修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　情報理工　学研究科情報・ネットワーク工学専攻　博士前期課程		
氏　　名	藤田 隆寛	学籍番号	173133
論 文 題 目	秘匿メッセージを有する通信路において 強安全性を達成するポーラ符号の構成		

要　旨

Wyner により提案された盗聴通信路(wiretap channel)における符号化問題は，盗聴者が存在する通信路において，送信者から正規受信者へのメッセージを盗聴者から秘匿して送ることを目的とする．Csiszár と Köner は，盗聴者への通信路が劣化するとは限らない一般の盗聴通信路を含む，正規受信者と盗聴者の両者に共通メッセージを送り，正規受信者には個別メッセージと秘匿メッセージを送る通信路である秘匿メッセージを有する放送型通信路(broadcast channel with confidential messages, BCC)の秘密保持容量を求めた．Liu らは，1 人の送信者が 2 人の受信者に対しそれぞれ独立した秘匿メッセージのみを送る通信路である秘匿メッセージを有する放送型通信路(broadcast channel with confidential messages, BC-CM)を提案した．Xu らは，BCC 及び BC-CM を拡張し，1 人の送信者が 2 人の受信者に対し，共通メッセージとそれぞれ独立した個別と秘匿メッセージを送る通信路である 2 つの秘匿メッセージを有する放送型通信路(broadcast channel with two confidential messages, BC-2CM)を提案した．BC-CM 及び BC-2CM に対しては，それぞれ受信者が他の受信者宛の秘匿メッセージを復号できないように通信を行える達成可能な符号化レートの領域(秘密保持領域)は明らかになっておらず，最も広い達成可能なレート領域が求められている．

2008 年に Arıkan により，確率過程の分極操作に基づくポーラ(polar)符号と呼ばれる符号が提案された．ポーラ符号は，定常無記憶情報源及び離散無記憶通信路における符号化レートの理論的限界を，低計算複雑度と低空間複雑度で達成できることが明らかにされている．ポーラ符号は，様々な符号化問題に対して，符号化レートの理論的限界を，低複雑度で達成する原理をもたらすと期待されている．以前，Şaşoğlu と Vardy により，劣化型対称盗聴通信路において強安全性を，Wei と Ulukus により，BC-CM において弱安全性を，Glucu と Barg によって，BCC において強安全性を達成するポーラ符号の構成が提案されている．

本研究では，BC-2CM における強安全性を達成するポーラ符号の構成を得ることを目的とする．共通メッセージの送信は，Glucu と Barg の構成の共通メッセージの考えを利用する．秘匿メッセージの送信は，Şaşoğlu と Vardy の構成の強安全性のためにポーラ符号の各ビット位置を受信者と盗聴者の復号の可否により厳密に区分する方法を，Wei と Ulukus の構成のサブブロックの連鎖構造を用いて弱安全性を達成する構成に適用する．個別メッセージの送信は，前述の秘匿メッセージを送信する構成に新たに個別メッセージの送信を組み込む．以上の構成で，目的を達成する．この提案構成法により，2 元入力の BC-2CM において強安全性と従来知られている最も広い達成可能なレート領域の任意の境界点を達成するポーラ符号が得られることを示す．

平成30年度　修士学位論文

秘匿メッセージを有する通信路において強安全性を達成するポーラ符号の構成

電気通信大学 大学院 情報理工学研究科
博士前期課程 情報・ネットワーク工学専攻
1731133　藤田 隆寛
指導教員　八木秀樹 准教授　大濱靖匡 教授

提出　平成31年1月28日

THE UNIVERSITY OF ELECTRO-COMMUNICATIONS
Department of Communication Engineering and Informatics

目 次

第 1 章

はじめに

Wyner [13] により提案された**盗聴通信路** (*wiretap channel*) における符号化問題は，盗聴者が存在する通信路において，送信者から正規受信者へのメッセージを盗聴者から秘匿して送ることを目的する．Wyner [13] は，送信者から盗聴者への通信路が正規受信者への通信路より劣化した通信路 (劣化型盗聴通信路) であるときに，盗聴者へメッセージの情報を漏らさずに通信を行える符号化レートの上限である**秘密保持容量**を求めた．Csiszár と Köner [3] は，盗聴者への通信路が劣化するとは限らない一般の盗聴通信路を含む，正規受信者と盗聴者の両者に共通メッセージを送り，正規受信者には個別メッセージと秘匿メッセージを送る通信路である**秘匿メッセージを有する放送型通信路** (*broadcast channel with confidential messages, BCC*) の秘密保持容量を求めた．Liu ら [9] は，1 人の送信者が 2 人の受信者に対しそれぞれ独立した秘匿メッセージのみを送る通信路である**秘匿メッセージを有する放送型通信路** (*broadcast channel with confidential messages, BC-CM*) を提案した．Csiszár と Köner のモデル [3] と Liu らのモデル [9] は同一の名称であるが，異なる通信路である．以下，Csiszár と Köner のモデル [3] を BCC，Liu らのモデル [9] を BC-CM と称する．Xu ら [14] は，BCC 及び BC-CM を拡張し，1 人の送信者が 2 人の受信者に対し，共通メッセージとそれぞれ独立した個別メッセージと秘匿メッセージを送る通信路である *2* **つの秘匿メッセージを有する放送型通信路** (*broadcast channel with two confidential messages, BC-2CM*) を提案した．BC-CM 及び BC-2CM に対しては，それぞれの受信者が他の受信者宛の秘匿メッセージを復号できないように通信を行える達成可能な符号化レートの領域 (**秘密保持領域**) は明らかになっておらず，最も広い達成可能なレート領域が求められている．

2008 年に Arıkan [1] により，確率過程の分極操作に基づく**ポーラ** (*polar*) **符号**と呼ばれる符号が提案された．ポーラ符号は，定常無記憶情報源及び離散無記憶通信路における符号化レートの理論的限界を，低計算複雑度と低空間複雑度で達成できることが明らかにされている．ポーラ符号は，様々な符号化問題に対して，符号化レートの理論的限界を，低複雑度で達成する原理をもたらすと期待されている．以前，Şaşoğlu と Vardy [11] により，劣化型対称盗聴通信路において**強安全性** (*strong secrecy*) を達成するポーラ符号

の構成が提案され，Wei と Ulukus [12] により，一般の**盗聴通信路**と BC-CM において**弱安全性** (*weak secrecy*) を達成するポーラ符号の簡潔な構成が提案されている．また，Glucu と Barg [7] によって，BCC において**強安全性**を達成するポーラ符号の構成が提案されている．

本稿では，BC-2CM における強安全性を達成するポーラ符号の構成を得ることを目的とする．共通メッセージは，Glucu と Barg の構成 [7] の共通メッセージの送信の考えを利用して送信する．秘匿メッセージは，Şaşoğlu と Vardy [11] によって提案された劣化型対称盗聴通信路において強安全性を達成するためにポーラ符号の各ビット位置を受信者と盗聴者の復号の可否により厳密に区分する方法を，Wei と Ulukus [12] によって提案された，BC-CM においてサブブロック間の連鎖構造を用いて弱安全性を達成するポーラ符号の構成に適用することで送信する．個別メッセージは，前述の秘匿メッセージを送信する構成に新たに個別メッセージの送信を組み込むことで送信する．以上の構成で，目的を達成する．この提案構成法により，2 元入力の BC-2CM において強安全性と従来知られている最も広い達成可能なレート領域の任意の境界点を達成するポーラ符号が得られることを示す．

本論文の構成を以下に記す．第 2 章では準備として，本論文で用いる BCC，BC-CM，BC-2CM，ポーラ符号について説明する．第 3 章では，BC- 2 CM におけるポーラ符号の構成と性能評価を記す．第 4 章では，BC-2CM におけるポーラ符号の構成が既存の BCC における構成と一致することを確認する．そして，BC-CM の構成としても利用できることを確認する．最後に，第 5 章では，本稿のまとめについて述べる．

第 2 章

準備

2.1 Csiszár と Köner のモデルによる秘匿メッセージを有する放送型通信路 (BCC)

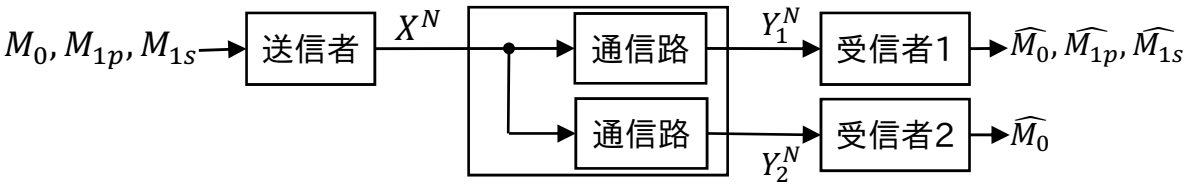

図 2.1: Csiszár と Köner のモデルによる秘匿メッセージを有する放送型通信路 (BCC)

Csiszár と Köner のモデルによる秘匿メッセージを有する放送型通信路 (BCC)[3] は，1 人の送信者が，2 人の受信者に共通メッセージを送り，そのうち 1 人の受信者には個別メッセージと秘匿メッセージも送る通信路である (図 2.1 参照)．BCC では，秘匿メッセージを他方の受信者から秘匿して送ることを目的とする．個別メッセージは他の受信者が得ることができるかは問わない．$k \in \{1,2\}$ で 2 人の受信者を区別し，共通メッセージ $M_0 \in \mathcal{M}_0 := \{1, \cdots, 2^{NR_0}\}$，個別メッセージ $M_{1p} \in \mathcal{M}_{1p} := \{1, \cdots, 2^{NR_{1p}}\}$ と秘匿メッセージ $M_{1s} \in \mathcal{M}_{1s} := \{1, \cdots, 2^{NR_{1s}}\}$ を送るものとする．送信者はメッセージ M_0, M_{1p}, M_{1s} を X^N に符号化して送り，受信者 k は Y_k^N を得る[1]．放送型通信路 $W : \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2$ を有限な入出力アルファベット $\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2$ を持つ定常無記憶通信路とする．個別メッセージと秘匿メッセージをあわせたレートを $R_1 = R_{1p} + R_{1s}$ とおく．あるメッセージを M_* と表記する．メッセージ M_* は一様に分布するものと仮定する．$\hat{M}_*$ を M_* の推定値として，受信者 1 がメッセージの復号を誤る確率を $P_{e,1}^{(N)} = \Pr(\hat{M}_0 \neq M_0 \vee \hat{M}_{1p} \neq M_{1p} \vee \hat{M}_{1s} \neq M_{1s})$

[1] X^N の表記により N 個の確率変数の組 $(X_1, X_2, \cdots, X_N)$ を表す．

とおき，受信者 2 がメッセージの復号を誤る確率を $P_{e,2}^{(N)} = \Pr(\hat{M}_0 \neq M_0)$ とおく．秘匿メッセージ M_{1s} の受信者 2 への**情報漏洩量**は相互情報量 $I(M_{1s}; Y_2^N)$ で測られる．

定義 1 (BCC の秘密保持領域)**.** BCC の符号化レート (R_0, R_1, R_{1s}) は，$N \to \infty$ としたとき，

$$\liminf_{N\to\infty} \frac{1}{N} \log M_* \geq R_*, \quad P_{e,k}^{(N)} \to 0, \quad I(M_{1s}; Y_2^N) \to 0, \quad (* = 0, 1s, 1p,\ k = 1, 2) \tag{2.1}$$

を満たす符号が存在するときに**強安全性**基準のもとで**達成可能**という．これをを単に強安全性を達成するということがある．強安全性が達成可能な符号化レート (R_0, R_1, R_{1s}) の集合を**秘密保持領域**という． □

BCC の秘密保持領域は，次のように与えられる．

命題 1 (BCC の秘密保持領域 [3, Theorem 1])**.** BCC の符号化レート (R_0, R_1, R_{1s}) の秘密保持領域は，U, V をマルコフ連鎖 $U - V - X - Y_1, Y_2$ を満たす補助確率変数 (channel prefixing) としたとき，

$$\begin{aligned}
0 \leq & R_{1s} \leq R_1, && (2.2)\\
R_{1s} \leq & I(V; Y_1|U) - I(V; Y_2|U), && (2.3)\\
R_1 + R_0 \leq & I(V; Y_1|U) + \min\{I(U; Y_1), I(U; Y_2)\}, && (2.4)\\
R_0 \leq & \min\{I(U; Y_1), I(U; Y_2)\} && (2.5)
\end{aligned}$$

となる． □

2.2　Liu らのモデルによる秘匿メッセージを有する放送型通信路 (BC-CM)

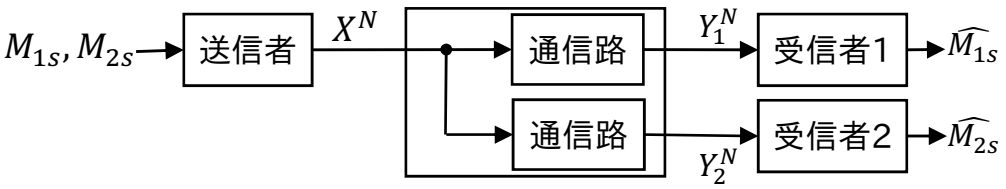

図 2.2: Liu らのモデルによる秘匿メッセージを有する放送型通信路 (BC-CM)

Liu らのモデルによる秘匿メッセージを有する放送型通信路 (BC-CM)[9] は，1 人の送信者が 2 人の受信者に対しそれぞれ独立した秘匿メッセージを送る通信路である (図 2.2 参

照)．BC-CM では，2 人の受信者へのメッセージをそれぞれ他の受信者から秘匿して送ることを目的とする．$k \in \{1,2\}$ で 2 人の受信者を区別し，送信者が受信者へそれぞれ独立した秘匿メッセージ $M_{ks} \in \mathcal{M}_{ks} := \{1, \cdots, 2^{NR_{ks}}\}$ を送る．送信者はメッセージ M_{1s}, M_{2s} を X^N に符号化して送り，受信者 k は Y_k^N を得る．放送型通信路 $W : \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2$ を有限な入出力アルファベット $\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2$ を持つ定常無記憶通信路とする．また，秘匿メッセージ M_{ks} が一様に分布するものと仮定する．$\hat{M}_{ks}$ を受信者 k による M_{ks} の推定値として，受信者 k が M_{ks} の復号を誤る確率を $P_{e,k}^{(N)} = \Pr(\hat{M}_k s \neq M_k s)$ とおく．秘匿メッセージ M_{1s} の受信者 2 への**情報漏洩量**は相互情報量 $I(M_{1s}; Y_2^N)$，秘匿メッセージ M_{2s} の受信者 1 への情報漏洩量は相互情報量 $I(M_{2s}; Y_1^N)$ で測られる．

定義 2 (BC-CM の秘密保持領域)．BC-CM の符号化レート (R_{1s}, R_{2s}) は，$N \to \infty$ としたとき，

$$\liminf_{N\to\infty} \frac{1}{N} \log M_{ks} \geq R_{ks}, \quad P_{e,k}^{(N)} \to 0, \quad I(M_{1s}; Y_2^N) \to 0, \quad I(M_{2s}; Y_1^N) \to 0, \quad (k = 1, 2) \tag{2.6}$$

を満たす符号が存在するときに**強安全性**基準のもとで**達成可能**という．これを満たす符号を単に強安全性を達成するということがある．強安全性が達成可能な符号化レート (R_{1s}, R_{2s}) の集合を**秘密保持領域**という．□

BC-CM の秘密保持領域はまだ明らかにされていない．従来知られている最も広い達成可能なレート領域は，次のように与えられる．

命題 2 (BC-CM の達成可能領域 [9, Theorem 4])．BC-CM の符号化レート (R_{1s}, R_{2s}) の達成可能領域は，V_1, V_2 をマルコフ連鎖 $U - V_1, V_2 - X - Y_1, Y_2$ を満たす補助確率変数 (channel prefixing) とし，U をマルコフ連鎖 $U - V_k - X$ を満たす送信者と受信者で共有する任意の補助確率変数としたとき，

$$0 \leq R_{1s} \leq [I(V_1; Y_1|U) - I(V_1; V_2|U) - I(V_1; Y_2|V_2, U)]^+, \tag{2.7}$$

$$0 \leq R_{2s} \leq [I(V_2; Y_2|U) - I(V_2; V_1|U) - I(V_2; Y_1|V_1, U)]^+ \tag{2.8}$$

となる．□

2.3　Xu らのモデルによる 2 つの秘匿メッセージを有する放送型通信路 (BC-2CM)

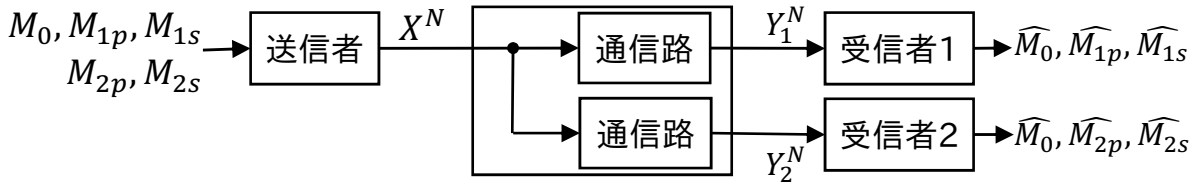

図 2.3: Xu らのモデルによる 2 つの秘匿メッセージを有する放送型通信路 (BC-2CM)

Xu らのモデルによる 2 つの秘匿メッセージを有する放送型通信路 (BC-2CM)[14] は，1 人の送信者が 2 人の受信者に対し，共通メッセージとそれぞれ独立した個別メッセージと秘匿メッセージを送る通信路である (図 2.3 参照)．個別メッセージは他の受信者が得ることができるかは問わず，秘匿メッセージは他の受信者から秘匿することを目的とする．$k \in \{1,2\}$ で 2 人の受信者を区別し，送信者が受信者へ共通メッセージ $M_0 \in \mathcal{M}_0 := \{1, \cdots, 2^{NR_0}\}$ とそれぞれ独立した個別メッセージ $M_{kp} \in \mathcal{M}_{kp} := \{1, \cdots, 2^{NR_{kp}}\}$ と秘匿メッセージ $M_{ks} \in \mathcal{M}_{ks} := \{1, \cdots, 2^{NR_{ks}}\}$ を送る．送信者はメッセージ $M_0, M_{1p}, M_{1s}, M_{2p}, M_{2s}$ を X^N に符号化して送り，受信者 k は Y_k^N を得る．放送型通信路 $W : \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2$ を有限な入出力アルファベット $\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2$ を持つ定常無記憶通信路とする．個別メッセージと秘匿メッセージをあわせたレートを $R_k = R_{kp} + R_{ks}$ とおく．あるメッセージを M_* と表記する．メッセージ M_* は一様に分布するものと仮定する．$\hat{M}_*$ を M_* の推定値として，受信者 k がメッセージの復号を誤る確率を $P_{e,k}^{(N)} = \Pr(\hat{M}_0 \neq M_0 \vee \hat{M}_{kp} \neq M_{kp} \vee \hat{M}_{ks} \neq M_{ks})$ とおく．秘匿メッセージ M_{1s} の受信者 2 への**情報漏洩量**は相互情報量 $I(M_{1s}; Y_2^N)$，秘匿メッセージ M_{2s} の受信者 1 への情報漏洩量は相互情報量 $I(M_{2s}; Y_1^N)$ で測られる．

定義 3 (BC-2CM の秘密保持領域)．BC-2CM の符号化レート $(R_0, R_1, R_2, R_{1s}, R_{2s})$ は，$N \to \infty$ としたとき，

$$\begin{aligned} \liminf_{N\to\infty} \frac{1}{N} \log M_* \geq R_*, \quad P_{e,ks}^{(N)} \to 0, \ (k = 1, 2), \\ I(M_{1s}; Y_2^N) \to 0, \quad I(M_{2s}; Y_1^N) \to 0 \end{aligned} \tag{2.9}$$

を満たす符号が存在するときに**強安全性**基準のもとで**達成可能**という．これをを単に強安全性を達成するということがある．強安全性が達成可能な符号化レート $(R_0, R_1, R_2, R_{1s}, R_{2s})$ の集合を**秘密保持領域**という．　□

BC-2CM の秘密保持領域はまだ明らかにされていない．従来知られている最も広い達成可能なレート領域は，次のように与えられる．

命題 3 (BC-2CM の達成可能領域 [14, Theorem 1])**.** BC-2CM の符号化レート $(R_0, R_1, R_2, R_{1s}, R_{2s})$ の達成可能領域は，U, V_1, V_2 をマルコフ連鎖 $U - V_1V_2 - X - Y_1Y_2$ を満たす補助確率変数としたとき，

$$\begin{aligned}
R_{1s} \leq & R_1, && (2.10)\\
R_{2s} \leq & R_2, && (2.11)\\
R_0 \leq & \min\{I(U;Y_1), I(U;Y_2)\}, && (2.12)\\
R_0 + R_1 \leq & I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\}, && (2.13)\\
R_0 + R_2 \leq & I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\}, && (2.14)\\
R_0 + R_1 + R_2 \leq & I(V_1;Y_1|U) + I(V_2;Y_2|U)\\
& - I(V_1;V_2|U) + \min\{I(U;Y_1), I(U;Y_2)\}, && (2.15)\\
R_{1s} \leq & \left[I(V_1;Y_1|U) - I(V_1;Y_2V_2|U)\right]^+, && (2.16)\\
R_{2s} \leq & \left[I(V_2;Y_2|U) - I(V_2;Y_1V_1|U)\right]^+ && (2.17)
\end{aligned}$$

となる．　□

この命題 3 について，$R_2 = 0$ としたときは BCC の秘密保持領域である命題 1 に，$R_1 = R_{1s}, R_2 = R_{2s}$ としたときは BC-CM の達成可能領域である命題 2 に一致する．

2.4　対称通信路におけるポーラ符号

Arıkan [1] により提案された，ポーラ符号について説明する．符号長 $N = 2^n,\ \ n = 1, 2, \cdots$ として，

$$G_N = {G_2}^{\otimes n} \tag{2.18}$$

という変換行列を定義する．ここで ${G_2}^{\otimes n}$ は，

$$G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

とクロネッカー積 $\otimes$ を用いて，

$$G_2^{\otimes n} = \begin{cases} G_2 \otimes G_2^{\otimes(n-1)} & (n \geq 2) \\ G_2 & (n = 1) \end{cases}$$

と定義する [1]．G_N は ${G_N}^{-1} = G_N$ を満たす．2 元入力対称無記憶通信路 $W : \{0,1\} \to \mathcal{Y}$ の入力を X，出力を Y とする．一様分布に従う 2 元確率変数 $U^N \in \{0,1\}^N$ を用いて，通信路を N 次拡大した通信路 W^N に対する入力を $X^N = U^N G_N$，その出力を Y^N とする．こ

のとき通信路 W^N は，入力 U_i，出力 (Y^N, U^{i-1}) とする通信路 W_i，$i \in [N] := \{1, \cdots, N\}$ に変換される．ここで $U^{i-1} = (U_1, U_2, \cdots, U_{i-1})$ と表す表記法を用いる．通信路 W_i における入出力間の相互情報量を $I(U_i; Y^N, U^{i-1})$ で表す．$|\mathcal{A}|$ により集合 $\mathcal{A}$ の要素数を表すものとすると，任意の $0 < \epsilon < 1$ に対して，

$$\lim_{N\to\infty} \frac{|\{i \in [N] : I(U_i; Y^N U^{i-1}) \in (1-\epsilon, 1]\}|}{N} = I(X;Y),$$
$$\lim_{N\to\infty} \frac{|\{i \in [N] : I(U_i; Y^N U^{i-1}) \in [0, \epsilon)\}|}{N} = 1 - I(X;Y) \tag{2.19}$$

となり，$N \to \infty$ において，1 に漸近する $I(U_i; Y^N, U^{i-1})$ と，0 に漸近する $I(U_i; Y^N, U^{i-1})$ に二分される．このような現象を**通信路分極** (*channel polarization*) と呼ぶ．$I(U_i; Y^N, U^{i-1}) \in [0, \epsilon)$ となる位置は**凍結ビット**と呼ばれる固定したビットを，それ以外の位置にメッセージビットを割り当て，u^N を変換行列 G_N により符号化する．この通信路符号を，**ポーラ符号**と呼ぶ．また，計算複雑度は $O(N \log N)$ となる．

2.5　非対称通信路におけるポーラ符号

Honda と Yamamoto [8] によって提案された，非対称通信路において通信路容量を達成するポーラ符号について説明する．S を 2 元確率変数，V を有限アルファベット $\mathcal{V}$ に値をとる確率変数とする．確率変数の組 (S, V) による同時確率分布を P_{SV} として，Bhattacharyya パラメータを次のように定義する．

$$Z(S|V) = 2 \sum_v P_V(v) \sqrt{P_{S|V}(0|v) P_{S|V}(1|v)}. \tag{2.20}$$

2 元入力の無記憶通信路において，入力 X^N に対して $U^N = X^N {G_N}^{-1} = X^N G_N$ とし，その出力を Y^N とする．$\delta_N = 2^{-N^\beta}$，$\beta \in (0, \frac{1}{2})$ とおき，インデックス集合 $[N]$ について，[10, Section III] で導入された次のインデックス集合を考える．

$$\begin{aligned}
\mathcal{H}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \geq 1 - \delta_N\}, \\
\mathcal{L}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \leq \delta_N\}, \\
\mathcal{H}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}Y^N) \geq 1 - \delta_N\}, \\
\mathcal{L}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}Y^N) \leq \delta_N\}.
\end{aligned} \tag{2.21}$$

この Bhattacharyya パラメータについて，$Z(U_i|U^{i-1}) \geq 1 - \delta_N$ のときに U_i は U^{i-1} からは確率 $1 - \delta_N$ 以上で**復号不可能**であり，$Z(U_i|U^{i-1}) \leq \delta_N$ のときに U_i は U^{i-1} から確率 $1 - \delta_N$ 以上で**復号可能**であることが示される．また，上記の位置集合に対し，

$$\mathcal{H}_{X|Y} \subseteq \mathcal{H}_X, \tag{2.22}$$
$$\mathcal{L}_X \subseteq \mathcal{L}_{X|Y} \tag{2.23}$$

の関係が成り立つ．さらに，これらの集合の 1 記号当たりのサイズについて，

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_X| &= H(X),\\ \lim_{N\to\infty}\frac{1}{N}|\mathcal{L}_X| &= 1-H(X),\\ \lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{X|Y}| &= H(X|Y),\\ \lim_{N\to\infty}\frac{1}{N}|\mathcal{L}_{X|Y}| &= 1-H(X|Y)\end{aligned} \tag{2.24}$$

が成立する．ここで $H(A)$ は A のエントロピーを，$H(A|B)$ は B を条件とする A の条件付エントロピーを表す．式 (2.21) を用いて，インデックス集合 $[N]$ を次の 3 つの集合に分割する．

$$\begin{aligned}\mathcal{J} &= \mathcal{H}_X \cap \mathcal{L}_{X|Y},\\ \mathcal{F}_r &= \mathcal{H}_X \cap \mathcal{L}^c_{X|Y},\\ \mathcal{F}_d &= \mathcal{H}^c_X.\end{aligned} \tag{2.25}$$

ここで $\mathcal{A}^c$ は集合 $\mathcal{A}$ の補集合を表す．$\mathcal{J}$ を情報ビット集合，$\mathcal{F}_r$ と $\mathcal{F}_d$ を凍結ビット集合と呼ぶ．対称通信路の場合，$\mathcal{F}_d$ は空集合となる．受信者が Y^N を観測したとき，インデックス i の小さい U_i から，Y^N と U^{i-1} を用いて復号すると考える．このとき，$\mathcal{J}$ に含まれる U_i は，受信者にとって復号可能であるので，メッセージとして利用できる．また，$\mathcal{F}_r$ に含まれる U_i は，受信者にとって復号不可能となるので，ランダムビットとして送受信者間で共有する．$\mathcal{F}_d$ に含まれる U_i は，$U^{i-1}=u^{i-1}$ から次式を用いてインデックス i の小さい順に決定する．

$$u_i = \arg\max_{u\in\{0,1\}} P_{U_i|U^{i-1}}(u|u^{i-1}). \tag{2.26}$$

式 (2.24) より，[8, Theorem 1] の結果と等価である次式が求まる．

$$\lim_{n\to\infty}\frac{1}{N}|\mathcal{J}| = I(X;Y). \tag{2.27}$$

よって，P_X を通信路容量 $C=\max_{P_X} I(X;Y)$ を達成する確率分布に選べば，受信者の誤り確率 P_e は，

$$P_e \le \sum_{i\in\mathcal{J}} Z(U_{1,i}|U_1^{i-1},Y^N) = O(N2^{-N^\beta}) \tag{2.28}$$

となり，符号化レートが通信路容量を達成する．また，計算複雑度は $O(N\log N)$ となる．

第 3 章

BC-2CMにおけるポーラ符号の構成

3.1　ポーラ符号の構成

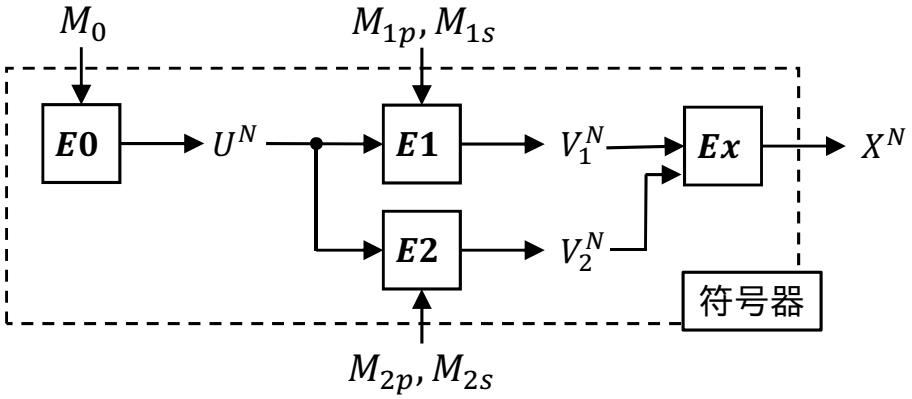

図 3.1: BC-2CM において共通メッセージを上限まで送るときの仮想符号器

図3.1のような仮想符号器を考える．仮想符号器 $E0$ により M_0 から $U^N = (U_1, U_2, \cdots, U_N)$ を生成し，仮想符号器 E_k において U^N と M_{kp}, M_{ks} から $V_k^N = (V_{k,1}, V_{k,2}, \cdots, V_{k,N})$ を生成する．$V_{1,i}, V_{2,i}$ のもとで仮想符号器 Ex では $P_{X|V_1V_2}$ により確率的に入力 X_i を生成する．U^N と V_k^N をポーラ符号により構成し，V_k^N に対し $T_k^N = V_k^N {G_N}^{-1} = V_k^N G_N$ とし，U^N に対し $Q_k^N = U^N {G_N}^{-1} = U^N G_N$ とする．一般性を失うことなく，式 (2.16), (2.17) の右辺が正の値をとる確率変数を定める．以下，式 (2.12) が等号を満たすもとで，式 (2.13) が等号を満たす例，つまり共有メッセージを上限まで送った上で，受信者 1 への個別メッセージと秘匿メッセージを上限まで送る例を考える．

3.1.1　共通メッセージの送信

共通メッセージを符号化する仮想符号器 $E0$ を考える．$\delta_N = 2^{-N^\beta},\ \beta \in (0, \frac{1}{2})$ とし，N 個の確率変数の組 Q^N, Y_1^N, Y_2^N を用いて，次のインデックス集合を定義する．

$$\begin{aligned}\mathcal{H}_U &= \{i \in [N] : Z(Q_i|Q^{i-1}) \geq 1 - \delta_N\},\\ \mathcal{L}_{U|Y_1} &= \{i \in [N] : Z(Q_i|Q^{i-1}Y_1^N) \leq \delta_N\},\\ \mathcal{L}_{U|Y_2} &= \{i \in [N] : Z(Q_i|Q^{i-1}Y_2^N) \leq \delta_N\}.\end{aligned} \tag{3.1}$$

さらに，これらの集合の 1 記号当たりのサイズについて，

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{N}|\mathcal{H}_U| &= H(U),\\ \lim_{N\to\infty} \frac{1}{N}|\mathcal{L}_{U|Y_1}| &= 1 - H(U|Y_1),\\ \lim_{N\to\infty} \frac{1}{N}|\mathcal{L}_{U|Y_2}| &= 1 - H(U|Y_2)\end{aligned} \tag{3.2}$$

が成立する．式 (3.1) を用いて，インデックス集合 $[N]$ を次の 4 つの集合に分割する．

$$\begin{aligned}\mathcal{A} &= \mathcal{H}_U \cap \mathcal{L}_{U|Y_1} \cap \mathcal{L}_{U|Y_2},\\ \mathcal{B} &= \mathcal{H}_U \cap \mathcal{L}_{U|Y_1} \cap \mathcal{L}^c_{U|Y_2},\\ \mathcal{C} &= \mathcal{H}_U \cap \mathcal{L}^c_{U|Y_1} \cap \mathcal{L}_{U|Y_2},\\ \mathcal{F} &= \mathcal{H}^c_U \cup \left(\mathcal{L}^c_{U|Y_1} \cap \mathcal{L}^c_{U|Y_2}\right).\end{aligned} \tag{3.3}$$

受信者 k がそれぞれ Q^N を復号するとき，インデックス i の小さい Q_i から Q^{i-1} と Y_k^N を用いて逐次的に復号すると想定する．このとき，$\mathcal{F}$ を式 (3.4) の 2 つの集合に分割して，各インデックス集合における Q_i の復号可能性を見る．$\mathcal{F}_d$ は Q^{i-1} から復号不可能ではないものとなり，その他は表 3.1 に示す．

$$\begin{aligned}\mathcal{F}_r &= \mathcal{H}_U \cap \mathcal{L}^c_{U|Y_1} \cap \mathcal{L}^c_{U|Y_2},\\ \mathcal{F}_d &= \mathcal{H}^c_U.\end{aligned} \tag{3.4}$$

	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{F}_r$
Q^{i-1}, Y_1^N	復号可能	復号可能	復号可能ではない	復号可能ではない
Q^{i-1}, Y_2^N	復号可能	復号可能ではない	復号可能	復号可能ではない

表 3.1: 各インデックス集合における Q_i の復号可能性

式 (3.3), (3.2) より

$$\begin{aligned}\lim_{N\to\infty} \frac{1}{N}|\mathcal{A} \cup \mathcal{B}| &= I(U; Y_1),\\ \lim_{N\to\infty} \frac{1}{N}|\mathcal{A} \cup \mathcal{C}| &= I(U; Y_2)\end{aligned} \tag{3.5}$$

となる．よって，$I(U;Y_1) \leq I(U;Y_2)$ であるとき，$|\mathcal{B}| \leq |\mathcal{C}|$ であり，$\mathcal{C}$ を $|\mathcal{C}'| = |\mathcal{B}|$ を満たす $\mathcal{C}'$ と $\mathcal{D} = \mathcal{C} \backslash \mathcal{C}'$ に分けることができる．$I(U;Y_1) > I(U;Y_2)$ であるときも同様に考えることができる．

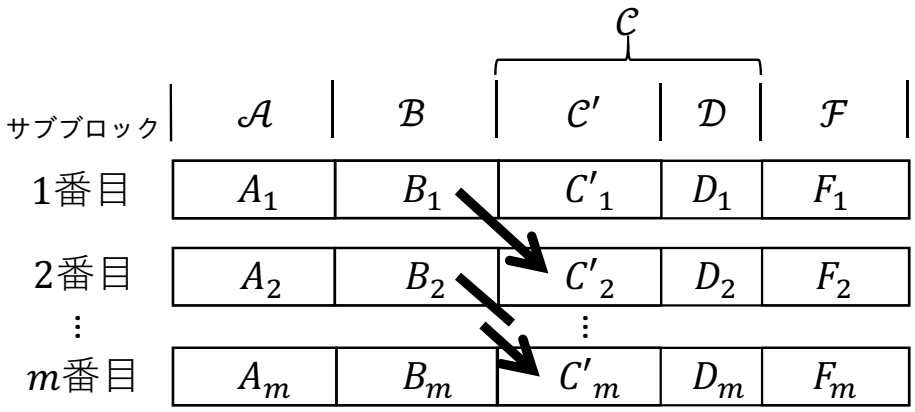

図 3.2: Q^N に対するポーラ符号の構成

提案する構成法では，m 個のサブブロックを連鎖させてポーラ符号を構成する．サブブロックは長さ N のポーラ符号を用いる．j 番目のサブブロックにおいて，A_j は $i \in \mathcal{A}$ となる Q_i の集合を表す．B_j から F_j も同様に定義する．図 3.2 のように，$1 \leq j < m$ に対し，j 番目のサブブロックにおける B_j を $j+1$ 番目のサブブロックにおける C'_{j+1} にコピーし，連鎖構造を作る．共通メッセージを A^m と B^{m-1} に分割して割り当て[1]，m 個のサブブロック上で $m|\mathcal{A}| + (m-1)|\mathcal{B}|$ ビットの共通メッセージを送る．D^m と C'_1, B_m は，一様なランダムビット (凍結ビット) を q_i として受信者 1,2 で共有する．F^m については，式 (3.4) の 2 つの集合に分け，$i \in \mathcal{F}_r$ では一様なランダムビット (凍結ビット) を q_i として受信者 1,2 で共有し，$i \in \mathcal{F}_d$ では次式を用いて q_i の値を決定する．

$$q_i = \arg \max_{q \in \{0,1\}} P_{Q_i|Q^{i-1}}(q|q^{i-1}). \tag{3.6}$$

3.1.2　個別及び秘匿メッセージの送信

以下では，受信者 1 に送るメッセージに関して説明する．受信者 2 に送るメッセージに関しては，ユーザーを表すインデックスを入れ替えることでほぼ同様に考えることができる．$\delta_N = 2^{-N^\beta}$，$\beta \in (0, \frac{1}{2})$ とし，N 個の確率変数の組 $T_1^N = (T_{1,1}, T_{1,2}, \cdots, T_{1,N})$ と

[1] A^m の表記により $(A_1, A_2, \cdots, A_m)$ を表す．

T_2^N, Y_1^N, Y_2^N, U^N を用いて，次のインデックス集合を定義する．

$$\begin{aligned}
\mathcal{H}_{V_1|U} &= \{i \in [N] : Z(T_{1,i}|T_1^{i-1}U^N) \geq 1-\delta_N\},\\
\mathcal{L}_{V_1|Y_1U} &= \{i \in [N] : Z(T_{1,i}|T_1^{i-1}Y_1^NU^N) \leq \delta_N\},\\
\mathcal{H}_{V_1|V_2U} &= \{i \in [N] : Z(T_{1,i}|T_1^{i-1}T_2^NU^N) \geq 1-\delta_N\},\\
\mathcal{H}_{V_1|V_2Y_2U} &= \{i \in [N] : Z(T_{1,i}|T_1^{i-1}T_2^NY_2^NU^N) \geq 1-\delta_N\}.
\end{aligned} \tag{3.7}$$

また，上記の位置集合に対し，

$$\mathcal{H}_{V_1|V_2Y_2U} \subseteq \mathcal{H}_{V_1|V_2U} \subseteq \mathcal{H}_{V_1|U} \tag{3.8}$$

の関係が成り立つ．さらに，これらの集合の 1 記号当たりのサイズについて，

$$\begin{aligned}
\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{V_1|U}| &= H(V_1|U),\\
\lim_{N\to\infty}\frac{1}{N}|\mathcal{L}_{V_1|Y_1U}| &= 1-H(V_1|Y_1U),\\
\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{V_1|V_2U}| &= H(V_1|V_2U),\\
\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{V_1|V_2Y_2U}| &= H(V_1|V_2Y_2U)
\end{aligned} \tag{3.9}$$

が成立する．式 (3.7) を用いて，インデックス集合 $[N]$ を次の 6 つの集合に分割する．

$$\begin{aligned}
\mathcal{A} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U}\\
&= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|V_2U},\\
\mathcal{B} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U},\\
\mathcal{C} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}_{V_1|V_2Y_2U}\\
&= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2Y_2U},\\
\mathcal{D} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U}\\
&= \mathcal{H}_{V_1|U} \cap \mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|V_2U},\\
\mathcal{E} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U},\\
\mathcal{F} &= \mathcal{H}^c_{V_1|U} \cup \left(\mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}_{V_1|V_2Y_2U}\right)\\
&= \mathcal{H}^c_{V_1|U} \cup \left(\mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2Y_2U}\right).
\end{aligned} \tag{3.10}$$

文献 [12] では，$\mathcal{H}^c_{V_1|V_2U}$ の部分に $\mathcal{L}_{V_1|V_2U} = \{i \in [N] : Z(T_{1,i}|T_1^{i-1}, T_2^N, U^N) \leq \delta_N\}$ が，$\mathcal{H}^c_{V_1|V_2Y_2U}$ の部分に $\mathcal{L}_{V_1|V_2Y_2U} = \{i \in [N] : Z(T_{1,i}|T_1^{i-1}, T_2^NY_2^NU^N) \leq \delta_N\}$ が用いられている．本稿では，秘匿メッセージの秘匿性を強めるために，Şaşoğlu と Vardy [11] による盗聴通信路に対するポーラ符号の構成を参考に，$\mathcal{H}_{V_1|V_2U}, \mathcal{H}_{V_1|V_2Y_2U}$ を用いる．受信者 1,2 がそれぞれ T_1^N を復号しようとするとき，インデックス i の小さい $T_{1,i}$ から，受信者 1 は Y_1^N

と T_1^{i-1} を用いて，受信者 2 は Y_2^N, T_2^N と T_1^{i-1} を用いて復号すると想定する．このとき，$\mathcal{F}$ を式 (3.11) の 2 つの集合に分割して，各インデックス集合における $U_{1,i}$ の復号可能性を見る．$\mathcal{F}_d$ は T_1^{i-1} から復号不可能ではないものとなり，その他は表 3.2 に示す．

$$\begin{aligned}\mathcal{F}_r &= \mathcal{H}_{V_1|U} \cap \mathcal{L}^{\mathrm{c}}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2Y_2U},\\ \mathcal{F}_d &= \mathcal{H}^{\mathrm{c}}_{V_1|U}.\end{aligned} \tag{3.11}$$

	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$
T_1^{i-1}, Y_1^N, U^N	復号可能	復号可能	復号可能
T_1^{i-1}, T_2^N, U^N	復号不可能ではない	復号不可能	復号不可能
$T_1^{i-1}, T_2^N, Y_2^N, U^N$	復号不可能ではない	復号不可能ではない	復号不可能
	$\mathcal{D}$	$\mathcal{E}$	$\mathcal{F}_r$
T_1^{i-1}, Y_1^N, U^N	復号可能ではない	復号可能ではない	復号可能ではない
T_1^{i-1}, T_2^N, U^N	復号不可能ではない	復号不可能	復号不可能
$T_1^{i-1}, T_2^N, Y_2^N, U^N$	復号不可能ではない	復号不可能ではない	復号不可能

表 3.2: 各インデックス集合における $T_{1,i}$ の復号可能性

一般性を失うことなく，$|\mathcal{C}| > |\mathcal{D}| + |\mathcal{E}|$ と仮定する ($|\mathcal{C}| \leq |\mathcal{D}| + |\mathcal{E}|$ のとき，

$$R_{1s} \leq [I(V_1; Y_1|U) - I(V_1; Y_2V_2|U)]^+ = 0$$

となる)．$|\mathcal{C}_1| = |\mathcal{D}|$，$|\mathcal{C}_2| = |\mathcal{E}|$，$\mathcal{C}_1, \mathcal{C}_2 \subset \mathcal{C}$，$\mathcal{C}_1 \cap \mathcal{C}_2 = \emptyset$ (空集合) となる $\mathcal{C}_1, \mathcal{C}_2$ を定める．また，$\mathcal{S} = \mathcal{C} \backslash (\mathcal{C}_1 \cup \mathcal{C}_2)$ を定義する．

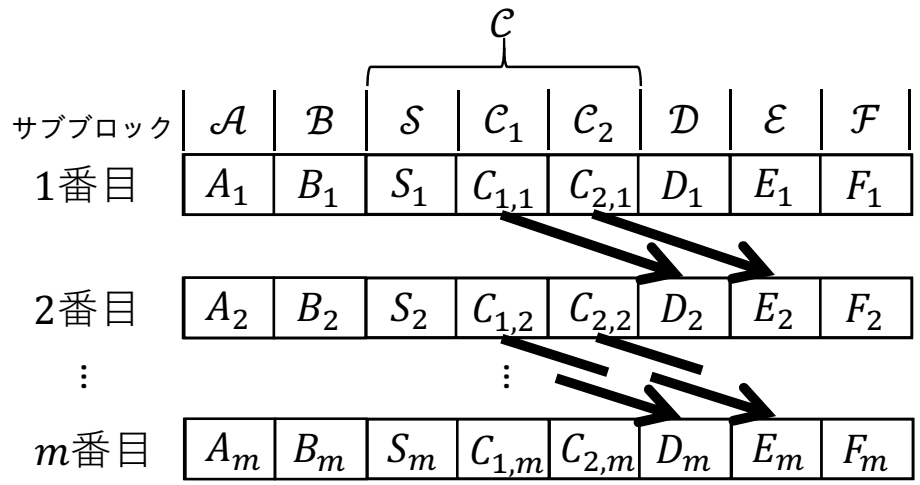

図 3.3: T_k^N に対するポーラ符号の構成

提案する構成法では，m 個のサブブロックを連鎖させてポーラ符号を構成する．サブブロックは，長さ N のポーラ符号を用いる．j 番目のサブブロックにおいて，A_j は $i \in \mathcal{A}$ となる $T_{1,i}$ の集合を表す．B_j から F_j も同様に定義する．図 3.3 のように，$1 \leq j < m$ に対し，j 番目のサブブロックにおける $C_{1,j}, C_{2,j}$ を $j+1$ 番目のサブブロックにおける $C_{1,j+1}, C_{2,j+1}$ にコピーし，連鎖構造を作る．秘匿メッセージを S^{m-1} に分割して割り当て，m 個のサブブロック上で $(m-1)|\mathcal{S}|$ ビットの秘匿メッセージを送る．個別メッセージを $A^m, B^m, C_1^{m-1}, C_2^{m-1}$ に分割して割り当て，m 個のサブブロック上で $m(|\mathcal{A}| + |\mathcal{B}|) + (m-1)(|\mathcal{C}_1| + |\mathcal{C}_1|)$ ビットの個別メッセージを送る．$D_1, E_1, S_m, C_{1,m}, C_{2,m}$ は，一様なランダムビット (凍結ビット) を $t_{1,i}$ として受信者 1,2 で共有する．F^m については，式 (3.11) の 2 つの集合に分け，$i \in \mathcal{F}_r$ では一様なランダムビット (凍結ビット) を $t_{1,i}$ として受信者 1,2 で共有し，$i \in \mathcal{F}_d$ では次式を用いて $t_{1,i}$ の値を決定する．

$$t_{1,i} = \arg \max_{t \in \{0,1\}} P_{T_{1,i}|T_1^{i-1}}(t|t^{i-1}). \tag{3.12}$$

受信者 2 においては，A^m, D^m の部分の $T_{2,i}$ が T_2^{i-1}, T_1^N, U^N より復号され得るので，個別メッセージを B^m, C_2^{m-1} に分割して割り当て，m 個のサブブロック上で $m|\mathcal{B}| + (m-1)|\mathcal{C}_1|$ ビットの個別メッセージを送ることになる．

3.2　性能評価

本節では，構成したポーラ符号の性能を示す．以下の補題は有用である．

補題 1 ([2, Proposition 2])**.** 確率変数の組 (X, Y) に対して，次の不等式が成立する．

$$Z(X|Y)^2 \leq H(X|Y). \tag{3.13}$$

X が Y によって決定されるとき又は Y を条件とした X が $p = \frac{1}{2}$ のベルヌーイ分布に従うとき，等式が成立する．　□

提案構成法により構成されるポーラ符号の性能を，以下の定理によって示す．

定理 1. 提案構成法のポーラ符号は，強安全性の基準のもとで，式 (2.10)–(2.17) で与えられる達成可能領域内の任意のレート $(R_0, R_1, R_2, R_{1s}, R_{2s})$ を達成する．　□

(証明). 各性能の評価を以下に示す．

3.2.1　符号化レート

共通メッセージ M_0 に関する符号化レート $R_{0(N,m)}$ は，$I(U;Y_1) \leq I(U;Y_2)$ であるとき，

$$R_{0(N,m)} = \frac{m|\mathcal{A}| + (m-1)|\mathcal{B}|}{mN} \tag{3.14}$$

となる．また，明らかに

$$\frac{m-1}{m}\cdot\frac{|\mathcal{A}|+|\mathcal{B}|}{N}\leq R_{0(N,m)}\leq\frac{|\mathcal{A}|+|\mathcal{B}|}{N} \tag{3.15}$$

という関係が成り立つので，N を十分に大きくしたとき，式 (3.5) より

$$\frac{m-1}{m}I(U;Y_1)\leq R_{0(N,m)}\leq I(U;Y_1) \tag{3.16}$$

となり，

$$\lim_{m\to\infty}\lim_{N\to\infty}R_{0(N,m)}=I(U;Y_1) \tag{3.17}$$

を得る．$I(U;Y_1)>I(U;Y_2)$ であるときも同様にして

$$\lim_{m\to\infty}\lim_{N\to\infty}R_{0(N,m)}=I(U;Y_2) \tag{3.18}$$

を得るので，共通メッセージ M_0 に関する符号化レート $R_{0(N,m)}$ は次のようになる．

$$\lim_{m\to\infty}\lim_{N\to\infty}R_{0(N,m)}=\min\{I(U;Y_1),I(U;Y_2)\}. \tag{3.19}$$

共通メッセージ M_0 を上限まで送ったときの受信者 1 への個別メッセージ M_{1p} と秘匿メッセージ M_{1s} に関する符号化レート $R_{1(N,m)}$ は

$$R_{1(N,m)}=\frac{m(|\mathcal{A}|+|\mathcal{B}|)+(m-1)|\mathcal{C}|}{mN} \tag{3.20}$$

となる．また，明らかに

$$\frac{m-1}{m}\cdot\frac{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{C}|}{N}\leq R_{1(N,m)}\leq\frac{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{C}|}{N} \tag{3.21}$$

という関係が成り立つ．$\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ について

$$\begin{aligned}\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}&=(\mathcal{A}\cup\mathcal{B})\cup\mathcal{C}\\&=\left(\mathcal{H}_{V_1U}\cap\mathcal{L}_{V_1|Y_1U}\cap\left(\mathcal{H}^c_{V_1|V_2U}\cup\left(\mathcal{H}_{V_1|V_2U}\cap\mathcal{H}^c_{V_1|V_2Y_2U}\right)\right)\right)\cup\mathcal{C}\\&=\left(\mathcal{H}_{V_1U}\cap\mathcal{L}_{V_1|Y_1U}\cap\mathcal{H}^c_{V_1|V_2Y_2U}\right)\cup\mathcal{C}\\&=\mathcal{H}_{V_1U}\cap\mathcal{L}_{V_1|Y_1U}\cap\left(\mathcal{H}^c_{V_1|V_2Y_2U}\cup\mathcal{H}_{V_1|V_2Y_2U}\right)\\&=\mathcal{H}_{V_1U}\cap\mathcal{L}_{V_1|Y_1U}\end{aligned} \tag{3.22}$$

と変形ができ，式 (3.9) より

$$\begin{aligned}\lim_{N\to\infty}\frac{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{C}|}{N}&=H(V_1|U)-(1-(1-H(V_1|Y_1U)))\\&=H(V_1|U)-H(V_1|Y_1U)\\&=I(V_1;Y_1|U)\end{aligned} \tag{3.23}$$

が成り立つ．よって，N を十分に大きくしたとき，

$$\frac{m-1}{m}I(V_1;Y_1|U) \leq R_{1(N,m)} \leq I(V_1;Y_1|U) \tag{3.24}$$

となるので，

$$\lim_{m\to\infty}\lim_{N\to\infty} R_{1(N,m)} = I(V_1;Y_1|U) \tag{3.25}$$

を得る．

共通メッセージ M_0 を上限まで送るもとで，受信者 1 が個別メッセージ M_{1p} を上限まで送ったときの，受信者 2 への個別メッセージ M_{2p} と秘匿メッセージ M_{2s} に関する符号化レート $R_{2(N,m)}$ は

$$R_{2(N,m)} = \frac{m|\mathcal{B}| + (m-1)(|\mathcal{C}| - |\mathcal{C}_1|)}{mN} \tag{3.26}$$

となる．$|\mathcal{C}_1| = |\mathcal{D}|, |\mathcal{C}_2| = |\mathcal{E}|$ より

$$R_{2(N,m)} = \frac{m|\mathcal{B}| + (m-1)(|C| - |\mathcal{D}|)}{mN} \tag{3.27}$$

となる．また，明らかに

$$\frac{m-1}{m}\cdot\frac{|\mathcal{B}| + |\mathcal{C}| - |\mathcal{D}|}{N} \leq R_{1(N,m)} \leq \frac{|\mathcal{B}| + |\mathcal{C}| + |\mathcal{D}|}{N} \tag{3.28}$$

という関係が成り立つ．そして，

$$|\mathcal{B}| + |\mathcal{C}| - |\mathcal{D}| = |\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}| - (|\mathcal{A}| + |\mathcal{D}|) \tag{3.29}$$

となる．$\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ について，式 (3.23) を受信者 2 への送信の形に変えると，

$$\lim_{N\to\infty}\frac{|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|}{N} = I(V_2;Y_2|U) \tag{3.30}$$

となる．$\mathcal{A}\cup\mathcal{D}$ について，

$$\mathcal{A}\cup\mathcal{D} = \mathcal{H}_{V_2|U}\cap\mathcal{H}^c_{V_2|V_1U} \tag{3.31}$$

と変形でき，式 (3.9) より

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}|\mathcal{A}\cup\mathcal{D}| &= H(V_2|U) - H(V_2|V_1U)\\ &= I(V_1;V_2|U)\end{aligned} \tag{3.32}$$

が成り立つ．式 (3.30)(3.32) より，N を十分に大きくしたとき，

$$\frac{m-1}{m}\left(I(V_2;Y_2|U) - I(V_1;V_2|U)\right) \leq R_{1(N,m)} \leq I(V_2;Y_2|U) - I(V_1;V_2|U) \tag{3.33}$$

となるので，

$$\lim_{m\to\infty}\lim_{N\to\infty} R_{2(N,m)} = I(V_2;Y_2|U) - I(V_1;V_2|U) \tag{3.34}$$

を得る．

秘匿メッセージ M_{1s} に関する符号化レート $R_{1s(N,m)}$ は

$$R_{1s(N,m)} = \frac{(m-1)|\mathcal{S}|}{mN} \tag{3.35}$$

となる．$|\mathcal{S}|$ について，

$$\begin{aligned} |\mathcal{S}| &= |\mathcal{C}| - |\mathcal{C}_1| - |\mathcal{C}_2| \\ &= (|\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}|) - (|\mathcal{A}| + |\mathcal{D}|) - (|\mathcal{B}| + |\mathcal{E}|) \\ &= |\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}| - |\mathcal{A} \cup \mathcal{D}| - |\mathcal{B} \cup \mathcal{E}| \end{aligned} \tag{3.36}$$

となる．また，$\mathcal{B} \cup \mathcal{E}$ について，

$$\begin{aligned} \mathcal{B} \cup \mathcal{E} &= \mathcal{H}_{V_1|U} \cap \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U} \\ &= \mathcal{H}_{V_1|V_2U} \cap \mathcal{H}^c_{V_1|V_2Y_2U} \end{aligned} \tag{3.37}$$

と変形でき，式 (3.9) より

$$\begin{aligned} \lim_{N\to\infty} \frac{1}{N}|\mathcal{B} \cup \mathcal{E}| &= H(V_1|V_2U) - H(V_1|V_2Y_2U) \\ &= I(V_1; Y_2|V_2U) \end{aligned} \tag{3.38}$$

が成り立つ．$\mathcal{A} \cup \mathcal{D}$ についての式 (3.32) は，受信者 1 への送信の形と受信者 2 への送信の形で，同じ値となる．式 (3.23)(3.32)(3.38) より，N を十分に大きくしたとき，

$$\begin{aligned} \lim_{N\to\infty} \frac{|\mathcal{S}|}{N} &= I(V_1; Y_1U) - I(V_1; V_2|U) - I(V_1; Y_2|V_2U) \\ &= I(V_1; Y_1|U) - I(V_1; Y_2V_2|U) \end{aligned} \tag{3.39}$$

となるので，

$$\lim_{m\to\infty} \lim_{N\to\infty} R_{1s(N,m)} = I(V_1; Y_1|U) - I(V_1; Y_2V_2|U) \tag{3.40}$$

が得られる．秘匿メッセージ M_{2s} に関する符号化レート $R_{2s(N,m)}$ についても同様に次式が成り立つ．

$$\lim_{m\to\infty} \lim_{N\to\infty} R_{2s(N,m)} = I(V_2; Y_2|U) - I(V_2; Y_1V_1|U). \tag{3.41}$$

$R_{0(N,m)} + R_{1(N,m)}$ について，式 (3.19)(3.25) より，

$$\lim_{m\to\infty} \lim_{N\to\infty} R_{0(N,m)} + R_{1(N,m)} = I(V_1; Y_1|U) + \min\{I(U; Y_1), I(U; Y_2)\} \tag{3.42}$$

を導くことができ，$R_{0(N,m)} + R_{1(N,m)} + R_{2(N,m)}$ について，式 (3.19)(3.25)(3.34) より，

$$\begin{aligned} \lim_{m\to\infty} \lim_{N\to\infty} R_{0(N,m)} + R_{1(N,m)} + R_{2(N,m)} =& I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_1; V_2|U) + \min\{I(U; Y_1), I(U; Y_2)\} \end{aligned} \tag{3.43}$$

を導くことができる．よって，$N \to \infty, m \to \infty$ としたとき，レート $(R_0, R_1, R_2, R_{1s}, R_{2s})$ は命題 3 で与えられる達成可能なレート領域の境界点である．

他の境界点について，受信者 2 への個別メッセージと秘匿メッセージを上限まで送ったときにも同様にして達成できる．また，共通メッセージを上限まで送らない場合は，共通メッセージの送信時に個別メッセージの一部を送信することで達成することができる．

3.2.2　誤り確率

この 3.2.2 節において，受信者 k が受信したサブブロック j について $Y_{k,j}$ と書き表す．

受信者 1 に対する誤り確率 $P_{e,1}^{(N)}$ は，ユニオン上界より，

$$\begin{aligned} P_{e,1}^{(N)} &= \Pr\left[(\hat{Q}^N)^m \neq (Q^N)^m \vee (\hat{T}_1^N)^m \neq (T_1^N)^m\right] \\ &\leq \sum_{j=1}^{m} \Pr\left[(\hat{Q}^N)_j \neq (Q^N)_j\right] + \sum_{j=1}^{m} \Pr\left[(\hat{T}_1^N)_j \neq (T_1^N)_j\right] \end{aligned} \tag{3.44}$$

となる．ここで，$(\hat{Q}^N)^m, (\hat{T}_1^N)^m$ は，それぞれ $(Q^N)^m, (T_1^N)^m$ の受信者 1 による推定値を表す．Q^N において $\mathcal{A} \cup \mathcal{B} \subseteq \mathcal{L}_{U|Y_1}$，$T_1^N$ において $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C} \subseteq \mathcal{L}_{V_1|Y_1U}$ の関係から，

$$\begin{aligned} \Pr\left[(\hat{Q}^N)_j \neq (Q^N)_j\right] &\leq \sum_{i \in A \cup B} Z(Q_i|Q^{i-1}Y_{1,j}) \\ &= O(N2^{-N^\beta}), \\ \Pr\left[(\hat{T}_1^N)_j \neq (T_1^N)_j\right] &\leq \sum_{i \in A \cup B \cup C} Z(T_{1,i}|T_1^{i-1}Y_{1,j}(U^N)^m) \\ &= O(N2^{-N^\beta}) \end{aligned} \tag{3.45}$$

のように上から抑えられる．よって，次式が成立する．

$$P_{e,1}^{(N)} \leq 2mO(N2^{-N^\beta}). \tag{3.46}$$

受信者 2 に対する誤り確率 $P_{e,2}^{(N)}$ も同様にして，

$$P_{e,2}^{(N)} \leq 2mO(N2^{-N^\beta}) \tag{3.47}$$

となる．

3.2.3　情報漏洩量

この 3.2.3 節において，受信者 k が受信した全てのサブブロック $(Y_k^N)^m$ を Y_k^m と書き表し，受信したサブブロック j について $Y_{k,j}$ と書き表す．

受信者 2 に受信者 1 への秘匿メッセージ M_{1s} が伝わる情報漏洩量 $I(M_{1s};Y_2^m)$ について，

$$\begin{aligned} I(M_{1s};Y_2^m) &\le I(S^m;Y_2^m) \\ I(S^m;Y_2^m) &\le I(S^mC_{1,m}C_{2,m};Y_2^m) \end{aligned} \tag{3.48}$$

の関係を利用して $I(S^mC_{1,m}C_{2,m};Y_{2,0}Y_2^m)$ を上から評価する．マルコフ連鎖

$$S^{m-1} - S_mC_{1,m}C_{2,m} - Y_{2,m} \tag{3.49}$$

$$S_mC_{1,m}C_{2,m} - S^{m-1}C_{1,m-1}C_{2,m-1} - Y_2^{m-1} \tag{3.50}$$

が成立しているので，

$$I(S^mC_{1,m}C_{2,m};Y_2^m) = I(S^mC_{1,m}C_{2,m};Y_{2,m}) + I(S^mC_{1,m}C_{2,m};Y_2^{m-1}|Y_{2,m}) \tag{3.51}$$

$$= I(S_mC_{1,m}C_{2,m};Y_{2,m}) + I(S^mC_{1,m}C_{2,m};Y_2^{m-1}|Y_{2,m}) \tag{3.52}$$

$$\begin{aligned} \le & I(S_mC_{1,m}C_{2,m};Y_{2,m}) + I(S^mC_{1,m}C_{2,m};Y_2^{m-1}|Y_{2,m}) \\ & + I(Y_{2,m};Y_2^{m-1}) + I(C_{1,m-1}C_{2,m-1};Y_2^{m-1}|S^mC_{1,m}C_{2,m}Y_{2,m}) \end{aligned} \tag{3.53}$$

$$\begin{aligned} = & I(S_mC_{1,m}C_{2,m};Y_{2,m}) + I(S^mC_{1,m}C_{2,m}Y_{2,m};Y_2^{m-1}) \\ & + I(C_{1,m-1}C_{2,m-1};Y_2^{m-1}|S^mC_{1,m}C_{2,m}Y_{2,m}) \end{aligned} \tag{3.54}$$

$$= I(S_mC_{1,m}C_{2,m};Y_{2,m}) + I(S^mC_{1,m-1}C_{2,m-1}C_{1,m}C_{2,m}Y_{2,m};Y_2^{m-1}) \tag{3.55}$$

$$= I(S_mC_{1,m}C_{2,m};Y_{2,m}) + I(S^{m-1}C_{1,m-1}C_{2,m-1};Y_2^{m-1}) \tag{3.56}$$

と評価できる．式 (3.51),(3.54),(3.55) の等号は相互情報量のチェインルール，式 (3.52) の等号は式 (3.49) のマルコフ連鎖，式 (3.56) の等号は式 (3.50) のマルコフ連鎖により成り立つ．これを $I(S_1C_{1,1}C_{2,1};Y_{2,1})$ が現れるまで繰り返すと，

$$I(S^mC_{1,m}C_{2,m};Y_{2,0}Y_2^m) \le \sum_{j=1}^{m} I(S_jC_{1,j}C_{2,j};Y_{2,j}) \tag{3.57}$$

が得られる．$i \in \mathcal{C}$ となる $T_{1,i}$ について，$l_N = |\mathcal{C}|$ と置いてインデックス i の小さい順に $\tilde{T}_1, \tilde{T}_2, \cdots, \tilde{T}_l, \cdots, \tilde{T}_{l_N}$ とし，その組を $\tilde{T}^{l_N}$ と表す．j 番目のサブブロックにおいて

$I(S_jC_{1,j}C_{2,j};Y_{2,j}) = I(\tilde{T}^{l_N};Y_{2,j})$ の関係を用いると

$$\begin{aligned} I(S_jC_{1,j}C_{2,j};Y_{2,j}) &= I(\tilde{T}^{l_N};Y_{2,j}) \\ &= \sum_{l=1}^{l_N} I(\tilde{T}_l;Y_{2,j}|\tilde{T}^{l-1}) \\ &= \sum_{l=1}^{l_N} (H(\tilde{T}_l) - H(\tilde{T}_l|Y_{2,j},\tilde{T}^{l-1})) \\ &\leq \sum_{i\in C} (H(T_{1,i}) - H(T_{1,i}|Y_{2,j},T_1^{i-1})) \end{aligned} \tag{3.58}$$

となる．補題 1 より，

$$Z(T_{1,i}|Y_{2,j},T_1^{i-1})^2 \leq H(T_{1,i}|Y_{2,j},T_1^{i-1}) \tag{3.59}$$

が成り立つ．また，$\mathcal{C}$ について，

$$\begin{aligned} \mathcal{C} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2Y_2U} \\ &\subseteq \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|Y_2U} \end{aligned} \tag{3.60}$$

となるため，$i \in \mathcal{C}$ において，

$$Z(T_{1,i}|Y_{2,j}T_1^{i-1}U^N) \geq 1 - \delta_N \tag{3.61}$$

が成り立つ．よって，$i \in \mathcal{C}$ において，

$$(1-\delta_N)^2 \leq H(T_{1,i}|Y_{2,j}T_1^{i-1}U) \tag{3.62}$$

が成立する．また，$T_{k,i}$ は 2 元の確率変数であるため，$H(T_{1,i}) \leq 1$ となる．式 (3.58),(3.62) より

$$I(S_jC_{1,j}C_{2,j};Y_{2,j}) \leq \sum_{i\in\mathcal{C}} (2\delta_N) \leq O(N2^{-N^\beta}) \tag{3.63}$$

となるので，式 (3.48),(3.57),(3.63) から次式が成立する．

$$I(M_{1s};Y_2^m) \leq mO(N2^{-N^\beta}). \tag{3.64}$$

受信者 1 に受信者 2 への秘匿メッセージが伝わる情報漏洩量についても，同様にして，

$$I(M_{2s};Y_1^m) \leq mO(N2^{-N^\beta}). \tag{3.65}$$

以上より，$N \to \infty$ としたとき，誤り確率と情報漏洩量が 0 に近づくため，強安全性の達成が示される．　□

第 4 章

BC-2CMに含まれる通信路におけるポーラ符号の構成

4.1 BCCにおけるポーラ符号の構成

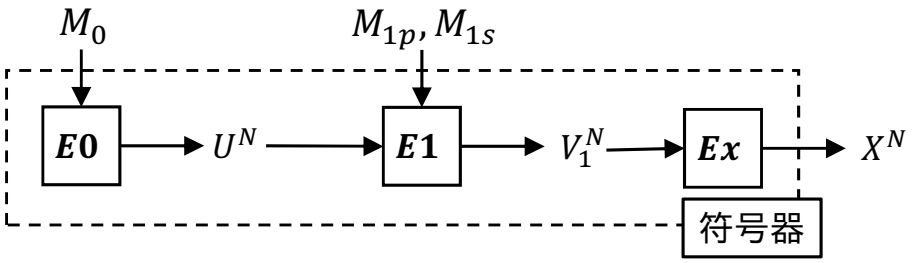

図 4.1: BCC において共通メッセージを上限まで送るときの仮想符号器

受信者 2 への個別メッセージ M_{2p} と秘匿メッセージ M_{2s} が存在しないとき，つまり $R_{2s} = R_2 = 0$ としたとき，BC-2CM は BCC に帰着する．このとき，V_2^N が無いものと看做すことができ，このときの符号器は図 4.1 となる．共通メッセージの送信は 3.1.1 節と同様であり，個別及び秘匿メッセージの送信について，

$$\begin{aligned} \mathcal{H}_{V_1|U} &= \mathcal{H}_{V_1|V_2U} \\ \mathcal{H}_{V_1|Y_2U} &= \mathcal{H}_{V_1|V_2Y_2U} \end{aligned} \tag{4.1}$$

となり，インデックス集合 $[N]$ の分割は，

$$\begin{aligned} \mathcal{B} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|V_2Y_2U}, \\ \mathcal{C} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}_{V_1|Y_1U} \cap \mathcal{H}_{V_1|Y_2U}, \\ \mathcal{E} &= \mathcal{H}_{V_1|U} \cap \mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}^c_{V_1|Y_2U}, \\ \mathcal{F} &= \mathcal{H}^c_{V_1|U} \cup \left(\mathcal{L}^c_{V_1|Y_1U} \cap \mathcal{H}_{V_1|V_2Y_2U}\right). \end{aligned} \tag{4.2}$$

となる．以後，3.1.2 節の個別及び秘匿メッセージの送信と同様に送信することができる．このときの提案構成法は，Glucu と Barg の構成 [7] と一致し，符号化レート (R_0, R_1, R_{1s}) は，

$$\begin{aligned}\lim_{m\to\infty}\lim_{N\to\infty} R_{0(N,m)} &= \min\{I(U;Y_1), I(U;Y_2)\},\\ \lim_{m\to\infty}\lim_{N\to\infty} R_{1(N,m)} + R_{1(N,m)} &= I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\},\\ \lim_{m\to\infty}\lim_{N\to\infty} R_{1s(N,m)} &= I(V_1;Y_1|U) - I(V_1;Y_2V_2|U)\end{aligned} \tag{4.3}$$

となり，命題 1 で示した領域の境界点と一致する．また，$N \to \infty$ としたとき，誤り確率と情報漏洩量は 0 に近づくため，強安全性を達成している．

4.2　BC-CM におけるポーラ符号の構成

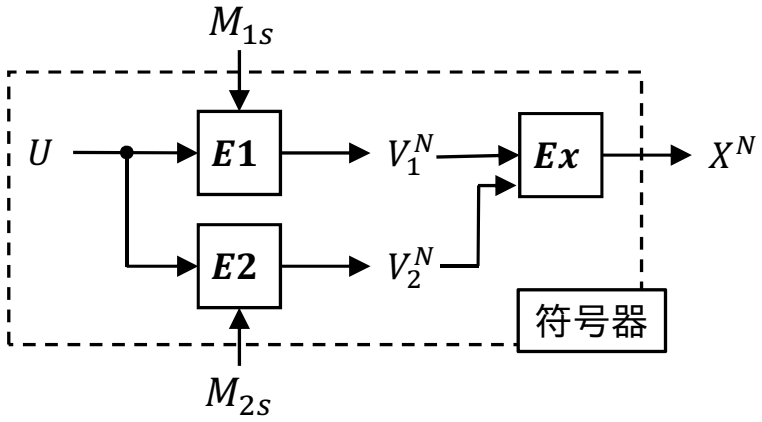

図 4.2: BC-CM において共通メッセージを上限まで送るときの仮想符号器

共通メッセージ M_0 と受信者それぞれへの個別メッセージ M_{1p}, M_{2p} が存在しないとき，つまり R_{1s}, R_{2s} のみに着目したとき，BC-2CM は BC-CM に帰着する．このとき，U^N はマルコフ連鎖 $U - V_k - X$ を満たす送信者と受信者で共有する任意の補助確率変数 U として扱い，このときの符号器は図 4.2 となる．秘匿メッセージのみとなるメッセージの送信について，3.1.2 節の秘匿メッセージの送信と同様となる．符号化レート (R_{1s}, R_{2s}) は，

$$\begin{aligned}\lim_{m\to\infty}\lim_{N\to\infty} R_{1s(N,m)} &= I(V_1;Y_1|U) - I(V_1;Y_2V_2|U),\\ \lim_{m\to\infty}\lim_{N\to\infty} R_{2s(N,m)} &= I(V_2;Y_2|U) - I(V_2;Y_1V_1|U)\end{aligned} \tag{4.4}$$

となり，命題 2 で示した領域の境界点と一致する．また，$N \to \infty$ としたとき，誤り確率と情報漏洩量は 0 に近づくため，強安全性を達成している．

第 5 章

まとめ

1 人の送信者が 2 人の受信者に対し，共通メッセージとそれぞれ独立した個別メッセージと秘匿メッセージを送る 2 つの秘匿メッセージを有する放送型通信路 (BC-2CM)[14] において，強安全性を達成するポーラ符号の構成法を提案した．ポーラ符号を用いる m 個のサブブロックを利用して，あるサブブロックの片方の受信者にのみ復号できる部分と，1 ブロック後のサブブロックのもう片方の受信者にのみ復号できる部分を結び付け，連鎖構造を作成し，通信路への入力のために使用した．このサブブロック構造により，共通メッセージと個別メッセージの符号化レートを最大化することができ，復号できる形で秘匿メッセージを組み込むことができた．受信者 2 に対する個別メッセージと秘匿メッセージが無い場合は，Glucu と Barg [7] による BCC[3] におけるポーラ符号の構成と一致することを確認し，共通メッセージと個別メッセージが無い場合は，BC-CM[9] におけるポーラ符号の構成となることを確認した．

参考文献

[1] E. Arıkan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[2] E. Arıkan, “Source polarization,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 899–903, Jun. 2010.

[3] I. Csiszár and J. Köner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] 藤田 隆寛, 八木 秀樹, “秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成,” 電子情報通信学会技術研究報告, vol.117, no.120, IT2017-28, pp.67–72, Jul. 2017.

[5] T. Fujita and H. Yagi, “Polar codes achieving strong secrecy for broadcast channel with confidential messages,” in *Proc. of 2018 RISP Int. Workshop on Nonlinear Circuits, Commun. and Signal Processing (NCSP2018)*, pp.631–634, Honolulu, USA, Mar. 2018.

[6] 藤田 隆寛, 八木 秀樹, “2 つの秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成,” 第 41 回情報理論とその応用シンポジウム予稿集, pp.499–504, いわき, 福島, Dec. 2018.

[7] T. C. Glucu and A. Barg, “Achieving secrecy capacity of the wiretap channel and broadcast channel With a confidential component,” *IEEE Trans. Inf. Theory*, vol. 63, no. 2, pp. 1311–1324, Feb. 2017.

[8] J. Honda and H. Yamamoto, “Polar coding without alphabet extension for asymmetric models,” *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7829–7838, Dec. 2013.

[9] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages secrecy rate regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[10] M. Mondelli, S. H. Hassani, I. Sason, and R. Urbanke, “Achieving Marton’s region for broadcast channels using polar codes,” *IEEE Trans. Inf. Theory*, vol. 61, no. 2, pp. 783–800, Jan. 2015.

[11] E. Şaşoğlu and A. Vardy, “A new polar coding scheme for strong security on wiretap channels,” in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1117–1121, Jul. 2013.

[12] Y.-P. Wei and S. Ulukus, “Polar coding for the general wiretap channel with extensions to multiuser scenarios,” *IEEE Journal on Selected Areas in Commun.*, vol. 34, no. 2, pp. 278–291, Feb. 2016.

[13] A. D. Wyner, “The wire-tap channel,” *Bell System Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[14] J. Xu, Y. Cao, and B. Chen, “Capacity bounds for broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

発表実績

[4] 藤田 隆寛, 八木 秀樹, “秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成,” 電子情報通信学会技術研究報告, vol.117, no.120, IT2017-28, pp.67–72, Jul. 2017.

[5] T. Fujita and H. Yagi, “Polar codes achieving strong secrecy for broadcast channel with confidential messages,” in *Proc. of 2018 RISP Int. Workshop on Nonlinear Circuits, Commun. and Signal Processing (NCSP2018)*, pp.631–634, Honolulu, USA, Mar. 2018.

[6] 藤田 隆寛, 八木 秀樹, “2 つの秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成,” 第 41 回情報理論とその応用シンポジウム予稿集, pp.499–504, いわき, 福島, Dec. 2018.

謝辞

最後に，本研究を進めるにあたり，時間を割いて丁寧かつ熱心なご指導を行っていただいた 八木 秀樹 准教授 に心より深く感謝いたします．また，ゼミの大学院セミナーをはじめ，様々な場面でお世話になった 大濱 靖匡 教授，川端 勉 教授，SANTOSO BAGUS 助教 に心より感謝いたします．そして，共に勉学に励み，助言をしていただいた研究室の皆様に心より感謝いたします．