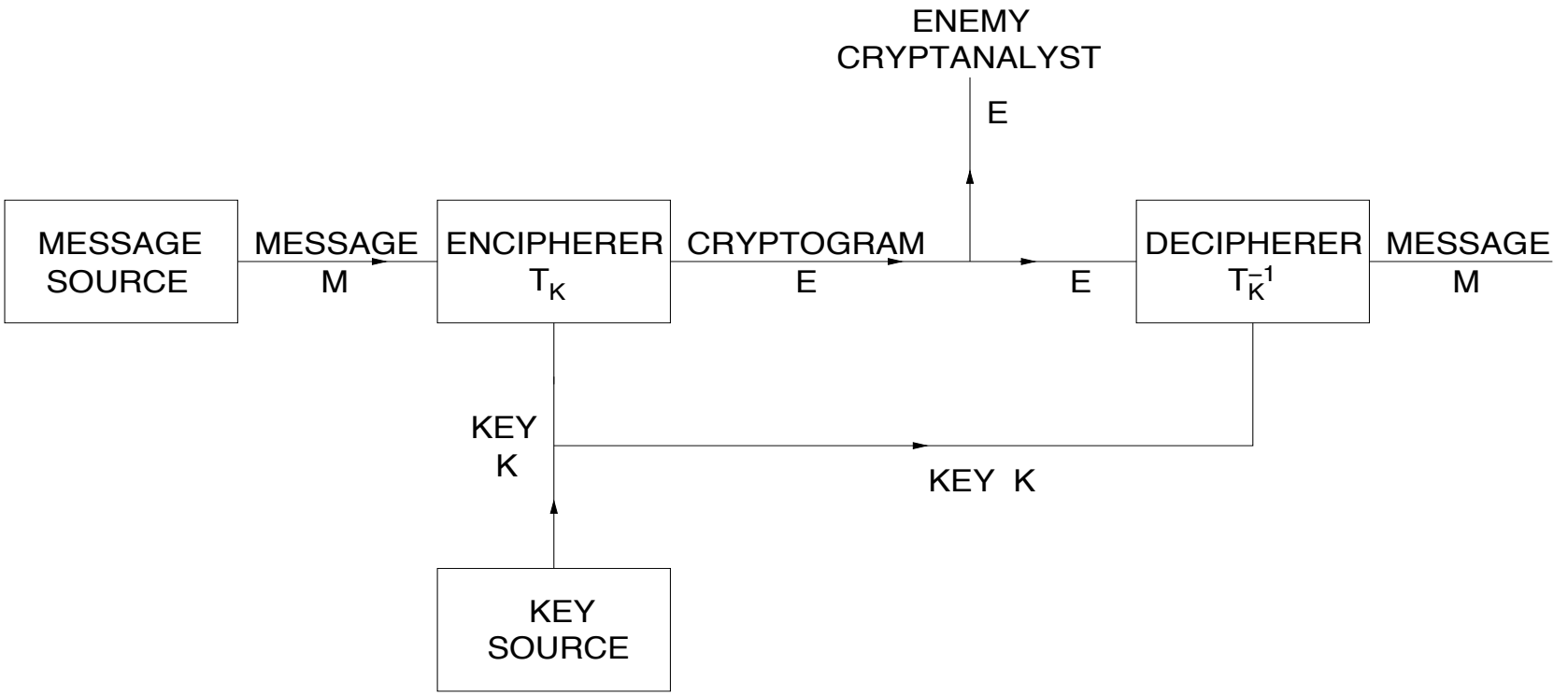
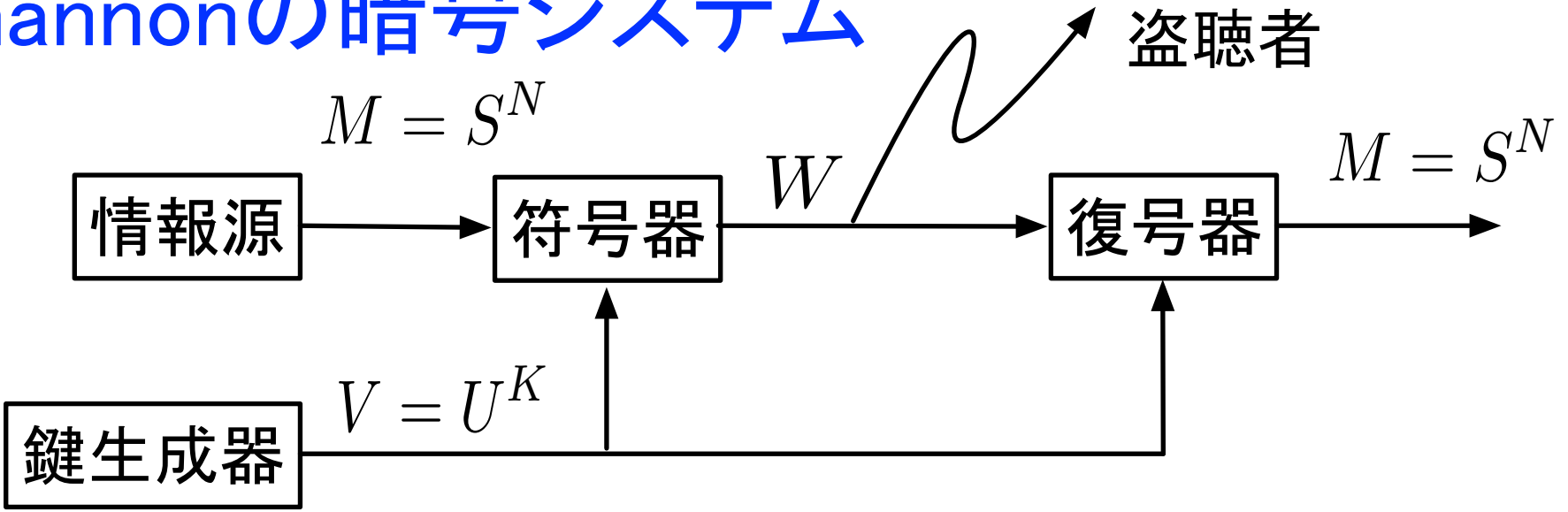


Fig. 1 Schematic of a general secrecy system

C.B.Shannon, “Communication Theory of Secrecy Systems”,
Bell Systems Technical Journal, vol.28, pp.656-715, October 1949
のFig.1に掲載されたシャノン暗号システム

Shannonの暗号システム



一様分布 $P(s) = \frac{1}{|\mathcal{S}|}, \quad P(U) = \frac{1}{|\mathcal{U}|}$

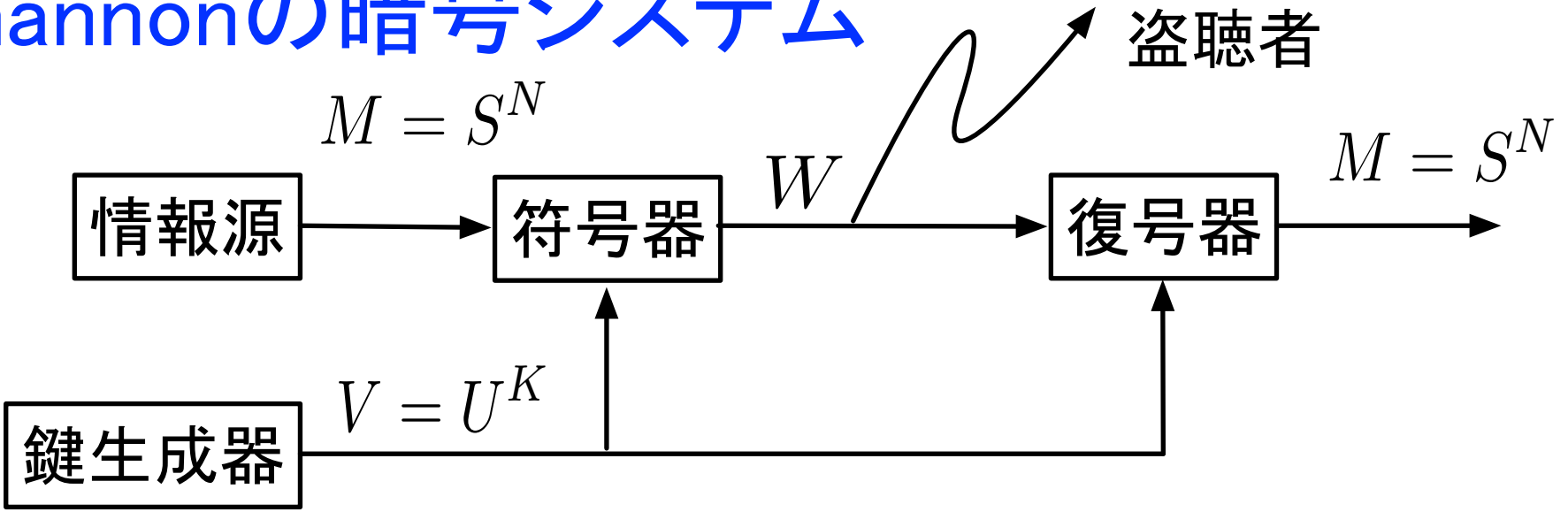
完全秘匿（Perfect Secrecy） $I(M;W) = 0$

$H(M|W) = H(M)$

$$H(V) \geq H(M)$$
$$KH(U) \geq NH(S)$$

$$\begin{aligned} H(V) &\geq H(V|W) = H(VM|W) = H(M|W) + H(V|MW) \\ &\geq H(M|W) = H(M) \end{aligned}$$

Shannonの暗号システム



一様分布 $P(s) = \frac{1}{|\mathcal{S}|}, \quad P(U) = \frac{1}{|\mathcal{U}|}$

完全秘匿(Perfect Secrecy) $I(M;W) = 0$

$H(M|W) = H(M)$

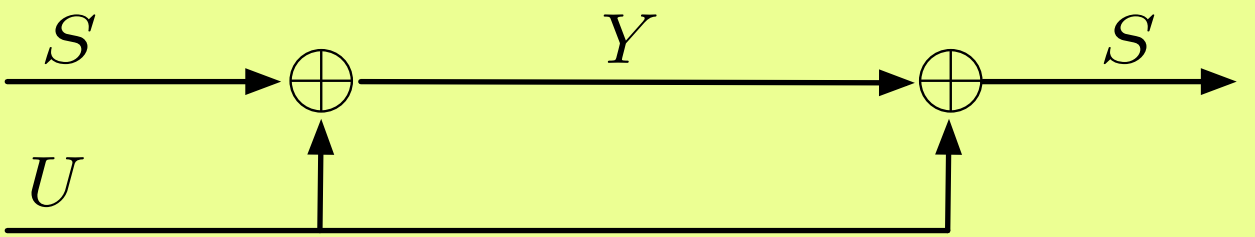
$\Rightarrow$ $H(V) \geq H(M)$

$KH(U) \geq NH(S)$

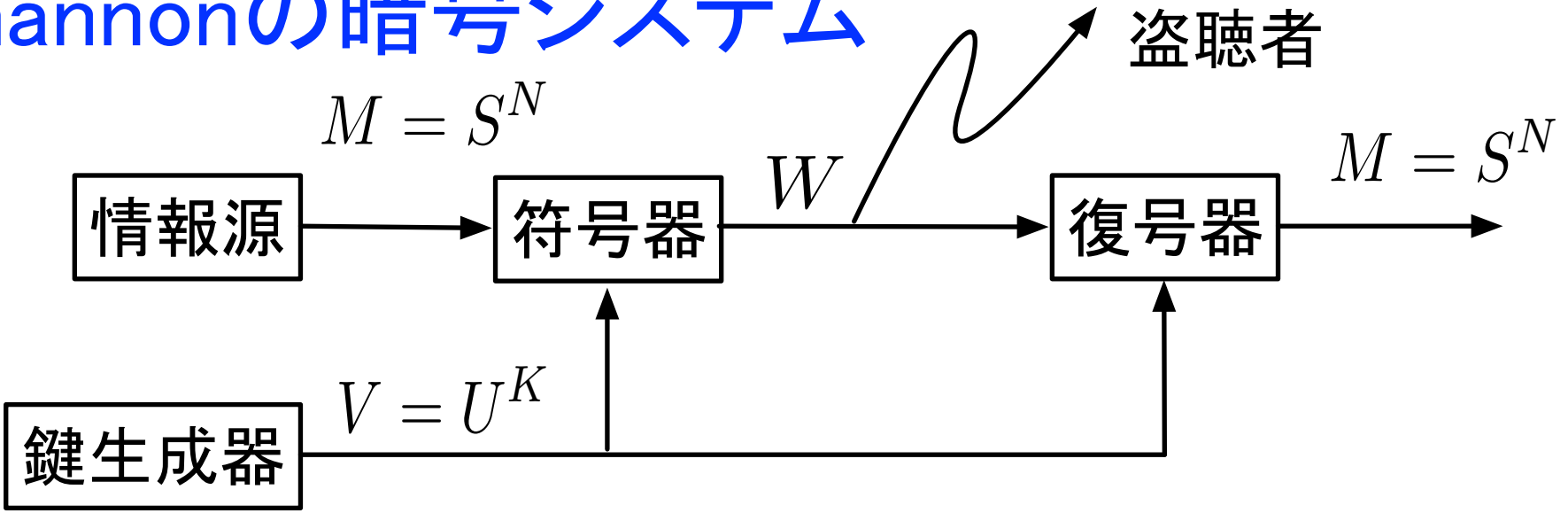
バーナム暗号(Vernam Cipher)

$\mathcal{S} = \mathcal{Y} = \mathcal{U} = \{0,1\}$

$N = K$



Shannonの暗号システム



一様分布 $P(s) = \dfrac{1}{|\mathcal{S}|}, \quad P(U) = \dfrac{1}{|\mathcal{U}|}$

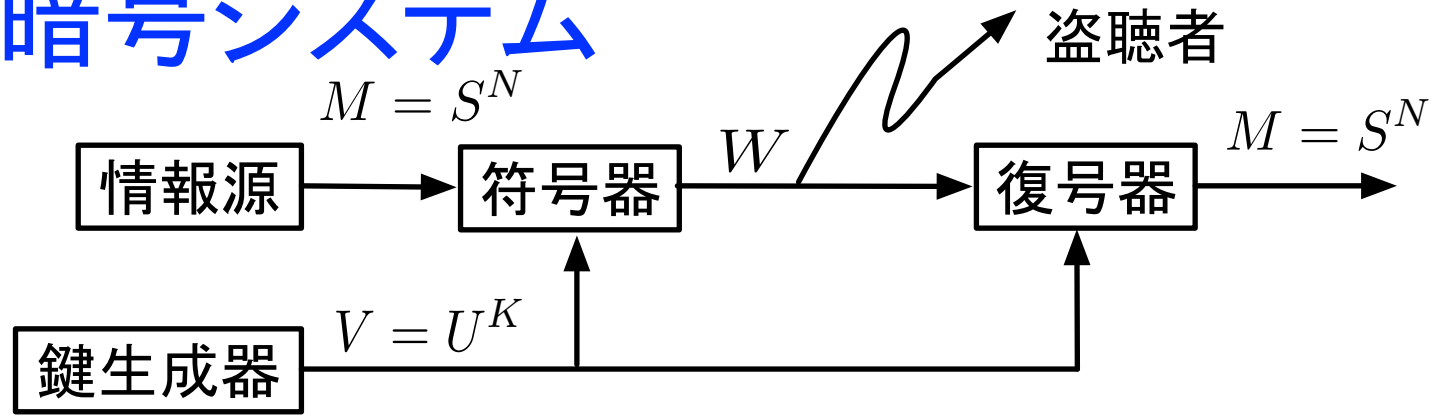
K : 固定, N が大きい場合

理想的(Ideal): $H(M|W) > 0, \quad H(V|W) > 0$

強理想的(Strongly Ideal): $H(V|W) = H(V)$ for any N

$$H(V|W) = H(VM|W) = H(M|W) + H(V|MW) \geq H(M|W)$$

Shannonの暗号システム



Random Cipher（Shannon 1949，Hellman 1977）

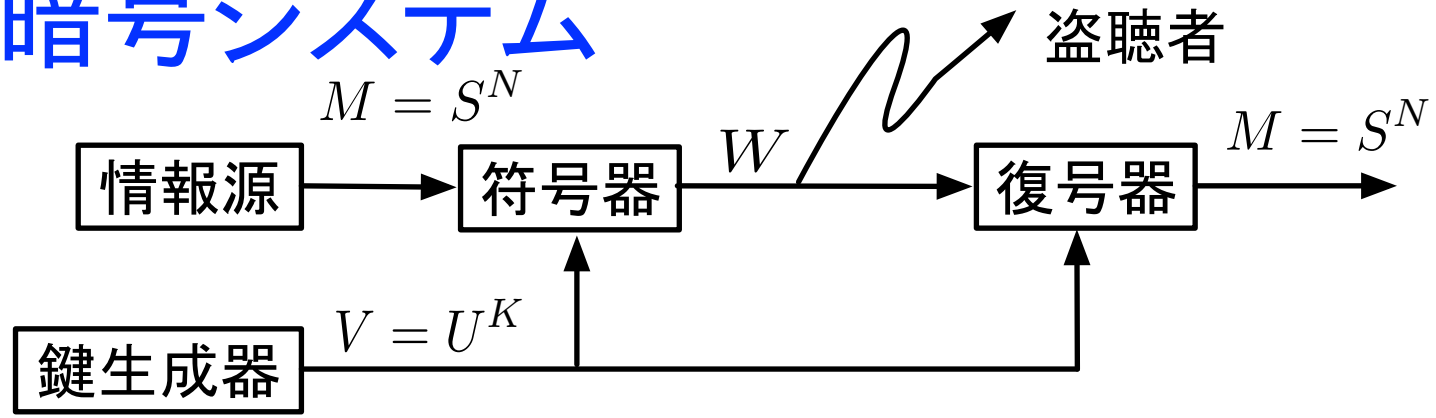
任意のシステム

$$
\begin{aligned}
H(V|W) &= H(VM|W) \\
&= H(VWM) - H(W) \\
&= H(V) + H(M|V) + H(W|MV) - H(W) \\
&= H(V) + H(M) - H(W) \\
&\geq H(V) + H(M) - \log|\mathcal{W}| \\
&= H(V) - N[\log|\mathcal{S}| - H(S)]
\end{aligned}
$$

$H(W) = \log|\mathcal{W}|$ のとき等号

$H(M) = NH(S)$
$\mathcal{W} = \mathcal{M} = \mathcal{S}^N$

Shannonの暗号システム



Random Cipher（Shannon 1949，Hellman 1977）

任意のシステム

$$H(V|W) = H(V) - N[\log|\mathcal{S}| - H(S)] > 0$$

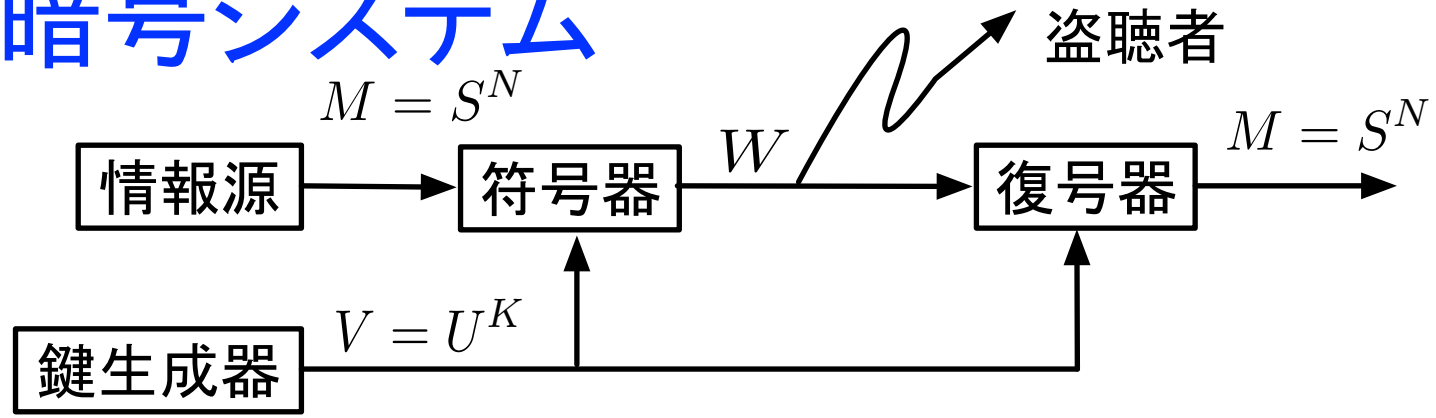
$$N < \frac{H(V)}{\log|\mathcal{S}| - H(S)}$$ ➡ 理想的(Ideal)

判別距離(Unicity Distance)

$H(S) = \log|\mathcal{S}|$ ➡ 強理想的（Strongly Ideal）

$H(S) < \log|\mathcal{S}|$ の場合はデータ圧縮が必要

Shannonの暗号システム



任意のシステム（Yamamoto, 1991）

$$\frac{H(M|W)}{N} = \frac{H(S^N|W)}{N} \geq h, \qquad 0 \leq h \leq H(S)$$

$$\begin{aligned} H(V) &\geq H(V|W) \\ &\geq H(V|W) - H(V|WM) \\ &= I(V;M|W) \\ &= H(M|W) - H(M|WV) \\ &= H(M|W) \\ &\geq Nh \end{aligned}$$

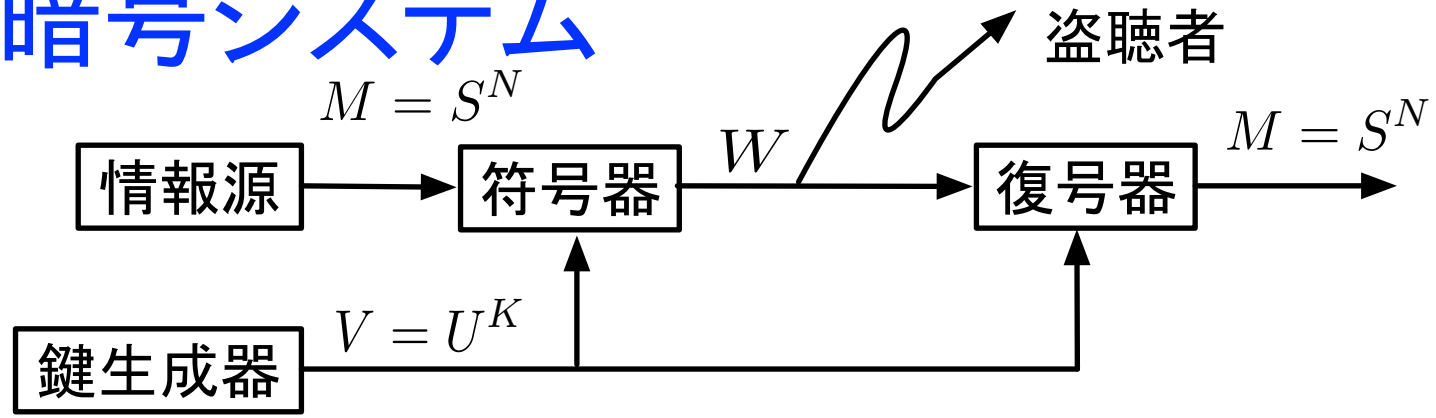
鍵レート

$$R_V = \frac{H(V)}{N} = \frac{KH(U)}{N} \geq h$$

暗号文レート

$$R_W = \frac{H(W)}{N} \geq H(S)$$

Shannonの暗号システム



任意のシステム（Yamamoto, 1991）

$$\frac{H(M|W)}{N} = \frac{H(S^N|W)}{N} \geq h, \qquad 0 \leq h \leq H(S)$$

問題点

情報 $M = S^N$ の一部が明確に漏洩する可能性がある

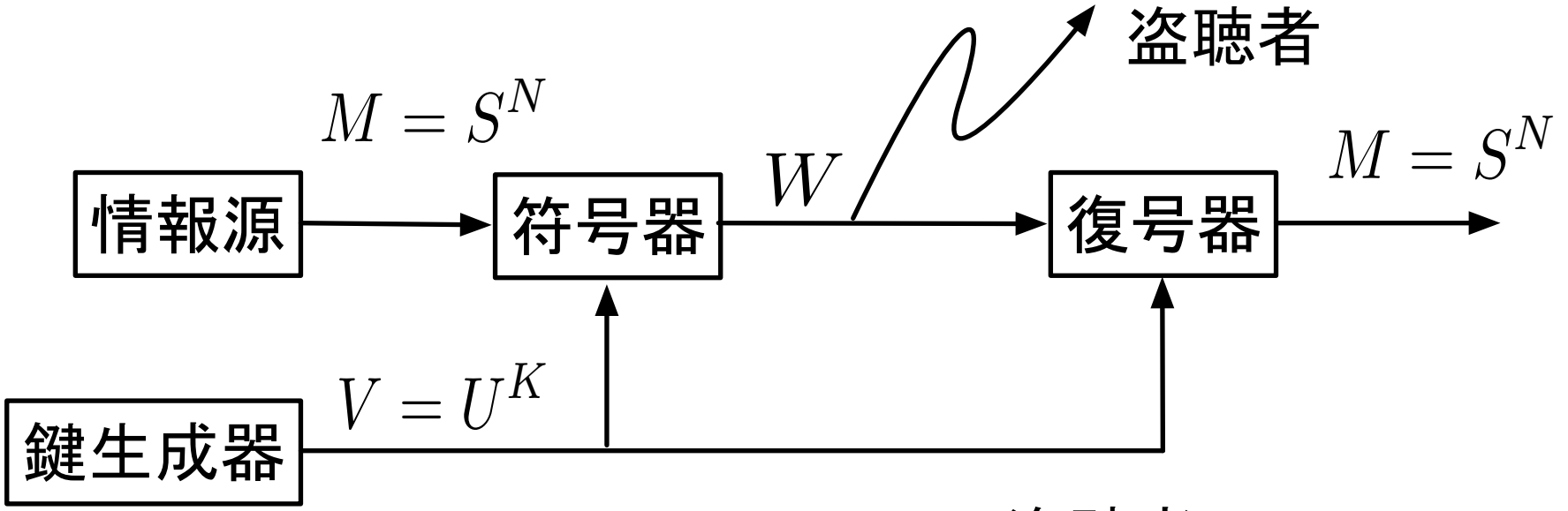
鍵レート

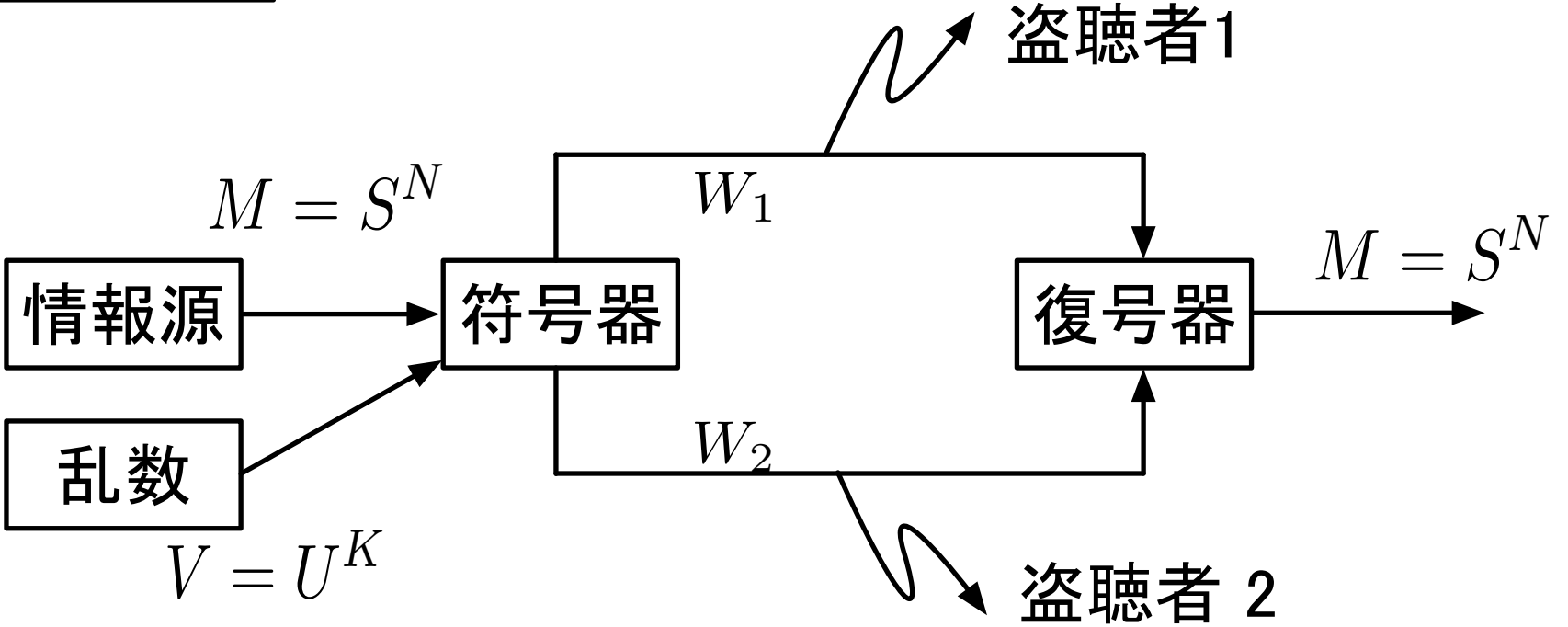
$$R_V = \frac{H(V)}{N} = \frac{KH(U)}{N} \geq h$$

暗号文レート

$$R_W = \frac{H(W)}{N} \geq H(S)$$

秘密分散通信システム(Yamamoto, 1986)

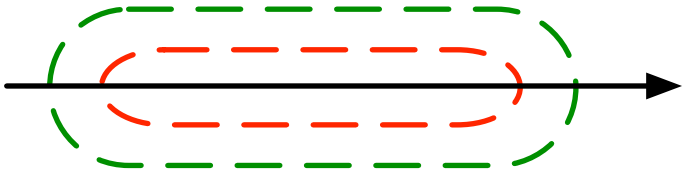




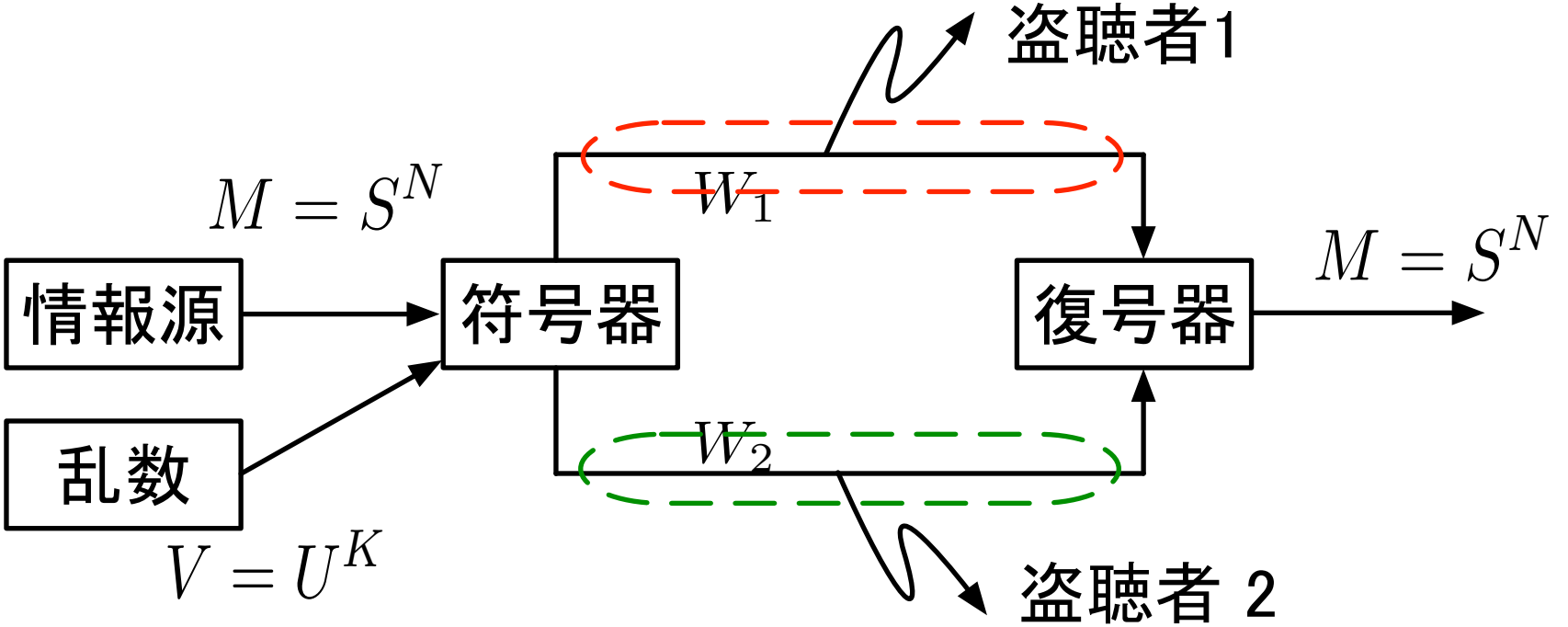
秘密分散通信システム(Yamamoto, 1986)

暗号1

暗号2

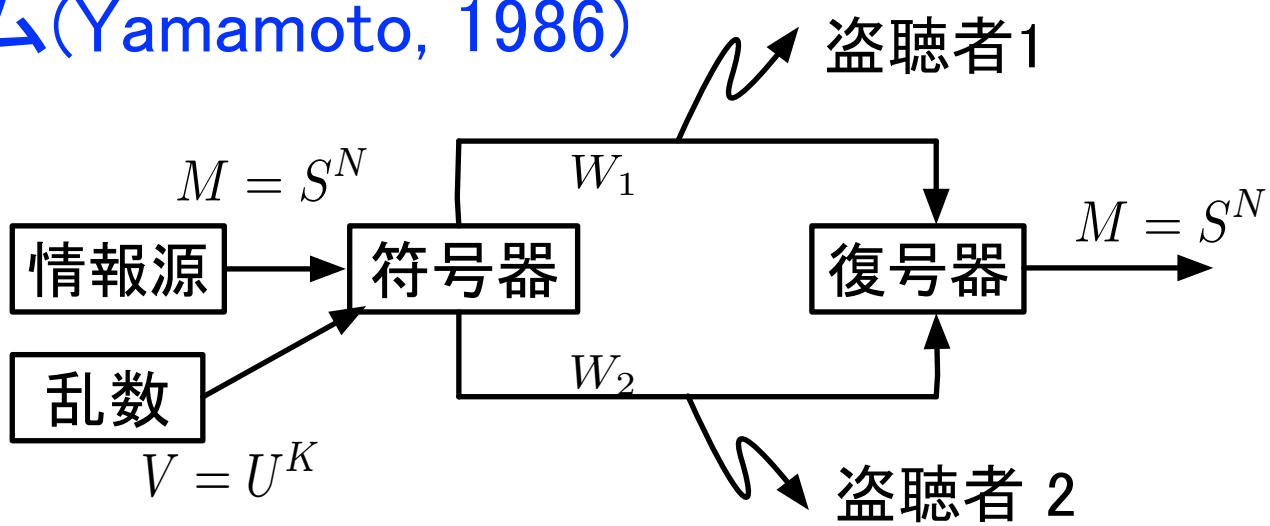


暗号1と2の縦続暗号化
暗号1，2より安全とは限らない



秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_1)}{N} = \frac{H(S^N|W_1)}{N} \geq h_1$$
$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$

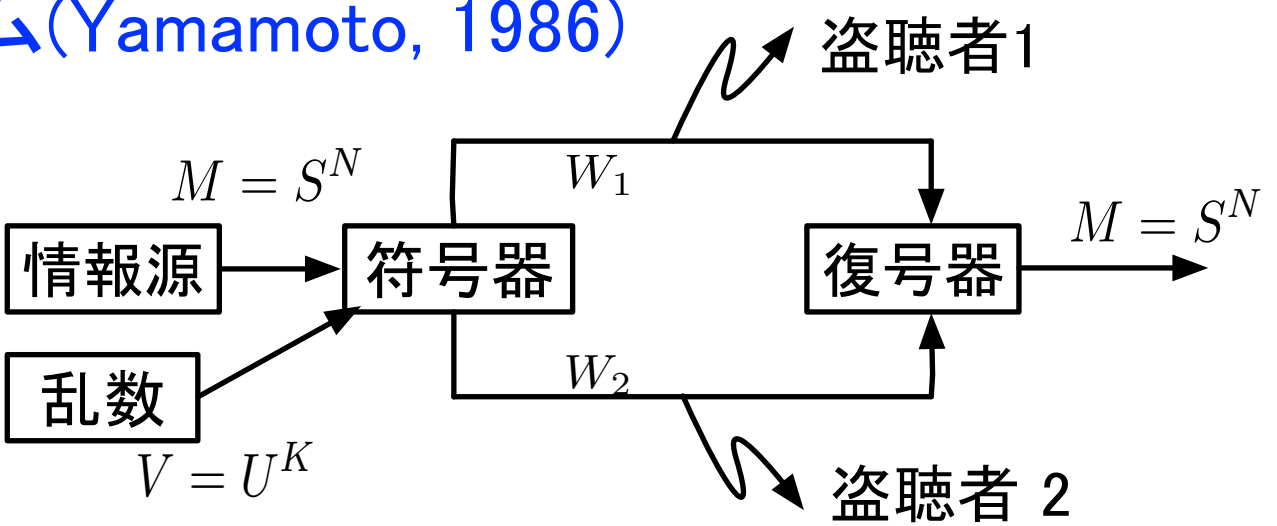


$$R_{W_1} = \frac{H(W_1)}{N} \geq \max\{h_2, H(S) - h_1\}$$
$$R_{W_2} = \frac{H(W_2)}{N} \geq \max\{h_1, H(S) - h_2\}$$
$$R_V = \frac{H(V)}{N} \geq \max\{h_1 + h_2 - H(S), 0\}$$

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$

$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$



$$R_{W_1} = \frac{H(W_1)}{N} \geq \max\{h_2, H(S) - h_1\}$$

$$R_{W_2} = \frac{H(W_2)}{N} \geq \max\{h_1, H(S) - h_2\}$$

$$R_V = \frac{H(V)}{N} \geq \max\{h_1 + h_2 - H(S), 0\}$$

$h_1 = h_2 = H(S)$ **完全秘匿**

$\Rightarrow R_{W_1} = R_{W_2} = R_V = H(S)$

$h_1 = h_2 = \frac{H(S)}{2}$ **不完全秘匿**

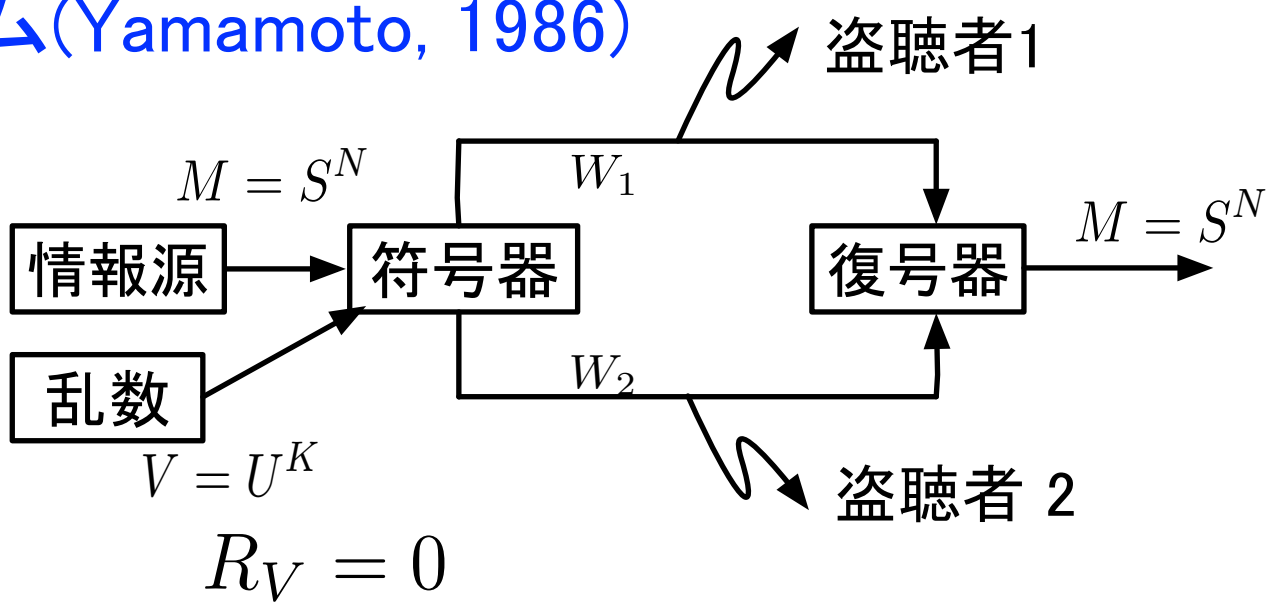
$\Rightarrow$

$$R_{W_1} = R_{W_2} = \frac{H(S)}{2}, R_V = 0$$

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$
$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$

$$h_1 = h_2 = \frac{H(S)}{2}$$



簡易な構成法

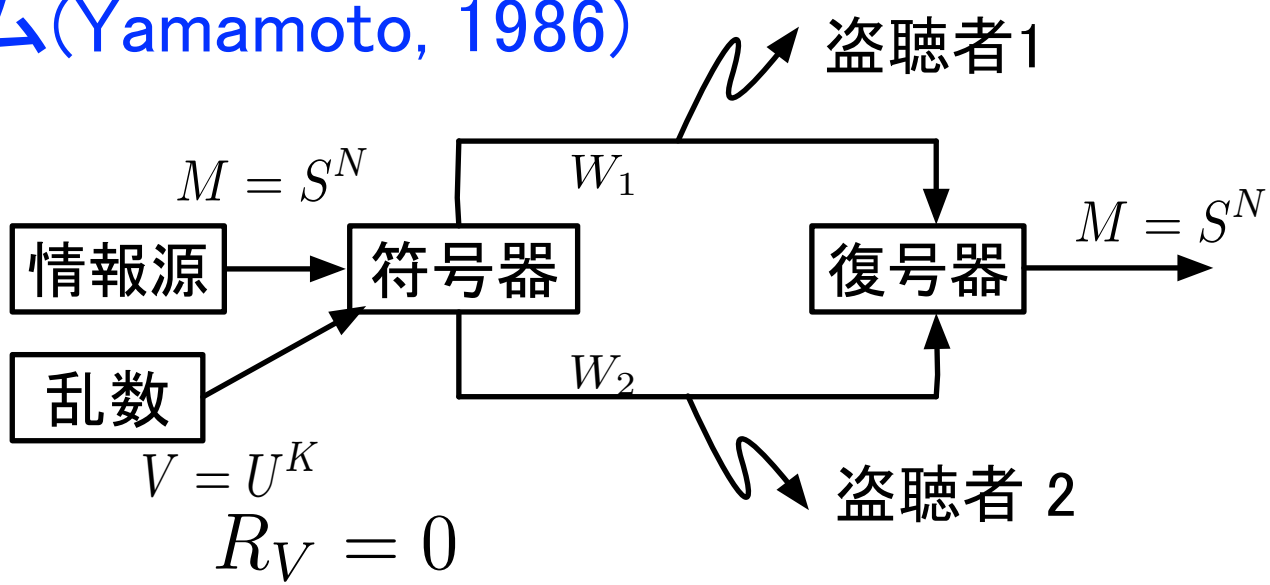
$$M = M_1 M_2 = S_1^{\frac{N}{2}} S_{\frac{N}{2}+1}^{N}$$
$$W_1 = M_1$$
$$W_2 = M_2$$

問題点

➡ 盗聴者 i に M_i が漏洩する.

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$
$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$



$$h_1 = h_2 = \frac{H(S)}{2}$$

不完全秘匿

安全な構成法

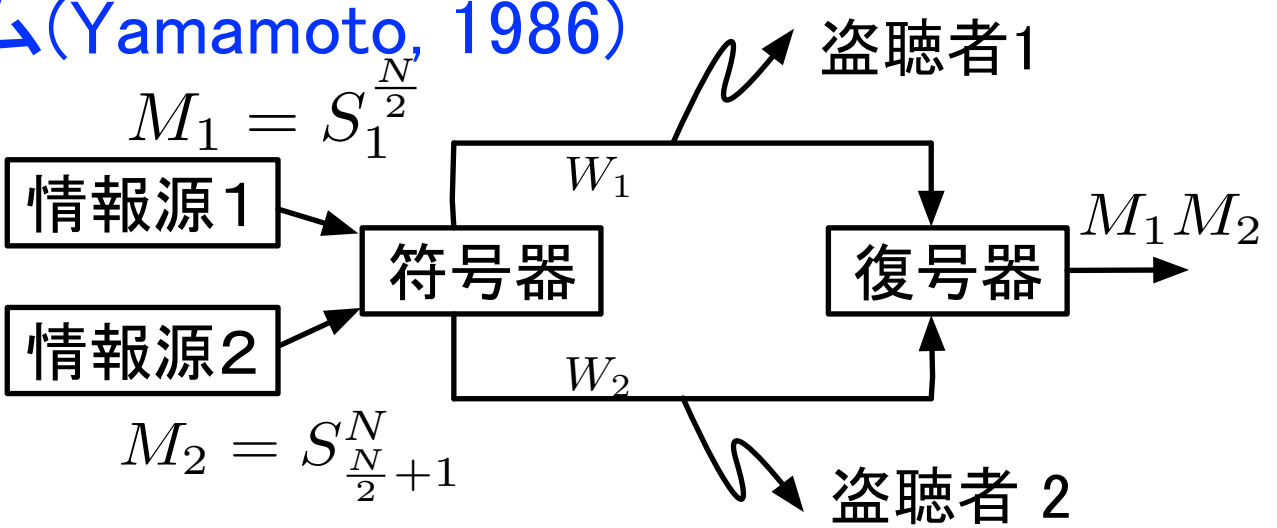
$$M = M_1 M_2 = S_1^{\frac{N}{2}} S_{\frac{N}{2}+1}^{N}$$
$$M_i \in \mathrm{GF}(q)$$
$$W_1 = M_1 + M_2$$
$$W_2 = M_1 + \alpha M_2$$
$$\alpha \neq 0, \quad \alpha \neq 1$$

$$\frac{H(M_i|W_j)}{N/2} = H(S), \qquad \begin{matrix} i = 1,2 \\ j = 1,2 \end{matrix}$$

M_1, M_2 に対する完全秘匿

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$
$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$



$$h_1 = h_2 = \frac{H(S)}{2}$$

不完全秘匿

強安全な秘密情報の多重符号化法

安全な構成法

$$M = M_1 M_2 = S_1^{\frac{N}{2}} S_{\frac{N}{2}+1}^{N}$$
$$M_i \in \mathrm{GF}(q)$$
$$W_1 = M_1 + M_2$$
$$W_2 = M_1 + \alpha M_2$$
$$\alpha \neq 0, \quad \alpha \neq 1$$

$$\frac{H(M_i|W_j)}{N/2} = H(S), \qquad \begin{matrix} i = 1,2 \\ j = 1,2 \end{matrix}$$

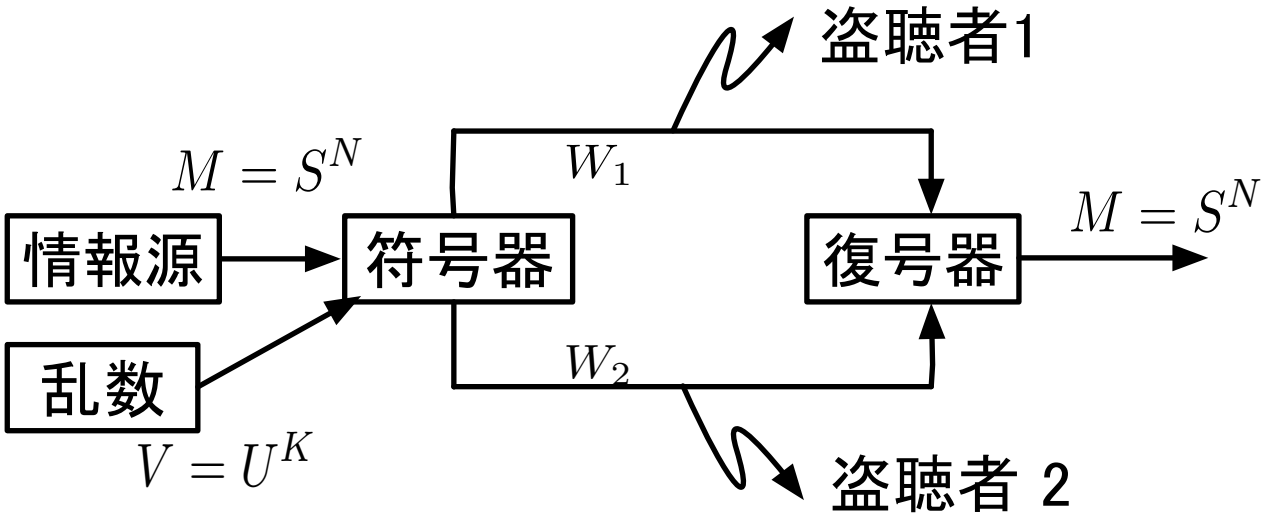
M_1, M_2 に対する完全秘匿

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$

$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$

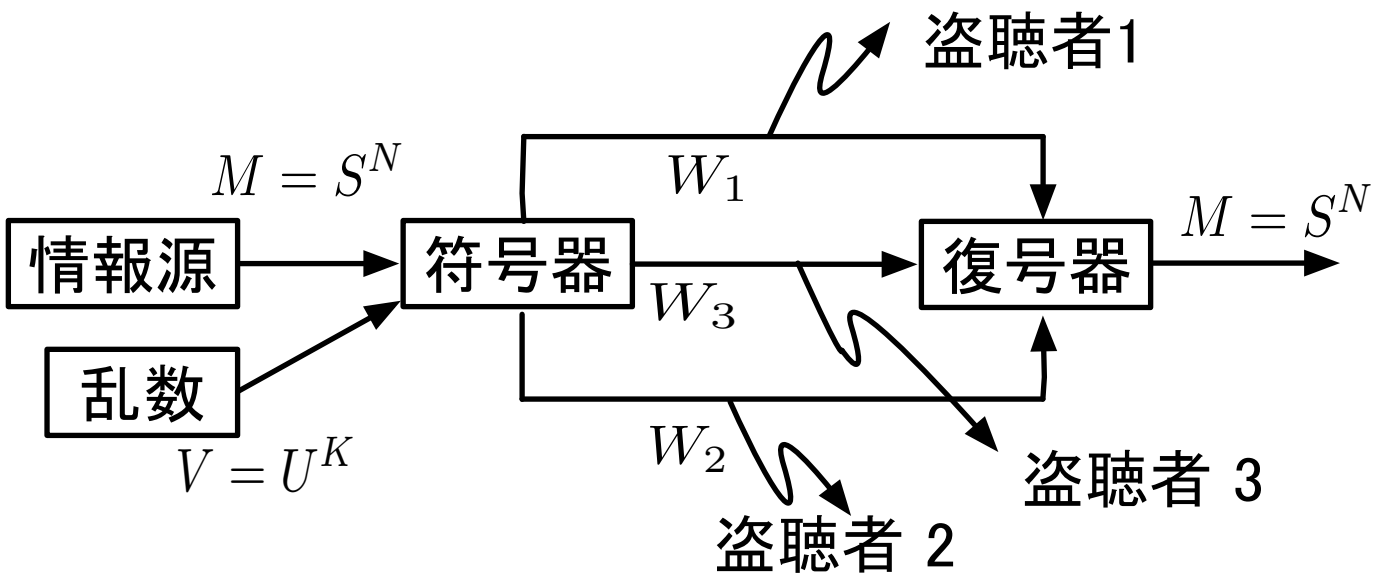
$$h_1 = h_2 = \frac{H(S)}{2}$$



強安全な秘密情報の
多重符号化法

他のh_1, h_2 の構成方法は？

秘密分散通信システム(Yamamoto, 1986)

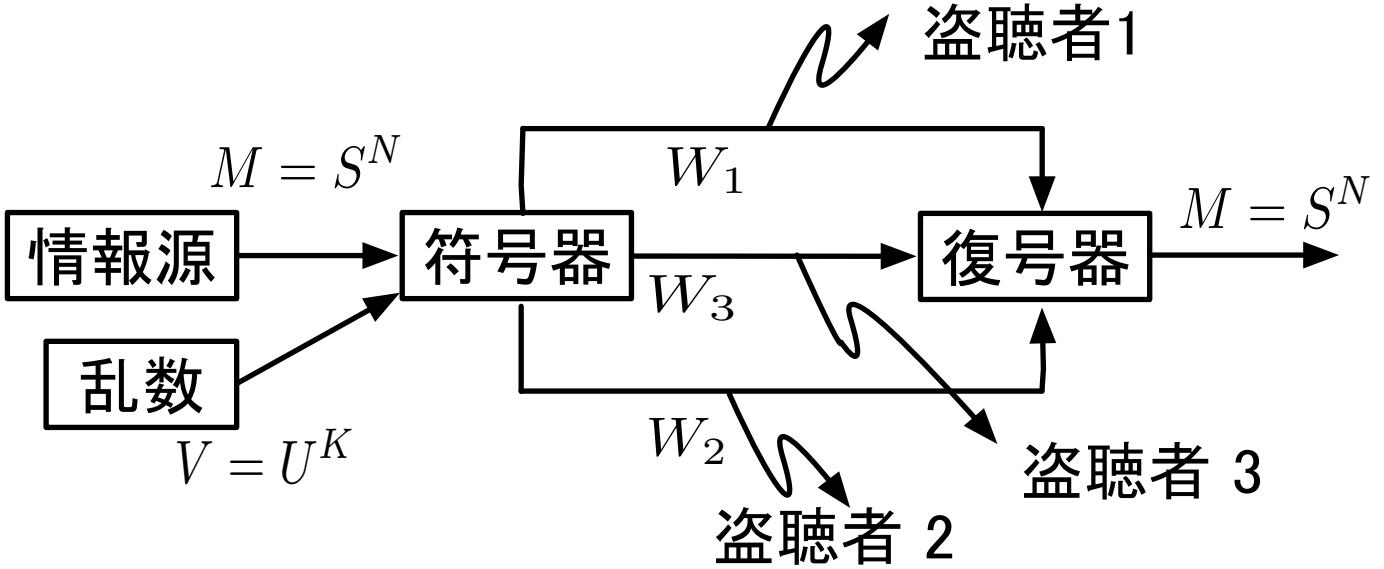


$$\frac{H(M|W_iW_j)}{N} = \frac{H(S^N|W_iW_j)}{N} \geq h_{ij}, \quad i \neq j$$

$$R_{W_i} = \frac{H(W_i)}{N} \geq \max\{h_{jk}, H(S) - h_{ij}, H(S) - h_{ik}\}, \quad i \neq j \neq k \neq i$$

$$R_V \geq \max\{h_{12} + h_{23} + h_{31} - H(S), 0\}$$

秘密分散通信システム(Yamamoto, 1986)



$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$

も考慮すると複雑

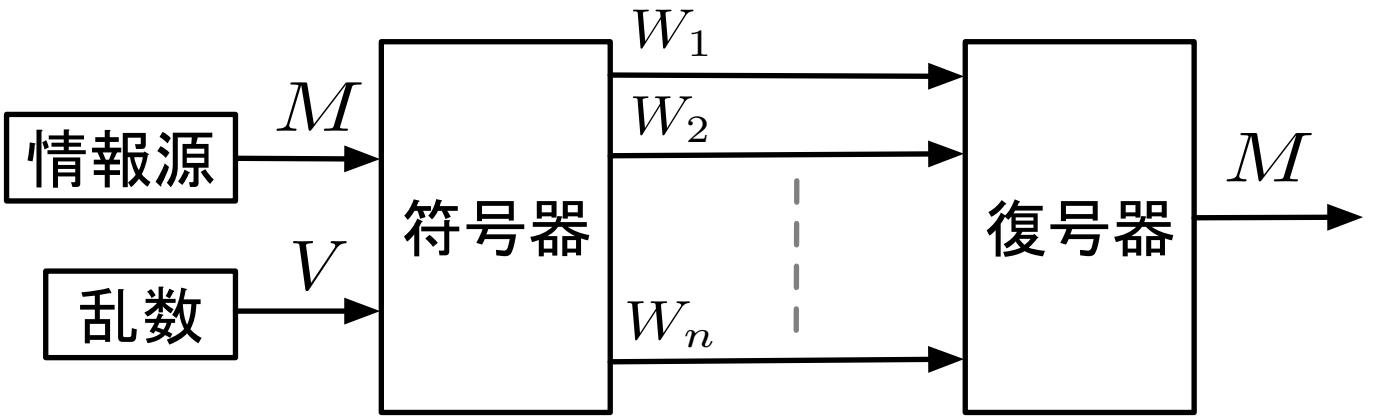
$$\frac{H(M|W_iW_j)}{N} = \frac{H(S^N|W_iW_j)}{N} \geq h_{ij}, \quad i \neq j$$

$$R_{W_i} = \frac{H(W_i)}{N} \geq \max\{h_{jk}, H(S) - h_{ij}, H(S) - h_{ik}\}, \quad i \neq j \neq k \neq i$$

$$R_V \geq \max\{h_{12} + h_{23} + h_{31} - H(S), 0\}$$

秘密分散法(Secret Sharing Scheme)

n通信路



$$H(M|W_{i_1}W_{i_2}\cdots W_{i_l}) \geq h_{i_1 i_2 \cdots i_l}$$

任意の$h_{i_1 i_2 \cdots i_l}$を取り扱うのは困難

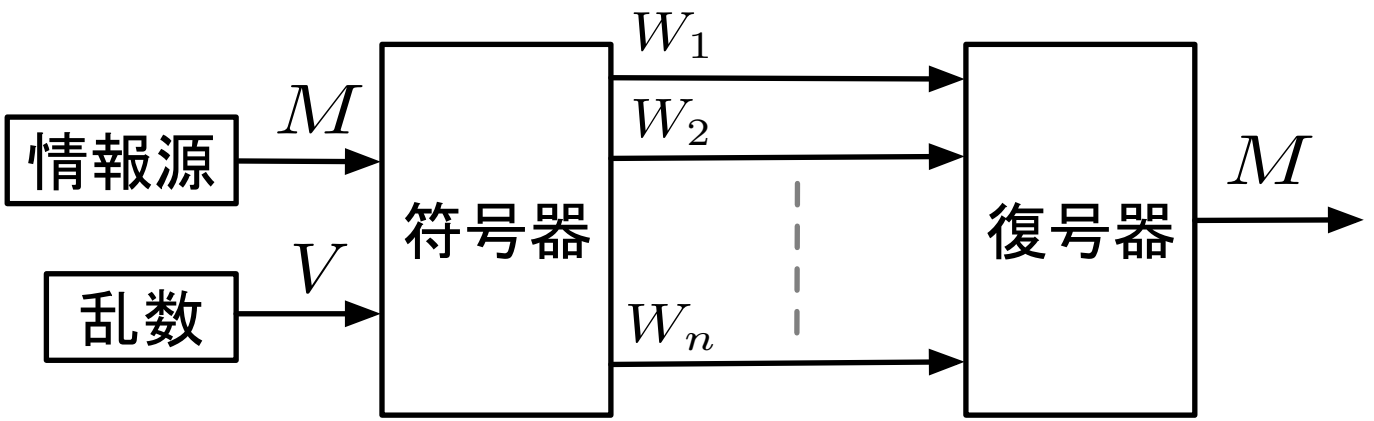
$h_{i_1 i_2 \cdots i_l}$：l にのみ依存 ➡ しきい値法

$h_{i_1 i_2 \cdots i_l}$：$0, H(M)$のみ ➡ 完全な秘密分散法

$0, \frac{1}{L}H(M), \frac{2}{L}H(M), \cdots, \frac{L-1}{L}H(M), H(M)$ のみ

➡ ランプ型秘密分散法

秘密分散法(Secret Sharing Scheme)



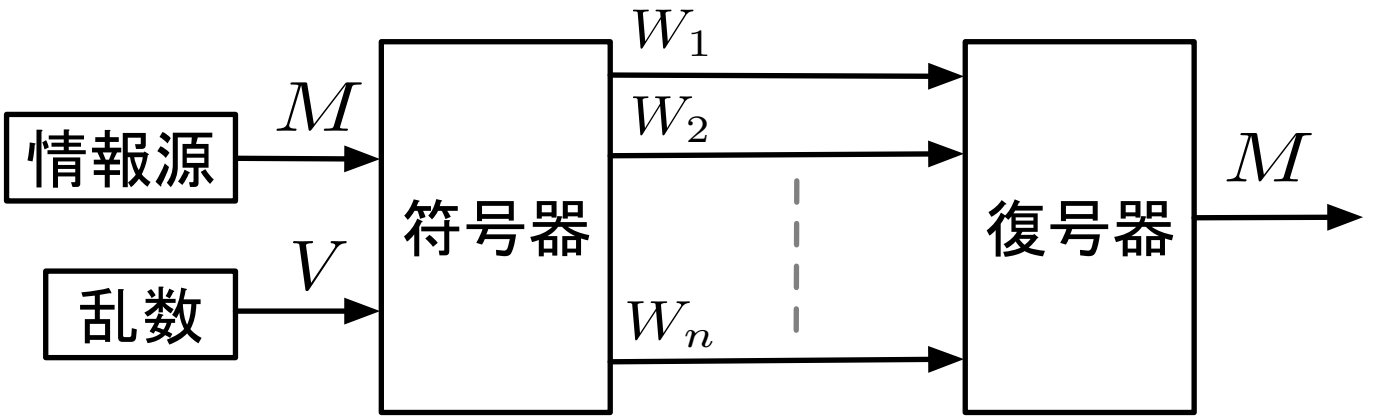
(k,n)しきい値法

$$H(M|W_{i_1}W_{i_2}\cdots W_{i_l}) = H(M) \quad \text{if } l < k$$
$$H(M|W_{i_1}W_{i_2}\cdots W_{i_l}) = 0 \quad \text{if } l \geq k$$

$$H(W_i) \geq H(M)$$
$$H(V) \geq (k-1)H(M)$$

秘密分散法の構成法

秘密情報
$M = S$
乱数
$V = U_1 U_2 \cdots U_{k-1}$



Shamir (1979) : $W_i = f_{MV}(i)$,

$$f_{MV}(t) = S + U_1 t + U_2 t^2 + \cdots U^{k-1} t^{t-1}$$

Karnin–Green–Hellman (1983) :

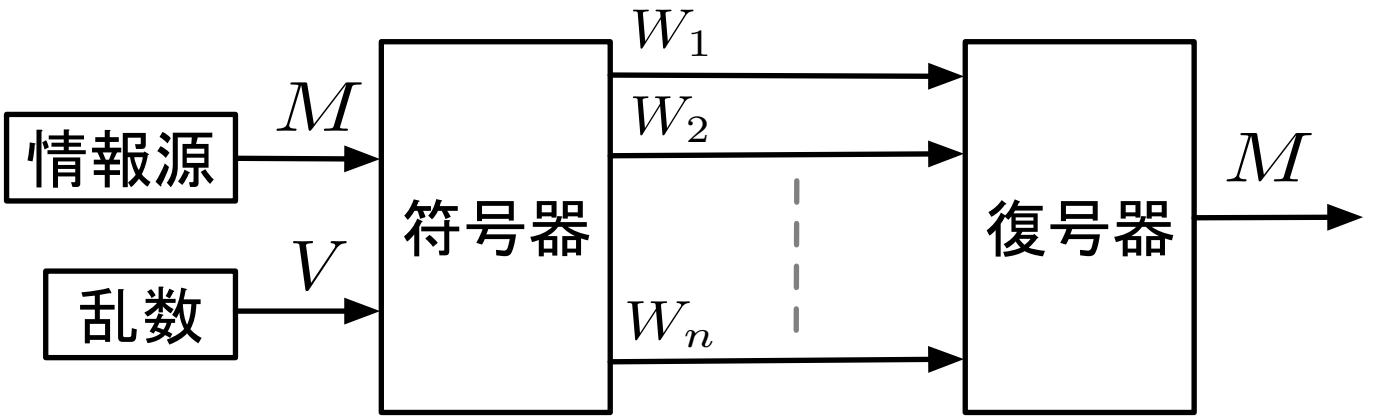
$$\mathcal{S} = \mathcal{W} = \mathcal{U} = \mathrm{GF}(p^m)$$

$$(S, W_1, W_2, \cdots, W_n) = (S, U_1, U_2, \cdots, U_{k-1})G$$

G: $k \times (n+1)$ 行列

任意の k 列が線型独立　　最大距離分離符号

ランプ型秘密分散法



(k, L, n) ランプ型しきい値法

Blakley-Meadows (1984), 山本(1985)

$$H(M|W_{i_1}W_{i_2}\cdots W_{i_l}) = H(M) \quad \text{if} \quad l \le k-L$$

$$H(M|W_{i_1}W_{i_2}\cdots W_{i_t}) = \frac{k-t}{L}H(M) \quad \text{if} \quad k-L \le l \le k$$

$$H(M|W_{i_1}W_{i_2}\cdots W_{i_l}) = 0 \quad \text{if} \quad l \ge k$$

$$\Rightarrow \quad H(W_i) \ge \frac{H(M)}{L}, \qquad H(V) \ge \frac{k-L}{L}H(M)$$

ランプ型秘密分散法

G.R.Blakley and C.Meadows

"Security of ramp scheme"
Advances in Cryptology-Crypto'84, LNCS 196, pp.242-269, 1985

(Crypto: 1984年夏開催, 予稿集:1985年1月出版)

山本博資

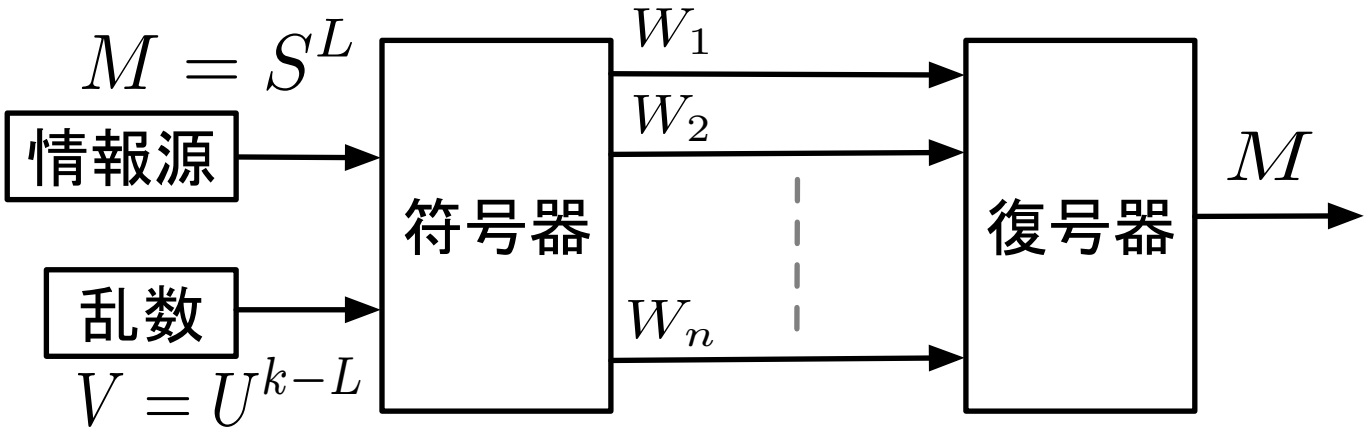
"秘密分散通信システムに対する実用暗号化法"
電子通信学会技術報告, IT84-8, pp.23-29, 1984年5月

"(k, L, n)しきい値秘密分散法"
電子通信学会論文誌, vol.J68-A, no.9, pp.945-952, 1985年

"Secret sharing system using (k, L, n) threshold scheme"
Electronics and Communications in Japan, vol.69 no.9, pp.46-54, 1986

多重符号化としてのランプ型秘密分散法

$M = S^L$
L個の情報の多重符号化



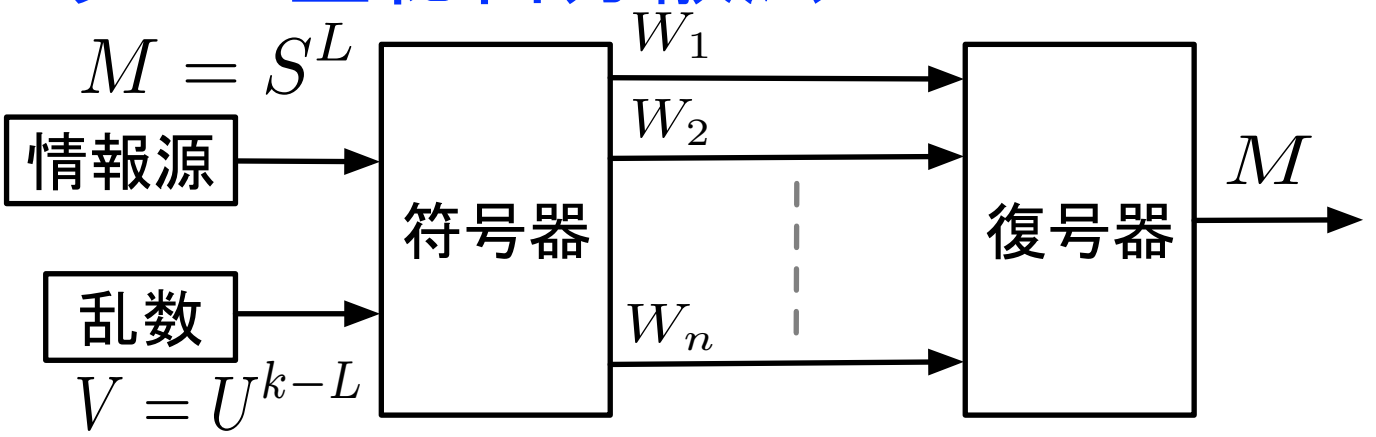
$$H(W_i) \geq \frac{H(M)}{L} \quad \Rightarrow \quad R_{W_i} = \frac{H(W_i)}{L} = \frac{H(M)}{L^2} = \frac{H(S)}{L}$$

$$H(V) \geq \frac{k-L}{L} H(M) \quad \Rightarrow \quad R_V = \frac{H(V)}{L} = \frac{k-L}{L^2} H(M) = \frac{k-L}{L} H(S)$$

効率がよい

多重符号化としてのランプ型秘密分散法

$M = S^L$
L個の情報の多重符号化



$$H(M|W_{i_1}W_{i_2}\cdots W_{i_t}) = \frac{k-t}{L}H(M) \text{ if } k-L<t<k$$

⇓ S^Lの一部が明確に漏洩する可能性がある.

強安全なランプ型秘密分散法（山本1985）

任意の$S_{j_1}S_{j_2}\cdots S_{j_{k-t}}$に対して完全秘匿

$$H(S_{j_1}S_{j_2}\cdots S_{j_{k-t}}|W_{i_1}W_{i_2}\cdots W_{i_t}) = H(S_{j_1}S_{j_2}\cdots S_{j_{k-t}})$$

強安全なランプ型秘密分散法の構成法 (山本1985)

秘密情報: $M = S^L = S_1 S_2 \cdots S_L$

乱数: $V = U^{k-L} = U_1 U_2 \cdots U_{k-L}$

$\mathcal{S} = \mathcal{W} = \mathcal{U} = \mathrm{GF}(p^m)$

強安全性

$$H(S_{j_1} S_{j_2} \cdots S_{j_{k-t}} | W_{i_1} W_{i_2} \cdots W_{i_t}) = H(S_{j_1} S_{j_2} \cdots S_{j_{k-t}})$$

Shamirの拡張 （弱安全）

$$W_i = f_{MV}(i), \quad f_{MV}(\alpha) = S_1 + S_2\alpha^2 + \cdots + S_L\alpha^{L-1} + U_1\alpha^L + U_2\alpha^{L+1} + \cdots + U_{k-L}\alpha^{t-1}$$

Karnin-Green-Hellman の拡張（強安全）

$$(S_1, S_2, \cdots, S_L, W_1, W_2, \cdots, W_n) = (S_1, S_2, \cdots, S_L, U_1, U_2, \cdots, U_{k-L})G$$

G: $k \times (L+n)$ 行列

任意の k 列が線型独立　最大距離分離符号

弱安全ランプ型秘密分散法の例

Shamirの拡張　（弱安全）

$$W_i = f_{MV}(i),\ \ f_{MV}(\alpha) = S_1 + S_2\alpha^2 + \cdots + S_L\alpha^{L-1}$$
$$+U_1\alpha^L + U_2\alpha^{L+1} + \cdots + U_{k-L}\alpha^{t-1}$$

$(4, 2, 15)$ ランプ型秘密分散

GF(17)

$$f_{MV}(\alpha) = S_1 + S_2\alpha^2 + U_1\alpha^3 + U_4\alpha^4$$

$$5S_2 = 7W_3 + 9W_6 + W_{15}$$

強安全なランプ型秘密分散法の構成法 (山本1985)

秘密情報: $M = S^L = S_1 S_2 \cdots S_L$

乱数: $V = U^{k-L} = U_1 U_2 \cdots U_{k-L}$

$\mathcal{S} = \mathcal{W} = \mathcal{U} = \mathrm{GF}(p^m)$

ISO/IEC 19592-2 (2017-10)

Shamirの拡張 （弱安全）

$$W_i = f_{MV}(i), \quad f_{MV}(\alpha) = S_1 + S_2\alpha^2 + \cdots + S_L\alpha^{L-1} + U_1\alpha^L + U_2\alpha^{L+1} + \cdots + U_{k-L}\alpha^{t-1}$$

Karnin-Green-Hellman の拡張（強安全）

$$(S_1, S_2, \cdots, S_L, W_1, W_2, \cdots, W_n) = (S_1, S_2, \cdots, S_L, U_1, U_2, \cdots, U_{k-L})G$$

G: $k \times (L+n)$ 行列

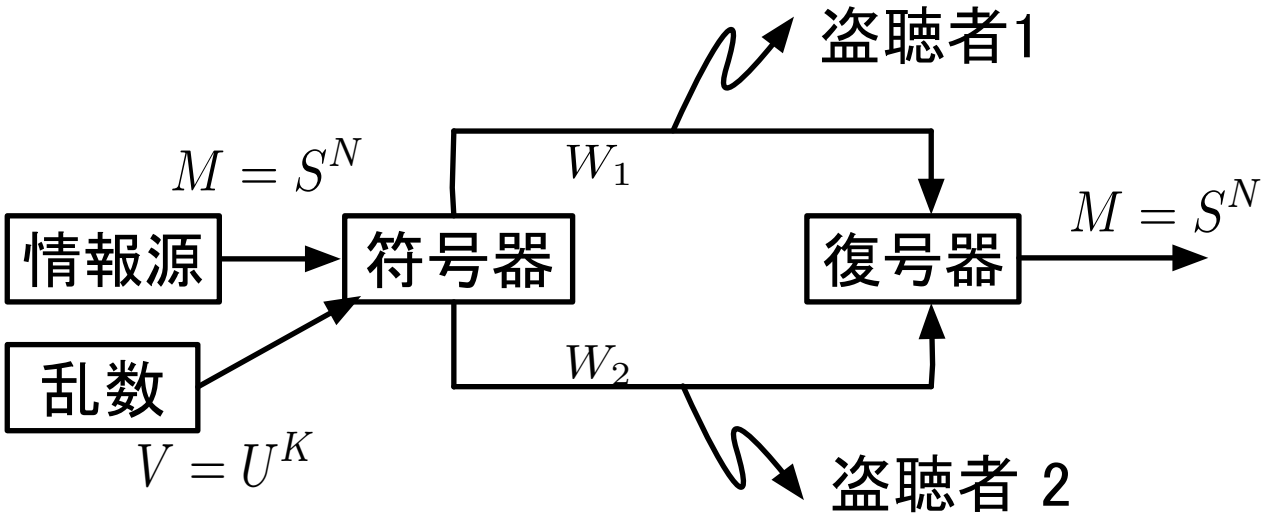
任意の k 列が線型独立　最大距離分離符号

秘密分散通信システム(Yamamoto, 1986)

$$\frac{H(M|W_i)}{N} = \frac{H(S^N|W_i)}{N} \geq h_i$$

$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$

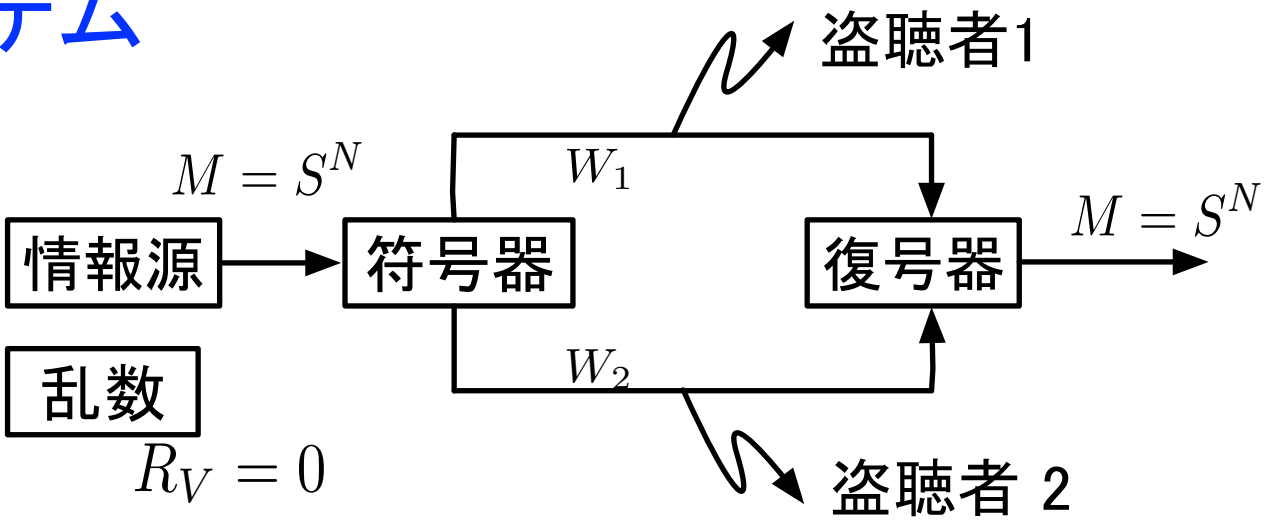
$$h_1 = h_2 = \frac{H(S)}{2}$$



強安全な秘密情報の
多重符号化法

他のh_1, h_2 の構成方法は？

秘密分散通信システム



強安全なランプ型秘密分散法

$$n = k = L = N$$

$$(\widehat{W}_1, \widehat{W}_2, \cdots, \widehat{W}_L)$$

$$W_1 = (\widehat{W}_1, \widehat{W}_2, \cdots, \widehat{W}_t)$$

$$W_2 = (\widehat{W}_{t+1}, \widehat{W}_{t+2}, \cdots, \widehat{W}_L)$$

符号化レート

$$R_{W_1} = \frac{H(W_1)}{L} = \frac{t}{L} H(S)$$

$$R_{W_2} = \frac{H(W_2)}{L} = \frac{L-t}{L} H(S)$$

任意の $S_{j_1} S_{j_2} \cdots S_{j_t}, S_{j_1} S_{j_2} \cdots S_{j_{L-t}}$ に対して完全秘匿

$$H(S_{j_1} S_{j_2} \cdots S_{j_{L-t}} | W_1) = H(S_{j_1} S_{j_2} \cdots S_{j_{L-t}})$$

$$H(S_{j_1} S_{j_2} \cdots S_{j_t} | W_2) = H(S_{j_1} S_{j_2} \cdots S_{j_t})$$

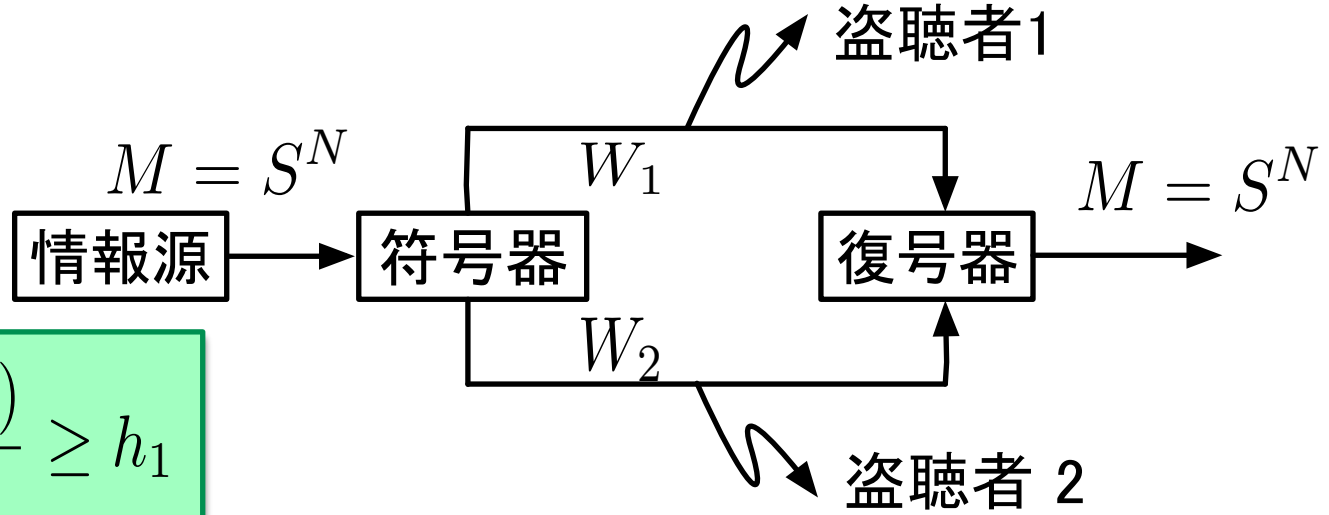
$$\frac{H(M|W_1)}{N} = \frac{L-t}{L} H(S)$$

$$\frac{H(M|W_2)}{N} = \frac{t}{L} H(S)$$

相関情報と秘密分散通信システム

Yamamoto (1994)

$S = (X, Y)$



$$\frac{H(M|W_1)}{N} = \frac{H(S^N|W_1)}{N} \geq h_1$$
$$\frac{H(M|W_2)}{N} = \frac{H(S^N|W_2)}{N} \geq h_2$$

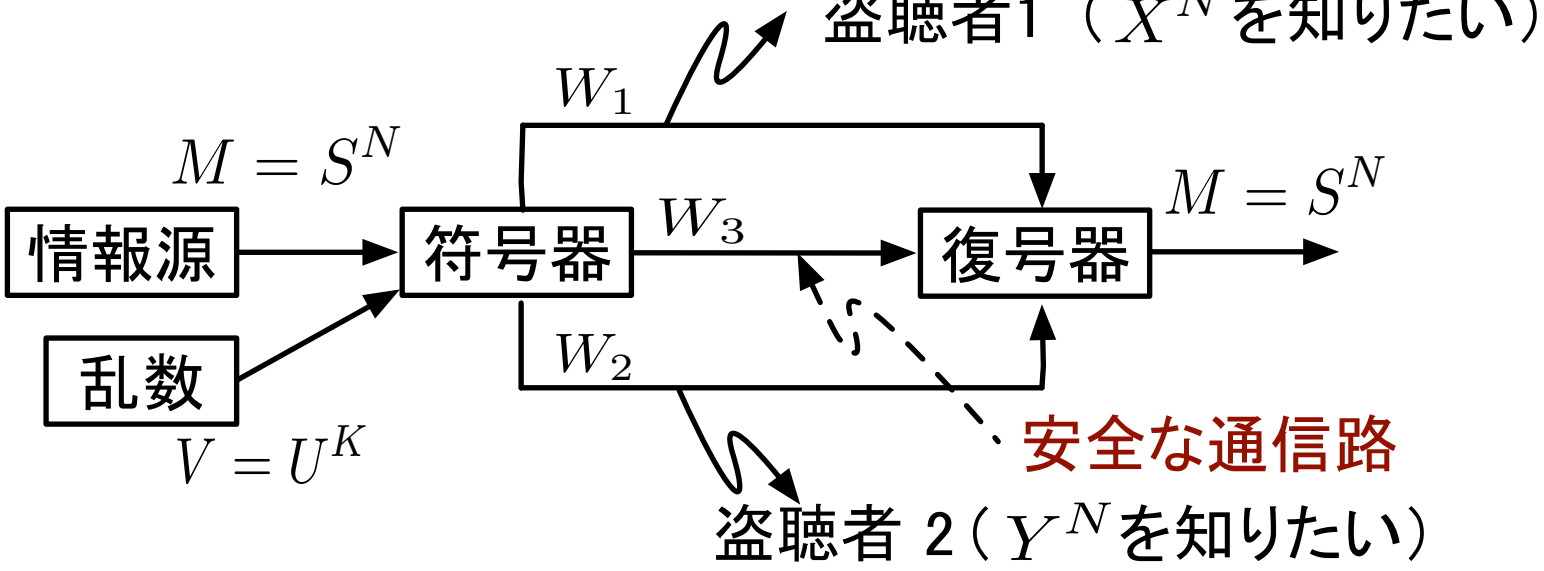
$$\frac{H(X^N|W_1)}{N} \geq h_1, \quad \frac{H(Y^N|W_1)}{N} \geq h_1,$$
$$\frac{H(S^N|W_2)}{N} \geq h_2$$

$$0 \leq h_1 \leq \min\{H(X), H(Y)\}$$
$$R_{W_1} = \frac{H(W_1)}{N} \geq \max\{h_2, H(XY) - h_1\}$$
$$R_{W_2} = \frac{H(W_2)}{N} \geq \max\{h_1, H(XY) - h_2\}$$

相関情報と秘密分散通信システム

Yamamoto (1994)

$S=(X,Y)$



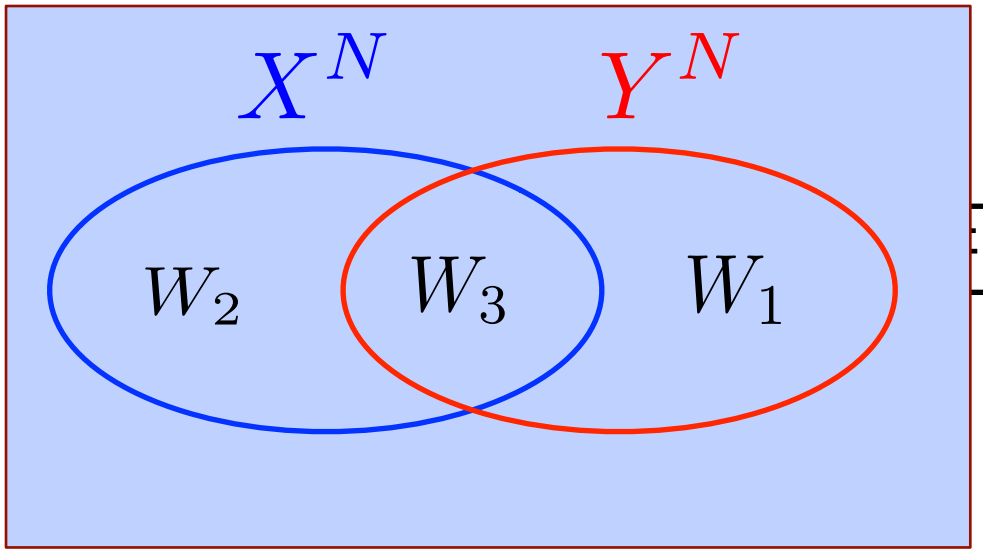
$$\frac{H(X^N|W_1)}{N}=H(X),\quad \frac{H(X^N|W_1W_2)}{N}\geq h_{12}\qquad I(X;Y)\leq h_{12}\leq \min\{H(X),H(Y)\}$$

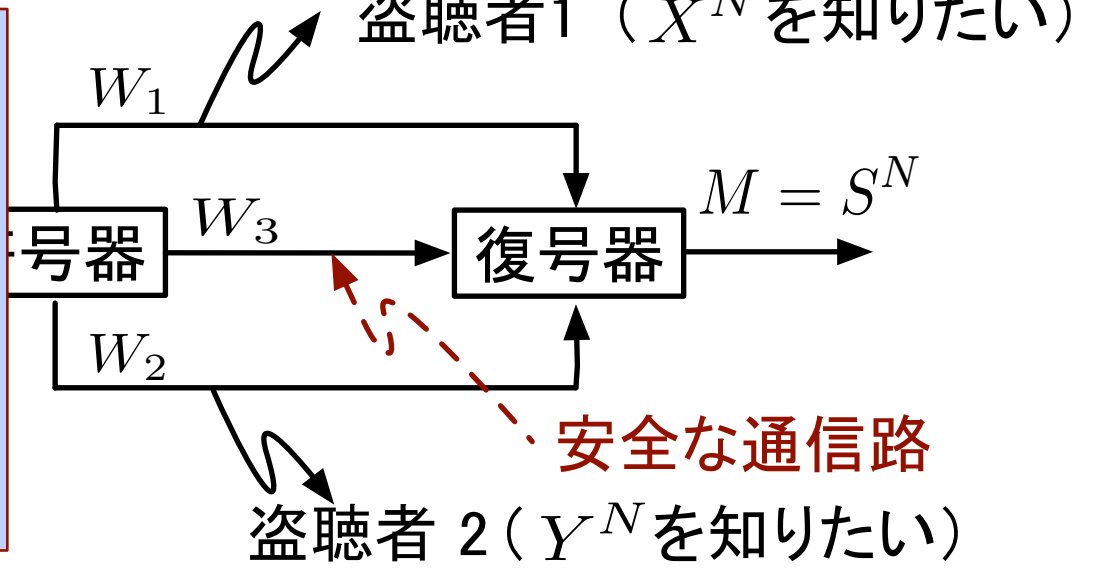
$$\frac{H(Y^N|W_2)}{N}=H(Y),\quad \frac{H(Y^N|W_1W_2)}{N}\geq h_{12}\qquad R_{W_1}+R_{W_2}+R_{W_3}\geq H(XY)$$

$$R_{W_3}\geq h_{12}$$

相関情報と秘密分散通信システム

Yamamoto (1994)





$$\frac{H(X^N|W_1)}{N} = H(X), \quad \frac{H(X^N|W_1W_2)}{N} \geq h_{12} \quad I(X;Y) \leq h_{12} \leq \min\{H(X), H(Y)\}$$

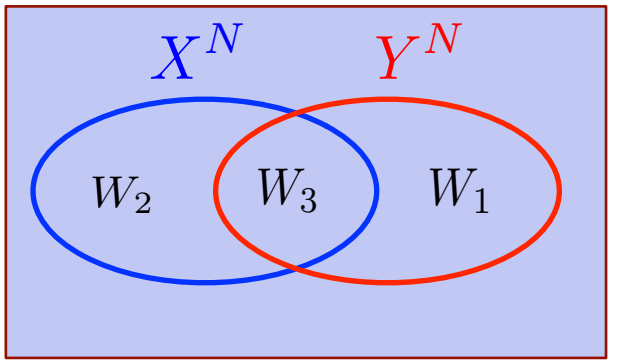
$$\frac{H(Y^N|W_2)}{N} = H(Y), \quad \frac{H(Y^N|W_1W_2)}{N} \geq h_{12} \quad R_{W_1} + R_{W_2} + R_{W_3} \geq H(XY)$$

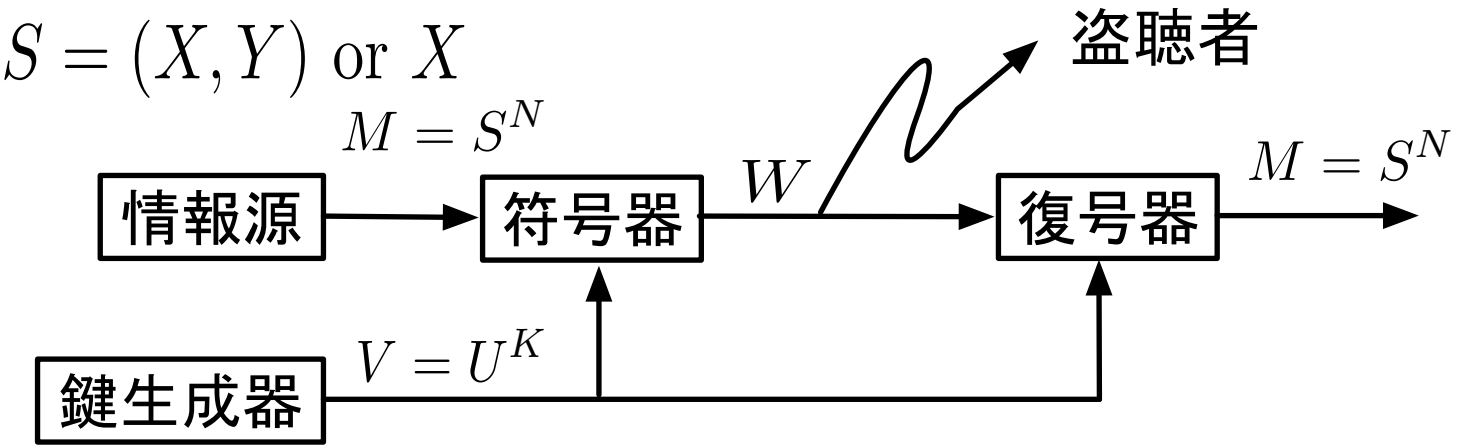
$$R_{W_3} \geq h_{12}$$

h_{12} の最小値: X と Y の共通情報量

相関情報とShannon暗号システム

Yamamoto (1994)





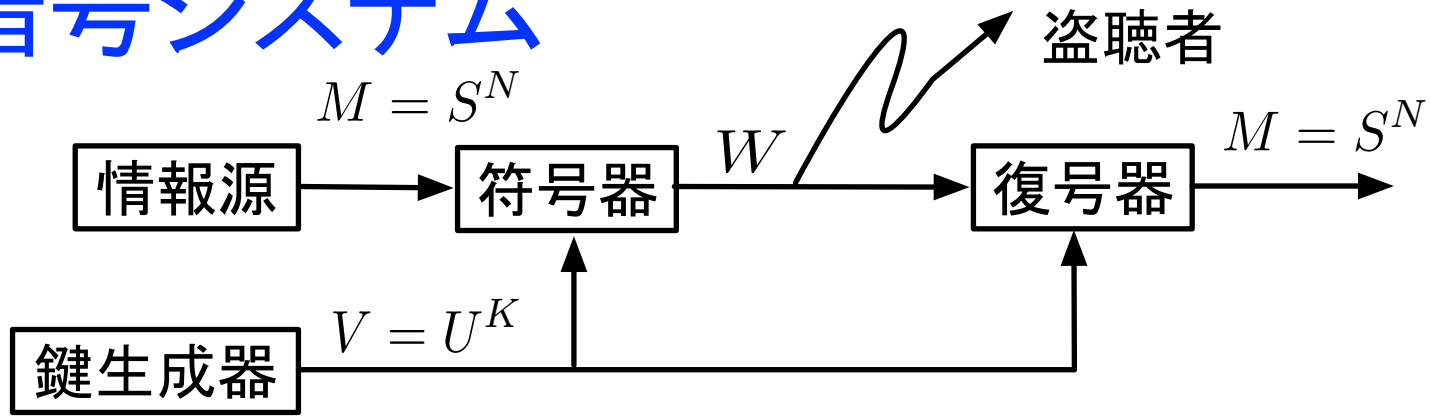
$$\frac{H(X^N Y^N)}{N} \geq h_{XY}$$

$$\frac{H(X^N)}{N} \geq h_X$$

$$\frac{H(Y^N)}{N} \geq h_Y$$

(X^N, Y^N) を送る	X^N を送る
$R_W \geq H(XY)$	$R_W \geq H(X)$
$R_V \geq h_{XY}$	$R_V \geq \max\{h_{XY} - H(Y\|X), 0\}$
$R_V \geq \max\{h_X, h_Y\}$	$R_V \geq \max\{h_X, h_Y - H(Y\|X)\}$

Shannonの暗号システム



任意のシステム（Yamamoto, 1991）

$$\frac{H(M|W)}{N} = \frac{H(S^N|W)}{N} \geq h, \qquad 0 \leq h \leq H(S)$$

鍵レート

$$R_V = \frac{H(V)}{N} = \frac{KH(U)}{N} \geq h$$

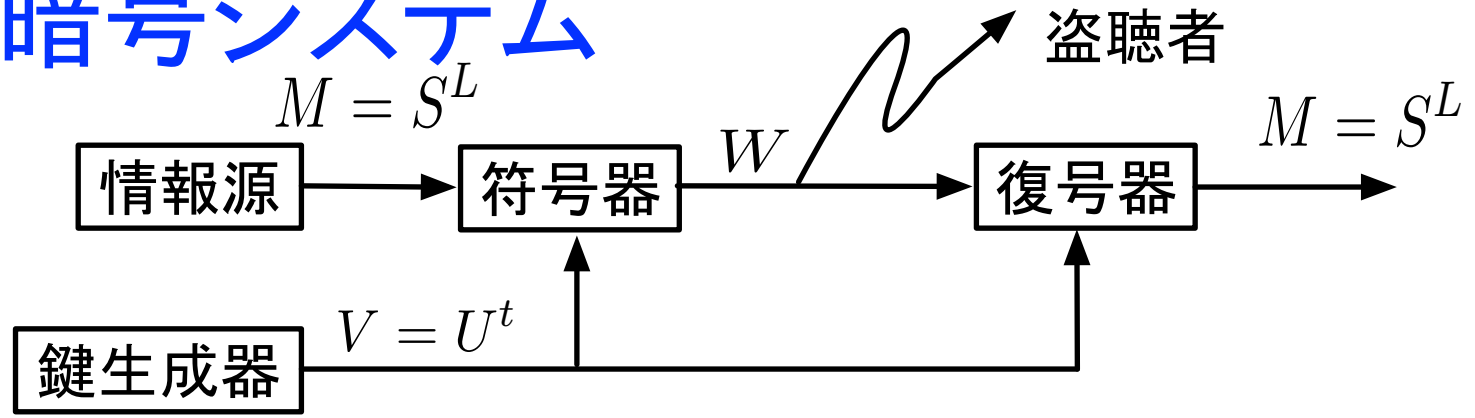
暗号文レート

$$R_W = \frac{H(W)}{N} \geq H(S)$$

問題点

情報 $M = S^N$ の一部が明確に漏洩する可能性がある

Shannonの暗号システム



強安全なランプ型秘密分散法

$n = k = L + t$

$$(\widehat{W}_1, \widehat{W}_2, \cdots, \widehat{W}_{L+t}) \overbrace{= (U_1, U_2, \cdots, U_t, \widehat{W}_{t+1}, \widehat{W}_{t+2}, \cdots, \widehat{W}_{L+t})}^{W}$$

$$R_W = \frac{H(W)}{L} = H(S)$$

$$R_V = \frac{H(V)}{N} = \frac{tH(U)}{L}$$

任意の $S_{i_1} S_{i_2} \cdots S_{i_t}$ に対して完全秘匿

$$H(S_{i_1} S_{i_2} \cdots S_{i_t} | W) = H(S_{i_1} S_{i_2} \cdots S_{i_t})$$

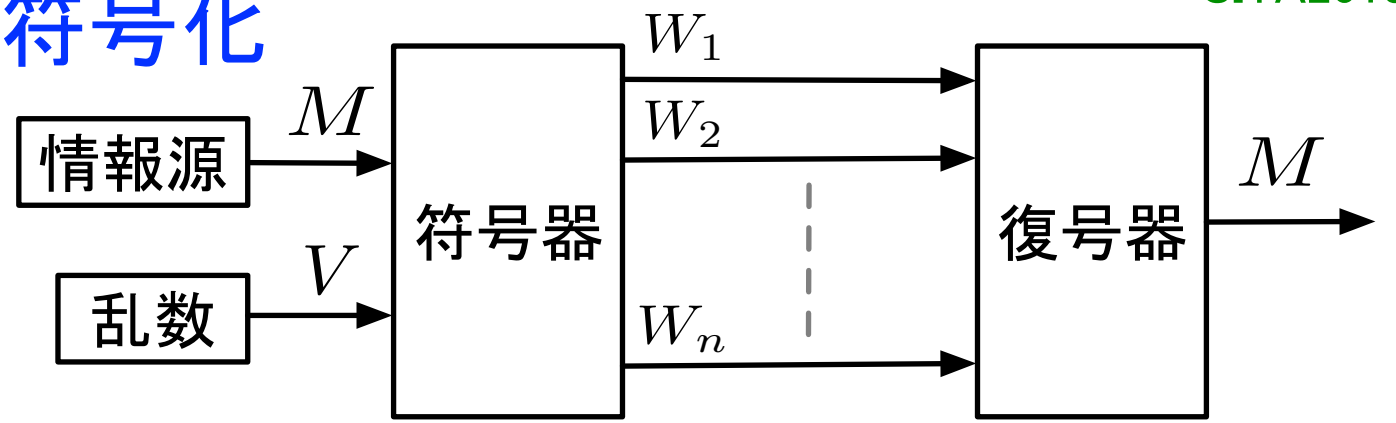
不完全秘匿

$$\frac{H(M|W)}{N} = \frac{tH(S)}{L}$$

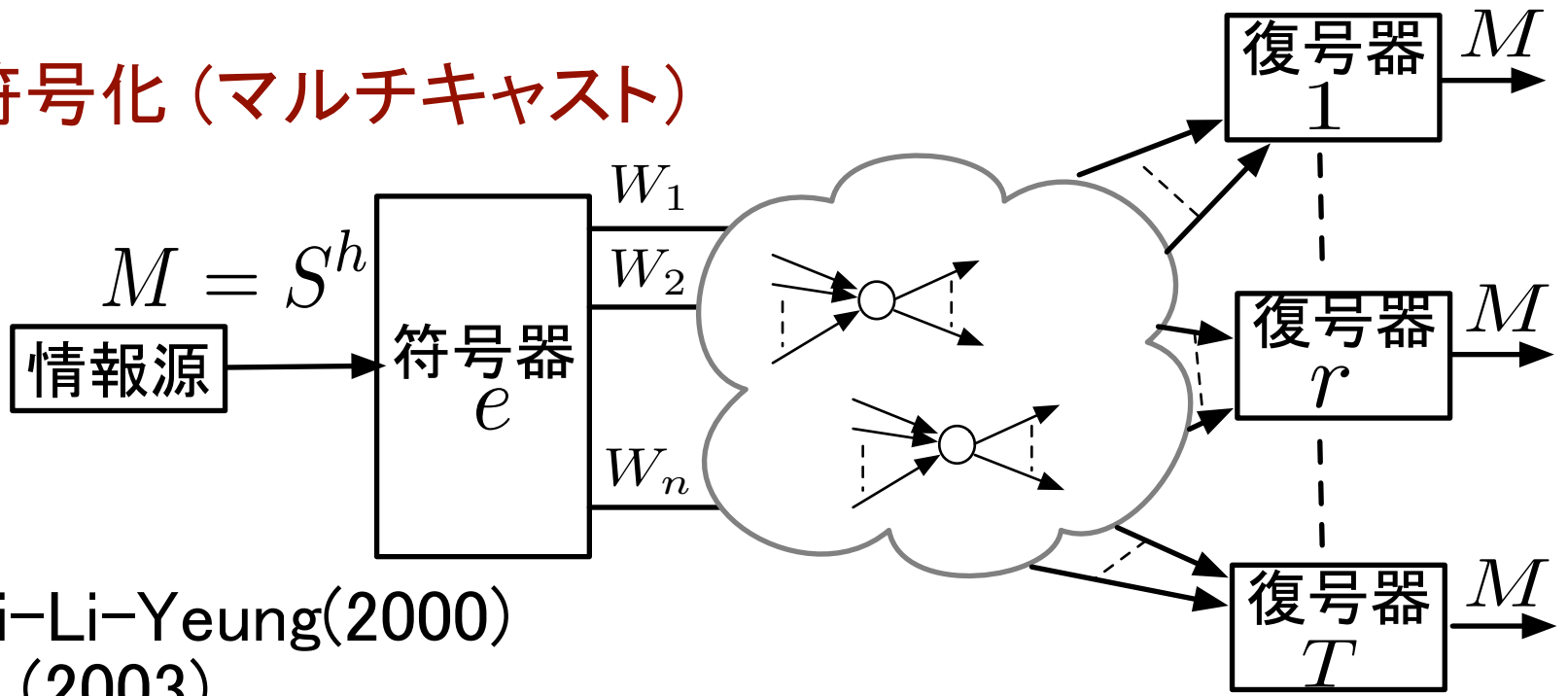
情報$M = S^N$の一部が明確に漏洩する可能性がない

ネットワーク符号化

秘密分散法



ネットワーク符号化（マルチキャスト）

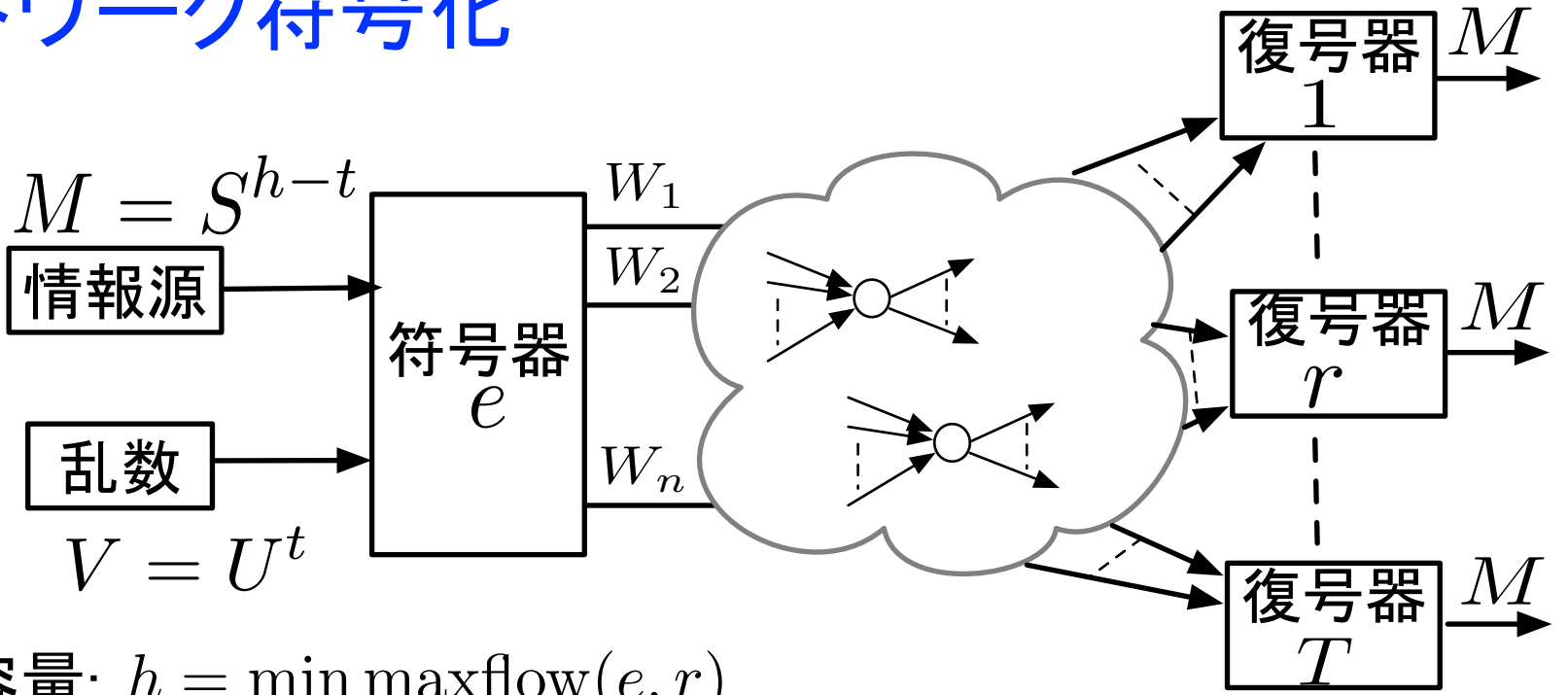


Alshwede–Cai–Li–Yeung(2000)
Li–Yeung–Cai (2003)

マルチキャスト容量： $h = \min_r \mathrm{maxflow}(e, r)$

安全なネットワーク符号化

$t < h$

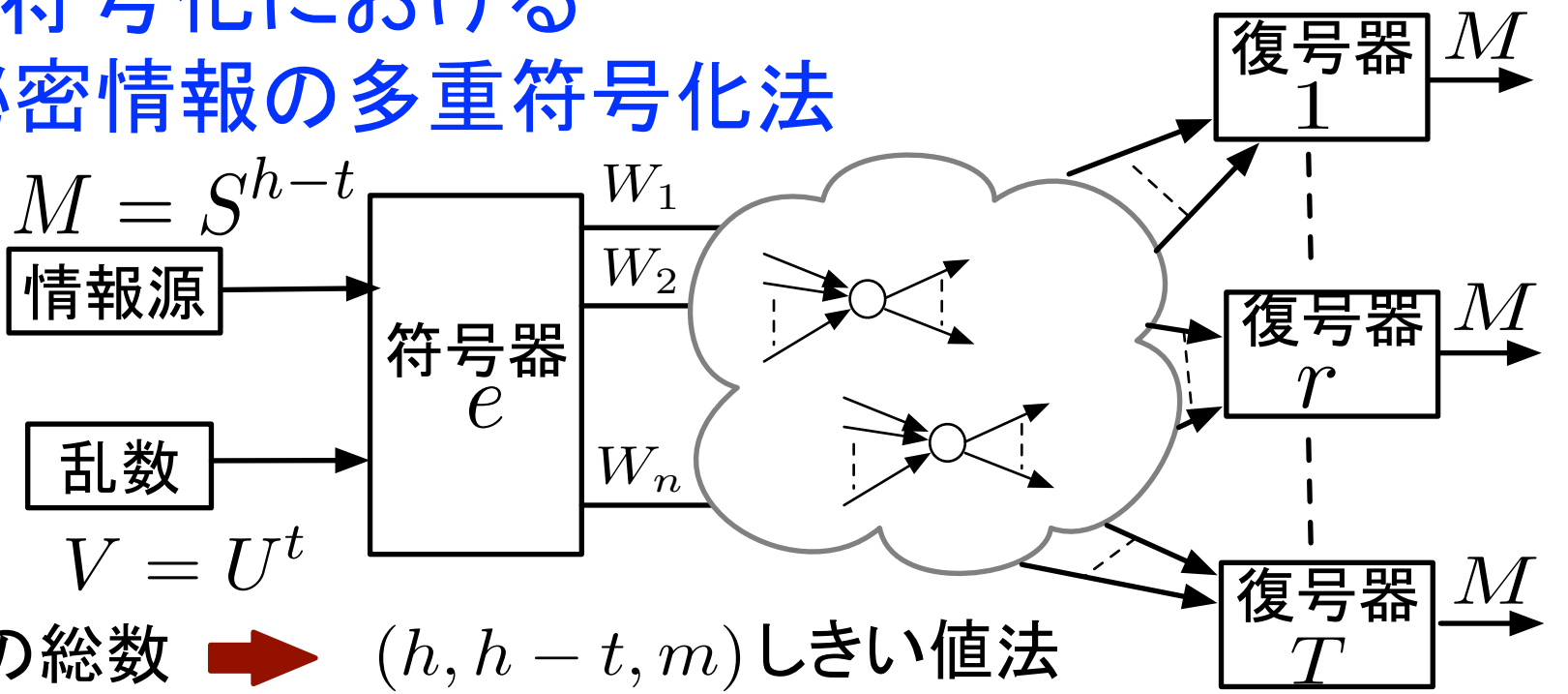


マルチキャスト容量: $h = \min_r \mathrm{maxflow}(e, r)$

Cai-Yeung (2002)　t -secureなネットワーク符号化
任意のt個の通信路を盗聴されても M が完全秘匿.

$t+1$ 個以上盗聴されるとM の一部が明確に漏れる可能性がある.

ネットワーク符号化における 強安全な秘密情報の多重符号化法



m：通信路の総数 ➡ $(h, h-t, m)$しきい値法

Harada-Yamamoto(2002): Strongly t-secureネットワーク符号化

任意の $W_{i_1}, W_{i_2}, \cdots, W_{i_{t+b}}$ と $S_{j_1}, S_{j_2}, \cdots, S_{j_{h-t-b}}$ に対して完全秘匿

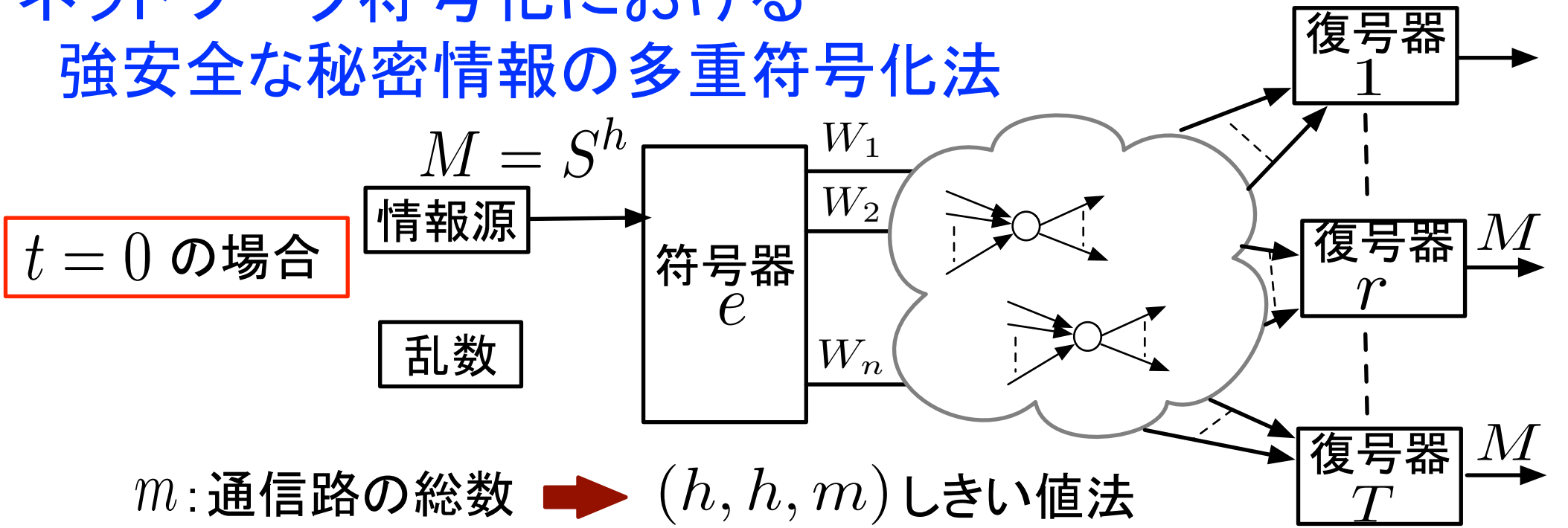
$$H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-t-b}} | W_{i_1}, W_{i_2}, \cdots, W_{i_{t+b}}) = H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-t-b}})$$

不完全秘匿

$$H(M | W_{i_1}, W_{i_2}, \cdots, W_{i_{t+b}}) = \frac{(h-t-b)H(M)}{h-t}$$

$0 \leq b < h-t$

ネットワーク符号化における 強安全な秘密情報の多重符号化法



m：通信路の総数 ➡ (h, h, m) しきい値法

Harada-Yamamoto(2002): Strongly 0-secureネットワーク符号化

任意の $W_{i_1}, W_{i_2}, \cdots, W_{i_b}$ と $S_{j_1}, S_{j_2}, \cdots, S_{j_{h-b}}$ に対して完全秘匿

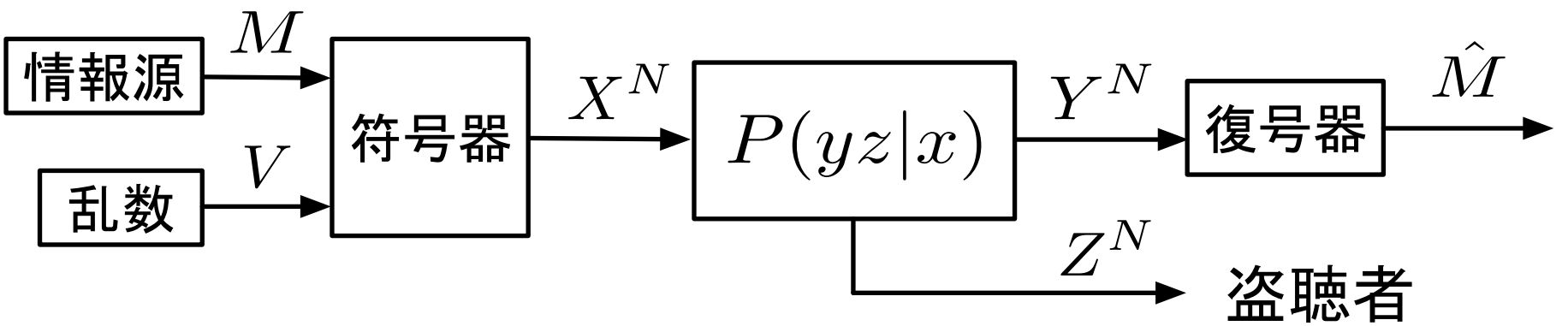
$$H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-b}} | W_{i_1}, W_{i_2}, \cdots, W_{i_b}) = H(S_{j_1}, S_{j_2}, \cdots, S_{j_{h-b}})$$

$0 \le b < h$

不完全秘匿

$$H(M | W_{i_1}, W_{i_2}, \cdots, W_{i_b}) = \frac{(h-b)H(M)}{h}$$

盗聴通信路符号化



$M \in I_A \in \{1, 2, \cdots, A\}$

通信路容量 $C = \max_X I(X;Y)$

符号化レート $R = \dfrac{1}{N} \log A$

復号誤り率 $P_e = \Pr\{M \neq \hat{M}\}$

安全性指標

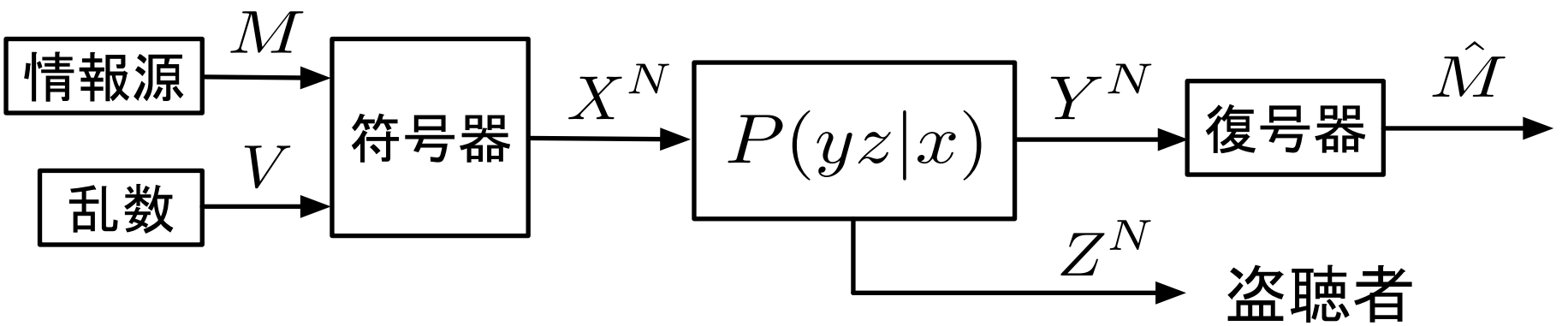
$$\frac{1}{N} I(M; Z^N) < \varepsilon$$

$$I(M; Z^N) < \varepsilon$$

$$\frac{1}{A(A-1)} \sum_m \sum_{m'} \| P_{Z^N|m} - P_{Z^N|m'} \| < \varepsilon$$

$$\max_{m,m'} \| P_{Z^N|m} - P_{Z^N|m'} \| < \varepsilon$$

盗聴通信路符号化



Wyner (1975)
Csiszár–Körner (1978)

通信路容量 $C = \max_X I(X;Y)$

秘匿容量 $C_S = \max_{\tilde{X}-X-YZ} I(\tilde{X};Y) - I(\tilde{X};Z) > 0$

$X \to Y$ が $X \to Z$ より Less Noisy

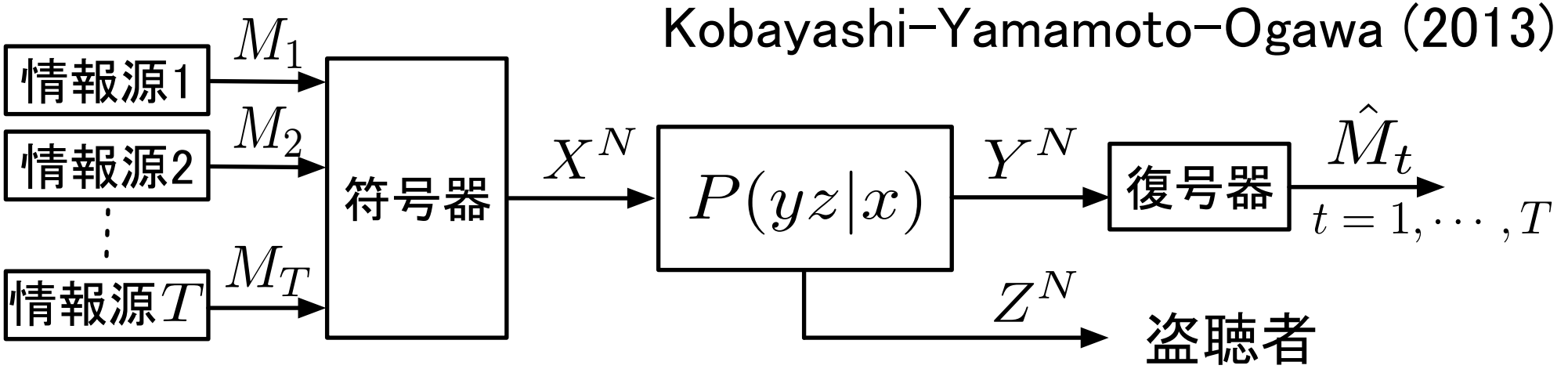
通信可能な情報量

Channel Resolvability
Z^N の分布を M に依存しなくさせる.

一般に $C_S < C$

盗聴通信路に対する強安全な多重符号化

Kobayashi-Yamamoto-Ogawa (2013)



$$M_t \in I_{A_t} = \{1, 2, \cdots, A_t\}$$

$$R_t = \frac{1}{N} \log A_t$$

$$R_{\text{total}} = \sum_{t=1}^{T} R_t$$

$\tilde{X} - X - YZ$

$R_{\text{total}} \leq I(\tilde{X}; Y)$

$R_{\text{total}} - R_t \geq I(\tilde{X}; Z)$

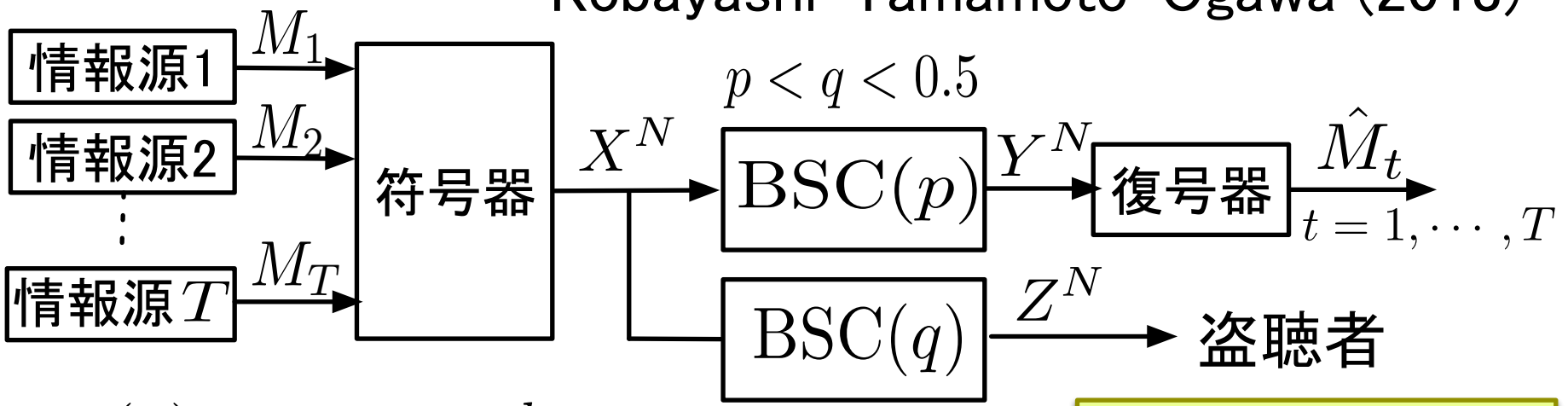
$T, A_t\ (t = 1, 2, \cdots, T)$を適切に選べば
$R_{\text{total}} \approx C$ を達成可能.

$I(M_t; Z^N) < \varepsilon$

$\max_{m_t, m_t'} \| P_{Z^N|m_t} - P_{Z^N|m_t'} \| < \varepsilon$

盗聴通信路に対する強安全な多重符号化

Kobayashi-Yamamoto-Ogawa (2013)



$$C = 1 - h(p)$$

$$C_S = h(q) - h(p)$$

$$T = \lceil C/C_S \rceil \geq 2$$

$$R_1 = R_2 = \cdots = R_T$$

$$\xi > 0$$

$$C - \xi = T(C_S - \lambda)$$

$$R_t = \frac{l}{N} = C_S - \lambda$$

$$R_{\text{total}} = \frac{lT}{N} = C - \xi$$

$$M_t = S_t^l = S_{t,1} S_{t,2} \cdots S_{t,l}$$

$$X^N = (M_1, M_2, \cdots, M_T) G$$

$$G = \begin{bmatrix} G_1 \\ G_2 \\ \vdots \\ G_T \end{bmatrix}$$

(N columns, l rows per block, Tl rows in total)

$$P_e \leq 2^{-NE(R_{\text{total}})} \qquad \frac{1}{N} I(M_t; Z^N) \leq \xi + (\xi/N)$$

まとめ

Shannonの暗号システム
秘密分散通信システム
秘密分散法
ネットワーク符号化法
盗聴通信路符号化法
など

乱数を情報に
置き換える

完全秘匿

$$H(M|W) = H(M)$$

不完全秘匿

$$0 < H(M|W) < H(M)$$

強安全な多重符号化

$$M = S^L = S_1 S_2 \cdots S_L$$

個別情報への完全秘匿

$$H(S_{i_1} S_{i_2} \cdots S_{i_t}|W) = H(S_{i_1} S_{i_2} \cdots S_{i_t})$$