(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-153837
(P2019-153837A)
(43)公開日　令和1年9月12日(2019.9.12)

(51)Int.Cl.	F I	テーマコード（参考）
H03M 13/13 (2006.01)	H03M 13/13	5J065

審査請求 未請求　請求項の数 5　OL　（全 31 頁）

(21)出願番号　特願2018-35547(P2018-35547)
(22)出願日　平成30年2月28日(2018.2.28)

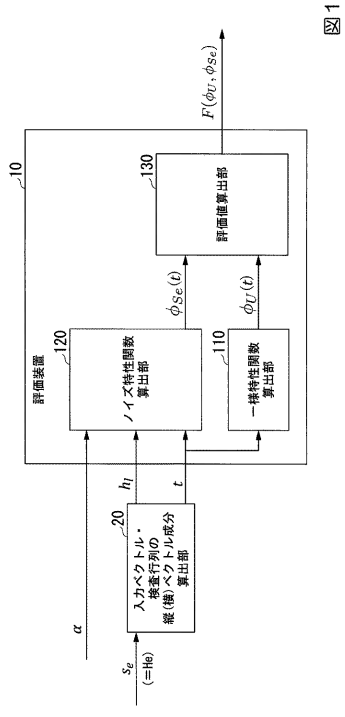
(71)出願人　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100175824
弁理士　小林　淳一
(74)代理人　100169764
弁理士　清水　雄一郎
(72)発明者　小川　朋宏
東京都調布市調布ケ丘一丁目５番地１　国立大学法人電気通信大学内
(72)発明者　森　雄喜
東京都調布市調布ケ丘一丁目５番地１　国立大学法人電気通信大学内

Fターム(参考)　5J065 AC02　AD03　AG02

(54)【発明の名称】評価装置

(57)【要約】
【課題】盗聴通信路符号化における安全性基準値の評価値を、実用的な手順により求める。
【解決手段】評価装置は、盗聴通信路符号化方式における公開パラメータである検査行列と、盗聴通信路のビット反転確率と、盗聴通信路を介して取得される盗聴者受信ビット列と検査行列とから得られる盗聴者推定メッセージに含まれる、ビット反転確率に基づくノイズを示すビット列であるノイズベクトルの確率分布を多変数離散フーリエ変換した関数の入力ベクトルと、を取得する取得部と、取得部が取得する入力ベクトルと、検査行列の縦ベクトル又は横ベクトルのいずれかのベクトル成分と、ビット反転確率とに基づいて、ノイズベクトルの確率分布の特性関数であるノイズ特性関数を算出するノイズ特性関数算出部と、ノイズ特性関数算出部が算出するノイズ特性関数と、ビット反転確率とに基づいて、検査行列の評価値をビット反転確率毎に算出する評価値算出部と、を備える。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
盗聴通信路符号化方式における公開パラメータである検査行列と、盗聴通信路のビット反転確率と、前記盗聴通信路を介して取得される盗聴者受信ビット列と前記検査行列とから得られる盗聴者推定メッセージに含まれる、前記ビット反転確率に基づくノイズを示すビット列であるノイズベクトルの確率分布を多変数離散フーリエ変換した関数の入力ベクトルと、を取得する取得部と、
前記取得部が取得する前記入力ベクトルと、前記検査行列の縦ベクトル又は横ベクトルのいずれかのベクトル成分と、前記ビット反転確率とに基づいて、ノイズベクトルの確率分布の特性関数であるノイズ特性関数を算出するノイズ特性関数算出部と、
前記ノイズ特性関数算出部が算出する前記ノイズ特性関数と、前記ビット反転確率とに基づいて、前記検査行列の評価値を前記ビット反転確率毎に算出する評価値算出部と、
を備える評価装置。
【請求項２】
前記取得部が取得する前記入力ベクトルに基づいて、一様分布の特性関数である一様特性関数を算出する一様特性関数算出部
を更に備え、
前記評価値算出部は、
前記ノイズ特性関数と、前記一様特性関数算出部が算出する前記一様特性関数とのノルムを前記ビット反転確率毎に前記検査行列の評価値として算出する
請求項１に記載の評価装置。
【請求項３】
前記評価値算出部は、
前記ノイズ特性関数と、前記一様特性関数との２ノルムを算出し、算出した２ノルムを１ノルムに変換することにより、前記評価値を算出する
請求項２に記載の評価装置。
【請求項４】
前記ノイズ特性関数は、前記入力ベクトルと、前記検査行列の前記ベクトル成分との内積によって示され、
前記評価値算出部は、
前記内積の値に基づいて前記評価値を算出する
請求項１から請求項３のいずれか一項に記載の評価装置。
【請求項５】
前記評価値算出部は、
複数の前記入力ベクトルのうち前記内積の値が互いに一致する前記入力ベクトルの計数値を前記評価値毎に算出する第１手順と、
前記第１手順によって算出された前記計数値を用いて、前記入力ベクトルのうち前記内積の値が法を２として１である前記入力ベクトルの総和を前記ビット反転確率毎に求める第２手順と、
によって前記評価値を算出する
請求項１から請求項４のいずれか一項に記載の評価装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、評価装置に関する。
【背景技術】
【０００２】
従来、盗聴者が存在する通信路モデルにおいて、安全な通信を行うための符号化レートの限界を求める技術が開示されている（例えば、非特許文献１を参照）。
【先行技術文献】

【非特許文献】
【０００３】
【非特許文献１】Ke Zhang, Martin Tomlinson, Mohammed Zaki Ahmed, Marcel Ambroze, Miguel R.D. Rodrigues、Best binary equivocation code construction forsyndrome coding、IET Commun.、2014,Vol.8, Iss. 10, pp. 1696-1704
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上記のような従来技術においては、検査行列Ｈを整数の組により表現しているため、具体的な数値を代入して計算をする場合の整合性が取れておらずｚ変換に特殊な演算が必要となるという問題があった。つまり、上記のような従来技術においては、実用的な手順による演算が必ずしも行えない、という問題があった。
【０００５】
本発明は、上記問題を解決すべくなされたもので、その目的は、盗聴通信路符号化における符号化レートの評価値を、実用的な手順により求めることができる評価装置を提供することにある。
【課題を解決するための手段】
【０００６】
本発明の一実施形態は、盗聴通信路符号化方式における公開パラメータである検査行列と、盗聴通信路のビット反転確率と、前記盗聴通信路を介して取得される盗聴者受信ビット列と前記検査行列とから得られる盗聴者推定メッセージに含まれる、前記ビット反転確率に基づくノイズを示すビット列であるノイズベクトルの確率分布を多変数離散フーリエ変換した関数の入力ベクトルと、を取得する取得部と、前記取得部が取得する前記入力ベクトルと、前記検査行列の縦ベクトル又は横ベクトルのいずれかのベクトル成分と、前記ビット反転確率とに基づいて、ノイズベクトルの確率分布の特性関数であるノイズ特性関数を算出するノイズ特性関数算出部と、前記ノイズ特性関数算出部が算出する前記ノイズ特性関数と、前記ビット反転確率とに基づいて、前記検査行列の評価値を前記ビット反転確率毎に算出する評価値算出部と、を備える評価装置である。
【０００７】
また、本発明の一実施形態は、上述の評価装置において、前記取得部が取得する前記入力ベクトルに基づいて、一様分布の特性関数である一様特性関数を算出する一様特性関数算出部を更に備え、前記評価値算出部は、前記ノイズ特性関数と、前記一様特性関数算出部が算出する前記一様特性関数とのノルムを前記ビット反転確率毎に前記検査行列の評価値として算出する。
【０００８】
また、本発明の一実施形態は、上述の評価装置において、前記評価値算出部は、前記ノイズ特性関数と、前記一様特性関数との２ノルムを算出し、算出した２ノルムを１ノルムに変換することにより、前記評価値を算出する。
【０００９】
また、本発明の一実施形態は、上述の評価装置において、前記ノイズ特性関数は、前記入力ベクトルと、前記検査行列の前記ベクトル成分との内積によって示され、前記評価値算出部は、前記内積の値に基づいて前記評価値を算出する。
【００１０】
また、本発明の一実施形態は、上述の評価装置において、複数の前記入力ベクトルのうち前記内積の値が互いに一致する前記入力ベクトルの計数値を前記評価値毎に算出する第１手順と、前記第１手順によって算出された前記計数値を用いて、前記入力ベクトルのうち前記内積の値が法を２として１である前記入力ベクトルの総和を前記ビット反転確率毎に求める第２手順と、によって前記評価値を算出する。
【発明の効果】
【００１１】

この発明によれば、盗聴通信路符号化における安全性基準値の評価値を、実用的な手順により求めることができる評価装置を提供することができる。

【図面の簡単な説明】

【００１２】

【図１】本実施形態の評価装置の機能構成の一例を示す図である。

【図２】本実施形態の評価装置の評価値を算出する概略動作の一例を示す図である。

【図３】本実施形態のノイズ特性関数算出部によるノイズ特性関数の算出手順の一例を示す図である。

【図４】本実施形態の評価装置による評価値のプロットの一例（その１）を示す図である。

【図５】本実施形態の評価装置による評価値のプロットの一例（その２）を示す図である。

【図６】本実施形態の理論値付近の評価値の一例を示す図である。

【図７】本実施形態において（ｎ，ｋ）＝（４０，１０）とした場合の評価値の一例を示す図である。

【図８】本実施形態において（ｎ，ｋ）＝（６０，３０）とした場合の評価値の一例を示す図である。

【図９】本実施形態において（ｎ，ｋ）＝（４００，３７０）とした場合の評価値の実験結果の一例を示す図である。

【図１０】本実施形態において（ｎ，ｋ）＝（４００，３７０）とした場合の評価値の実験結果の一例を示す図である。

【図１１】本実施形態の変形例に係る評価装置の評価値を算出する概略動作の一例を示す図である。

【図１２】本実施形態の変形例に係る評価装置による評価値の算出手順の一例を示す図である。

【図１３】本実施形態の変形例のアルゴリズムによる評価値の実験結果の一例を示す図である。

【図１４】盗聴者が存在する通信路モデルの一例を示す図である。

【図１５】盗聴通信路符号化モデルの一例を示す図である。

【図１６】コセット分解の概念の一例を示す図である。

【図１７】コセット符号化の概念の一例を示す図である。

【図１８】（ｎ，ｋ）符号の乱数レートとビット反転確率との関係の一例を示す図である。

【図１９】乱数レートと（ｎ，ｋ）の組との関係の一例を示す図である。

【発明を実施するための形態】

【００１３】

［前提事項及び実施形態の概要］

以下、本発明の実施形態を説明する前に、実施形態の前提事項及び実施形態の概要について図を参照しつつ説明する。

【００１４】

［盗聴通信路符号化］

図１４は、盗聴者が存在する通信路モデルの一例を示す図である。Ｗｙｎｅｒは盗聴者が存在する通信路モデルにおいて安全な通信を行うことができる盗聴通信路符号化問題を考案した。図１４で定義する送信者Ａｌｉｃｅから盗聴者Ｅｖｅへの通信路を盗聴通信路という。盗聴通信路符号化モデルに対する要請は次の２つである。

【００１５】

ｎ→∞という漸近的な状況において、

要請１：送信者Ａｌｉｃｅは誤り確率　０でメッセージを正規受信者Ｂｏｂに伝えること。

要請２：盗聴者Ｅｖｅにメッセージの情報が一切伝わらないこと。

【００１６】
上記の要請を同時に満たす符号の符号化レートの限界を考えるのが盗聴通信路符号化問題であり、そのレートを盗聴通信路容量と呼ぶ。要請２に対する安全性の基準として、次の式（１）～式（３）の３つを考える。
【００１７】
【数１】

$$\frac{1}{n}J(S;Z^n)\xrightarrow{n\to\infty}0 \qquad \cdots（1）$$

【００１８】
【数２】

$$J(S;Z^n)\xrightarrow{n\to\infty}0 \qquad \cdots（2）$$

【００１９】
【数３】

$$\frac{1}{\#\mathcal{M}(\#\mathcal{M}-1)}\sum_{i=0}^{\#\mathcal{M}-1}\sum_{j\neq i,j=0}^{\#\mathcal{M}-1}||P_{Z_i^n}-P_{Z_j^n}||_1\xrightarrow{n\to\infty}0 \qquad \cdots（3）$$

【００２０】
ただし、式（３）の$P_{z^n{}_i}$、$P_{z^n{}_j}$（ｎはｚの右上の添字。ｉ、ｊはｚの右下の添字。）はｉ番目、ｊ番目のメッセージを入力した時の通信に関する確率分布である。式（２）が示す基準２は式（１）が示す基準１よりも強い基準なので、基準２を満たせば、基準１は自然と成り立つ。このことから基準１を弱安全性、基準２を強安全性と呼ぶ。基準１および基準２は、ｎ→∞の時、漸近的にＳとZ^nが独立であることを意味している。基準３は異なるメッセージを入力した時の出力分布の差に関する１－ｎｏｒｍ（いち・ノルム）の平均値である。盗聴者Ｅｖｅが通信路出力を観測しても、確率分布がメッセージに依存していないため、メッセージについての情報が全く得られなくなる。正規受信者Ｂｏｂへの通信路よりも盗聴者Ｅｖｅへの通信路の方にノイズが多く含まれる時に、以下の盗聴通信路符号化定理が成立する。
【００２１】
［盗聴通信路符号化定理］
上述した２つの要請（要請１及び要請２）が達成可能な符号化レートの上限である盗聴通信路容量（Ｔ（Ｗ、Ｖ））は、正規受信者Ｂｏｂの通信路（正規通信路Ｂ）をＷ、盗聴者Ｅｖｅの通信路（盗聴通信路Ｅ）をＶとしたとき、次の式（４）を満たす。
【００２２】
【数４】

$$T(W,V)\geq\max_{P_X}\{J(X;Y)-J(X;Z)\} \qquad \cdots（4）$$

【００２３】
二元対称通信路ＢＳＣ(Binary Symmetric Channel)のビット反転確率がビット反転確率αである場合を、二元対称通信路BSC_αと記載する。正規通信路Ｂがノイズレスで盗聴通信路Ｅが二元対称通信路BSC_αの場合、式（４）の不等号で等号が成立し、盗聴通信路容量は、次の式（５）で与えられることが知られている。

【００２４】
【数５】

$$T(W,V) = 1 - (1 - h(\alpha)) = h(\alpha) \qquad \cdots (5)$$

【００２５】
［盗聴通信路符号化モデル］
図１５は、盗聴通信路符号化モデルの一例を示す図である。図１５に示す盗聴通信路符号化モデルは、図１４に示した正規通信路Ｂにノイズレス通信路を、盗聴通信路Ｅに二元対称通信路ＢＳＣを用いたものである。以降、盗聴通信路符号化モデルとして図１５に示す盗聴通信路符号化モデルを用いることとする。なお、上述した基準２を安全性の指標として考える。盗聴通信路符号化の要請について、要請１に関しては送信者Ａｌｉｃｅから正規受信者Ｂｏｂへの通信路にノイズレス通信路を用いている。要請２に関しては、式（６）を満たすべき条件として考えることにする。
【００２６】
【数６】

$$J(S;S') \xrightarrow{n\to\infty} 0 \qquad \cdots (6)$$

【００２７】
［線形符号］
長さｋのベクトルが長さｎのベクトルに変換される場合、線形符号Ｃを（ｎ，ｋ）線形符号または（ｎ，ｋ）符号と呼ぶ。以下、ｍ：＝ｎ－ｋとして議論する。成分がF_2の元のｍ×ｎ行列Ｈを考える。ここで、Ｈは行ベクトルがすべて一次独立すなわち行フルランクであると仮定する。この行列Ｈにより、線形符号Ｃは式（７）のように指定される。
【００２８】
【数７】

$$\begin{aligned} C &= \{\boldsymbol{x} \in \mathbb{F}_2^n | H\boldsymbol{x} = \boldsymbol{0}\} \\ &= \mathrm{Ker}\ H \end{aligned} \qquad \cdots (7)$$

【００２９】
この線形符号Ｃを指定する行列Ｈを検査行列と呼ぶ。検査行列Ｈによる指定方法は同次連立一次方程式の解空間として線形符号Ｃを指定している。一方、検査行列Ｈが行フルランクであると仮定したことから式（８）が成り立つ。
【００３０】
【数８】

$$\dim \mathrm{Im}\ H = \mathrm{rank}\ H = m. \qquad \cdots (8)$$

【００３１】
次元定理より、式（９）であるから、
【００３２】
【数９】

$$\dim \mathrm{Im}\ H + \dim \mathrm{Ker}\ H = n \qquad \cdots (9)$$

【００３３】
次の式（１０）となり、生成行列による場合と同じ次元の符号を与えている。
【００３４】

【数１０】

$$\begin{aligned}\dim \mathrm{Ker}\, H &= n - \dim \mathrm{Im}\, H \\ &= n - m \\ &= n - (n-k) \\ &= k\end{aligned} \qquad \cdots (10)$$

【００３５】

［コセット］

次に、図１６を参照してコセットについて説明する。

図１６は、コセット分解の概念の一例を示す図である。式（１１）に示すように、任意のシンドロームｓ＝（s_0，…，s_{m-1}）$\in F^m_2$に対応する検査行列Ｈ：$F^n_2 \to F^m_2$の逆像を、シンドロームｓに対応するコセットと呼ぶ。

【００３６】

【数１１】

$$C_{\boldsymbol{s}} := \{\boldsymbol{x} \in \mathbb{F}_2^n | H\boldsymbol{x} = \boldsymbol{s}\} \qquad \cdots (11)$$

【００３７】

［コセット符号化］

図１７は、コセット符号化の概念の一例を示す図である。コセット符号化では、メッセージを送信者のシンドロームと同一視する。メッセージとコセットを一対一に対応させることで、確率的符号器の一つであるコセット符号を構成することができる。任意のメッセージｓ∈Ｍ（＃Ｍ＝2^m）（すなわち、ｍビットのビット列）を送信するとき、あらかじめ対応付けられているコセットの要素から一様乱数ｕ∈Ｕ（＃Ｕ＝2^k）（すなわち、ｋビットのビット列）を用いて符号語ｘを決定し、通信路に入力する。この時、メッセージレートR_Sと乱数レートR_Uは以下で与えられる。

【００３８】

【数１２】

$$R_S = \frac{\log_2 2^m}{n} = \frac{m}{n} = \frac{n-k}{n} = 1 - \frac{k}{n} \qquad \cdots (12)$$

【００３９】

【数１３】

$$R_U = \frac{\log_2 2^k}{n} = \frac{k}{n} \qquad \cdots (13)$$

【００４０】

［コセット符号化による盗聴通信路符号化の実現］

図１５に示した盗聴通信路符号化モデルを用いた、コセット符号化による盗聴通信路符号化の実現について説明する。

送信者Ａｌｉｃｅ、正規受信者Ｂｏｂ間の通信環境と送信者Ａｌｉｃｅ、盗聴者Ｅｖｅ間の通信環境において、前者の通信品質が上回っている状況を仮定する。例として無線ＬＡＮがある部屋の中と外、衛星通信の見通し範囲とその外側が挙げられる。このような状況で通信品質の差を利用することで、送信者Ａｌｉｃｅと正規受信者Ｂｏｂとの間で安全な通信を行うことができる。

簡単のため、送信者Ａｌｉｃｅから正規受信者Ｂｏｂへの通信路はノイズレス通信路で

あると仮定する。また、送信者Ａｌｉｃｅから盗聴者Ｅｖｅへの通信路は二元対称通信路ＢＳＣであると仮定する。

【００４１】

以降で用いる検査行列Ｈの形について説明する。上述した（ｎ，ｋ）符号を考え、ｍ：＝ｎ－ｋとする。

【００４２】

【数１４】

$$\boldsymbol{h}_l \in \mathbb{F}_2^m (l = 0, \cdots, n-1) \qquad \cdots（１４）$$

【００４３】

検査行列Ｈの縦ベクトル表示を、式（１４）を用いて式（１５）の形で書く。

【００４４】

【数１５】

$$H = [\boldsymbol{h}_0, \cdots, \boldsymbol{h}_l, \cdots, \boldsymbol{h}_{n-1}] \qquad \cdots（１５）$$

【００４５】

コセット符号化における盗聴通信路符号化を実現できるような（ｎ，ｋ）符号の探索が試みられている。

【００４６】

１：検査行列Ｈを一つ固定して公開パラメータとする。

２：送信者Ａｌｉｃｅのフェーズ：

メッセージに対応するシンドロームｓを生成する。

コセット符号化によりＨｘ＝ｓを満たすｘを求め、正規受信者Ｂｏｂに送信する。

３：正規受信者Ｂｏｂのフェーズ：

送信者Ａｌｉｃｅから、$x_r = x$を受け取ることで、$s = Hx_r$を計算する。

４：盗聴者Ｅｖｅのフェーズ：

二元対称通信路ＢＳＣによる誤りベクトルをｅとして$x_e = x + e$を受け取ることで、ｓ′＝Ｈx_eを計算する。

【００４７】

ただし、送信者Ａｌｉｃｅのメッセージに関する確率変数Ｓと盗聴者Ｅｖｅの持つ情報に関する確率変数Ｓ′について、相関の指標を表す情報量である相互情報量を用いることで、上述した式（６）を安全性の定義として用いる。

【００４８】

［エンコーダとデコーダについて］

メッセージのエンコーダとデコーダの方法を与え、安全性評価をエントロピーを用いて行う技術が提示されている。

Ｈ＝（Ｉ、Ｈ２）と指定する。送信者Ａｌｉｃｅは、Ｈｘ＝ｓを満たす$x \in F^n_2$を以下の３ステップで生成する。

【００４９】

１：送信者Ａｌｉｃｅは一様ランダムに決まる$a \in F^k_2$とｎ×ｋの生成行列Ｇを用いて、符号語$x_1 \in F^n_2$を以下のように定める。

【００５０】

【数１６】

$$\boldsymbol{x}_1 := G\boldsymbol{a} \qquad \cdots（１６）$$

【００５１】

２：送信者Ａｌｉｃｅは、$x_2 \in F^n_2$をメッセージ$s \in F^m_2$を用いて以下のように

生成する。

【００５２】

【数１７】

$$\boldsymbol{x}_2 := \left(\boldsymbol{s}^T, 0, \cdots, 0\right)^T \qquad \cdots（１７）$$

【００５３】

３：送信者Ａｌｉｃｅは、式（１６）及び式（１７）を用いて$x \in F^{n}{}_{2}$を以下のように生成する。

【００５４】

【数１８】

$$\boldsymbol{x} := \boldsymbol{x}_1 + \boldsymbol{x}_2 \qquad \cdots（１８）$$

【００５５】

このようにして、送信者Ａｌｉｃｅは、

【００５６】

【数１９】

$$H\boldsymbol{x} = \boldsymbol{s} \qquad \cdots（１９）$$

【００５７】

を満たすｘを生成できる。

正規受信者Ｂｏｂは、受信したベクトルのシンドロームを式（２０）で計算する。送信者Ａｌｉｃｅから正規受信者Ｂｏｂへの通信路は、ノイズレスであることから$x_r = x$である。よって、正規受信者Ｂｏｂは、式（２０）に示すようにデコードできる。

【００５８】

【数２０】

$$\boldsymbol{s} = H\boldsymbol{x}_{\mathrm{r}} \qquad \cdots（２０）$$

【００５９】

一方、盗聴者Ｅｖｅは、式（２１）に示すベクトル

【００６０】

【数２１】

$$\boldsymbol{x}_{\mathrm{e}} = \boldsymbol{x} + \boldsymbol{e} \qquad \cdots（２１）$$

を受信し、式（２２）を計算することが想定される。

【００６１】

【数２２】

$$\boldsymbol{s}' = H\boldsymbol{x}_{\mathrm{e}} = H\left(\boldsymbol{x} + \boldsymbol{e}\right) = H\boldsymbol{x} + H\boldsymbol{e} = \boldsymbol{s} + \boldsymbol{s}_{\mathrm{e}} \qquad \cdots（２２）$$

【００６２】

よって、盗聴者Ｅｖｅは、式（２３）に示すように

【００６３】

【数２３】

$$\boldsymbol{s}' = \boldsymbol{s} + \boldsymbol{s}_{\mathrm{e}} \qquad \cdots（２３）$$

【００６４】

としてメッセージを推測すると考えられる。メッセージに関する確率変数が一様分布に従うという仮定をしてよい理由は、一様分布が扱いやすいという理由の他、送信者Ａｌｉｃｅがどのメッセージを選択しても、同様の安全性を持つ符号を構成したいからである。

もし、メッセージの分布に偏りがあると盗聴者Ｅｖｅに頻繁に使われるメッセージの情報を推測され頻度攻撃の標的にされるおそれがある。

【００６５】

［特性関数を用いた安全性評価］

確率変数Ｓ、Ｓｅが独立でＳが一様分布に従う時、確率変数Ｓ＋Ｓｅも一様分布に従う。式（２４）を満たすとき、式（２５）に示すＳｅは確率変数である。

【００６６】

【数２４】

$$\boldsymbol{e} \overset{i.i.d}{\sim} (\alpha, 1-\alpha) \qquad \cdots (24)$$

【００６７】

【数２５】

$$\boldsymbol{s}_e = \boldsymbol{He} \qquad \cdots (25)$$

【００６８】

その他の文字も大文字で書くとＳとＳｅが独立である。この時、確率変数Ｓ＋ＳｅをＳ′とおくと、式（２６）によって式（２７）が成立する。

【００６９】

【数２６】

$$\begin{aligned}\mathrm{Ent}(S|S') &= \mathrm{Ent}(S', S) - \mathrm{Ent}(S') \\ &= \mathrm{Ent}(S, S') - \mathrm{Ent}(S') \\ &= \mathrm{Ent}(S) - \mathrm{Ent}(S') + \mathrm{Ent}(S'|S) \qquad \cdots (26) \\ &= \mathrm{Ent}(S) - \mathrm{Ent}(S + S_e) + \mathrm{Ent}(S + S_e|S) \\ &= m - m + \mathrm{Ent}(S_e|S) = \mathrm{Ent}(S_e)\end{aligned}$$

【００７０】

【数２７】

$$\mathrm{Ent}(S|S') = \mathrm{Ent}(S_e) \qquad \cdots (27)$$

【００７１】

この式（２７）から、上述した式（６）は、次の式（２８）と同値であることがわかる。

【００７２】

【数２８】

$$\mathrm{Ent}(S_e) \xrightarrow{n\to\infty} m \qquad \cdots (28)$$

【００７３】

以下、式（６）の代わりに式（２８）を（ｎ，ｋ）符号の安全性評価に用いる。

【００７４】

［特性関数］

特性関数を定義しその性質を調べることで、相互情報量を直接計算することなく、（ｎ，ｋ）符号の安全性評価を行うことを考える。なお、以下の説明において記号ｉとは、虚数単位である。

【００７５】

$2 \leqq a \in \mathbb{N}$で$\mathbf{x} = (x_0, \cdots, x_{m-1}) \in \mathbb{Z}_a^m$、$\mathbf{t} = (t_0, \cdots, t_{m-1}) \in \mathbb{Z}_a^m$とする時、確率分布ｐの特性関数φｐを式（２９）に示す。

【００７６】
【数２９】

$$\phi_p(\boldsymbol{t}) := \frac{1}{\sqrt{a^m}} \sum_{\boldsymbol{x} \in \mathbb{Z}_a^m} p(\boldsymbol{x}) \exp\left[i \frac{2\pi}{a} \langle \boldsymbol{t}, \boldsymbol{x} \rangle \right] \qquad \cdots (29)$$

【００７７】
ここでｔとは、ビット列の確率分布を多変数離散フーリエ変換した関数の入力ベクトルである。
特性関数φｐを上記のように定義すると、式（２９）の逆変換が存在し、特性関数φｐの入力と出力で内積の結果を保存する（すなわち、ユニタリ性が成り立つ）。
【００７８】
この特性関数φｐ（ｔ）には、a^mの平方根が含まれ、独立な確率変数の和に関する定理が成り立たない。このため、数値実験を行う際は、式（３０）によって特性関数φｐ（ｔ）を定義する。
【００７９】
【数３０】

$$\phi_p(\boldsymbol{t}) := \sum_{\boldsymbol{x} \in \mathbb{Z}_a^m} p(\boldsymbol{x}) \exp\left[i \frac{2\pi}{a} \langle \boldsymbol{t}, \boldsymbol{x} \rangle \right] \qquad \cdots (30)$$

【００８０】
このように定義すると、ユニタリ変換ではなくなるが、逆変換の存在は満たされ独立な確率変数の和に関する定理も成り立つ。よって、以降では式（３０）を特性関数として定義する。このように定義した場合、次の式（３１）が成り立つ。
【００８１】
【数３１】

$$||p - q||_2 = \frac{1}{\sqrt{a^m}} ||\phi_p - \phi_q||_2 \qquad \cdots (31)$$

【００８２】
［安全性評価］
アルファベットχ上の確率分布P_xに従う確率変数Ｘについて、確率変数Ｘの１－ｎｏｒｍ（いち・ノルム）を、式（３２）により定義する。
【００８３】
【数３２】

$$||P_X||_1 := \sum_{x \in \mathcal{X}} |P_X(x)| \qquad \cdots (32)$$

【００８４】
同様に確率変数Ｘの２－ｎｏｒｍ（に・ノルム）を、式（３３）により定義する。
【００８５】
【数３３】

$$||P_X||_2 := \sqrt{\sum_{x \in \mathcal{X}} P_X(x)^2} \qquad \cdots (33)$$

【００８６】
ここで、ファネス型不等式とは、エントロピーとｎｏｒｍの関係を表す不等式である。エントロピーの連続性に関する不等式としても知られている。
X_1、X_2をアルファベットχ上の確率分布に従う確率変数とする。この時、式（３４）を満たす場合、式（３５）が成り立つ。
【００８７】
【数３４】

$$||P_{X_1} - P_{X_2}||_1 \leq \frac{1}{3} \qquad \cdots（34）$$

【００８８】
【数３５】

$$|\mathrm{Ent}(X_1) - \mathrm{Ent}(X_2)| \leq ||P_{X_1} - P_{X_2}||_1 \log \#\mathcal{X} + \eta(||P_{X_1} - P_{X_2}||_1)$$
$$\text{ただし}, \eta(t) = -t \log t$$

$$\cdots（35）$$

【００８９】
この式（３５）は、１－ｎｏｒｍにおいて成立する式であるが、特性関数を考える上では２－ｎｏｒｍを求める方が簡単である。そこで、１－ｎｏｒｍと２－ｎｏｒｍとの関係について以下に述べる。
【００９０】
アルファベットχ上の確率分布P_xに従う確率変数Ｘについて以下の式（３６）に示す関係が成立する。
【００９１】
【数３６】

$$||P_X||_2 \leq ||P_X||_1$$
$$||P_X||_1 \leq \sqrt{\#\mathcal{X}} \cdot ||P_X||_2 \qquad \cdots（36）$$

【００９２】
ｎｏｒｍに関する不等式とファネス型不等式から安全性評価を行う。まず、ファネス型不等式から、式（３７）に示す関係に注意して、式（３８）が成立する。
【００９３】
【数３７】

$$\lim_{t \to 0} t \log t = 0 \qquad \cdots（37）$$

【００９４】
【数３８】

$$||P_{X_1} - P_{X_2}||_1 \to 0 \Rightarrow |\mathrm{Ent}(X_1) - \mathrm{Ent}(X_2)| \to 0 \qquad \cdots（38）$$

【００９５】
このことから以下が成立する。すなわち、送信者Ａｌｉｃｅのメッセージに関する確率変数Ｓは一様分布に従うことに注意すると、確率変数Ｓのエントロピー Ｅｎｔ（Ｓ）はｍになる。このことから、一様分布Ｕのエントロピー Ｅｎｔ（Ｕ）はｍになることを考慮すると次の式（３９）が成立する。
【００９６】

【数３９】

$$||P_U - P_{S_e}||_1 \to 0 \Rightarrow \text{十分小さい正の数}\epsilon\text{に対して}, |m - \mathrm{Ent}(S_e)| < \epsilon \quad \cdots (39)$$

【００９７】

すなわち、正の数εが十分小さいという仮定のもとで、式（４０）を満たすとき、

【００９８】

【数４０】

$$|\mathrm{Ent}(S_e) - m| < \epsilon \quad \cdots (40)$$

【００９９】

上述した式（２８）に示す場合と同様の状況と考えることができる。よって、式（４１）を満たす（ｎ，ｋ）符号を探すことで上記の目的が達成される。

【０１００】

【数４１】

$$||P_U - P_{S_e}||_1 \to 0 \quad \cdots (41)$$

【０１０１】

［数値実験アルゴリズムの導出］

上述した特性関数を数値実験で用いるために式変形を行う。以降では、式（３０）においてａ＝２とした場合を考える。この時、剰余類環Z_aはａが素数だと有限体F_aに等しくなるため、$Z^m{}_a = F^m{}_a$である。すなわち、式（４２）及び式（４３）に示すように、

【０１０２】

【数４２】

$$\boldsymbol{t} = (t_0, \cdots, t_{m-1}) \in \mathbb{F}_2^m \quad \cdots (42)$$

【０１０３】

【数４３】

$$\boldsymbol{x} = (x_0, \cdots, x_{m-1}) \in \mathbb{F}_2^m \quad \cdots (43)$$

【０１０４】

とすると、特性関数φｐ（ｔ）は、式（４４）に示す通りになる。

【０１０５】

【数４４】

$$\phi_p(\boldsymbol{t}) := \sum_{x_0=0}^{1} \cdots \sum_{x_{m-1}=0}^{1} p(\boldsymbol{x}) \exp[\sqrt{-1}\pi \langle \boldsymbol{t}, \boldsymbol{x} \rangle] \quad \cdots (44)$$

$$= \sum_{x_0=0}^{1} \cdots \sum_{x_{m-1}=0}^{1} p(\boldsymbol{x})(-1)^{\langle \boldsymbol{t}, \boldsymbol{x} \rangle}$$

【０１０６】

なお、一般的に、F_2の元（例えば、０（ゼロ）や１（いち））同士の積はＡＮＤ、加

算はＸＯＲを用いるが、ここでは通常の足し算や掛け算と同様の表記を行う。

【０１０７】

［一様分布の特性関数］

まず、式（４５）に示す一様分布の特性関数について考える。

【０１０８】

【数４５】

$$U(\boldsymbol{x}) = \frac{1}{2^m} \qquad \cdots（45）$$

【０１０９】

式（４６）に示す式変形を行うことで、一様分布の特性関数である一様特性関数φＵ（ｔ）の値について、入力ベクトルｔが零ベクトル０である場合とそうでない場合の２通りに帰着される。

【０１１０】

【数４６】

$$\phi_U(\boldsymbol{t}) := \sum_{x_0=0}^{1} \cdots \sum_{x_{m-1}=0}^{1} U(\boldsymbol{x})(-1)^{\sum_{k=0}^{m-1} t_k x_k} = \frac{1}{2^m} \sum_{x_0=0}^{1} \cdots \sum_{x_{m-1}=0}^{1} (-1)^{\sum_{k=0}^{m-1} t_k x_k}$$
$$= \frac{1}{2^m} \prod_{k=0}^{m-1} (1 + (-1)^{t_k}) = \prod_{k=0}^{m-1} \frac{1 + (-1)^{t_k}}{2} = \begin{cases} 1 & (\boldsymbol{t} = \boldsymbol{0}) \\ 0 & (otherwise) \end{cases}$$
$$\cdots（46）$$

【０１１１】

［確率変数Ｓｅについての特性関数］

確率変数Ｓｅについての特性関数について考える。以下、検査行列Ｈの縦ベクトル成分を式（４７）及び式（４８）を用いて、式（４９）と表す。

【０１１２】

【数４７】

$$[\boldsymbol{h}_0, \cdots, \boldsymbol{h}_l, \cdots, \boldsymbol{h}_{n-1}] \qquad \cdots（47）$$

【０１１３】

【数４８】

$$\mathbb{F}_2^n \ni \boldsymbol{e} = [e_0, \cdots, e_l, \cdots, e_{n-1}]^T \qquad \cdots（48）$$

【０１１４】

【数４９】

$$\boldsymbol{f}_l := e_l \boldsymbol{h}_l \qquad \cdots（49）$$

【０１１５】

この時、確率変数Ｓｅは式（５０）のように書ける。

【０１１６】

【数５０】

$$\boldsymbol{s}_{\mathrm{e}} = H\boldsymbol{e} = \sum_{l=0}^{n-1} e_l \boldsymbol{h}_l = \sum_{l=0}^{n-1} \boldsymbol{f}_l \qquad \cdots（５０）$$

【０１１７】

ここで、ｅｌ（ｌ＝０，…，ｎ－１）は、二元対称通信路ＢＳＣの誤りベクトルの成分であり、独立に与えられる確率変数である。よって、ｆｌ（ｌ＝０，…，ｎ－１）はｅｌで定まる確率変数とも見ることができる。すなわち、ｆｌ（ｌ＝０，…，ｎ－１）は独立であるから、ｆｌの和の分布に従う確率変数Ｓｅの特性関数は、式（５１）に示すようにｆｌの特性関数の積に分解できる。

【０１１８】

【数５１】

$$\begin{aligned}\phi_{S_e}(\boldsymbol{t}) :&= \prod_{l=0}^{n-1} \phi_{\boldsymbol{f}_l}(\boldsymbol{t}) = \prod_{l=0}^{n-1} \sum_{\boldsymbol{f}_l \in \mathbb{F}_2^m} p(\boldsymbol{f}_l)(-1)^{\langle \boldsymbol{t}, \boldsymbol{f}_l \rangle} = \prod_{l=0}^{n-1} \left\{ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} \right\} \\ &= \prod_{l=0}^{m-1} \left\{ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} \right\} \prod_{l=m}^{n-1} \left\{ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} \right\} \\ &= \prod_{l=0}^{m-1} \left\{ (1-\alpha) + \alpha(-1)^{t_l} \right\} \prod_{l=m}^{n-1} \left\{ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} \right\}\end{aligned} \qquad \cdots（５１）$$

【０１１９】

ここで、式（５１）の総乗の中身は式（５２）に示すように簡単化される。

【０１２０】

【数５２】

$$\begin{aligned}(1-\alpha) + \alpha(-1)^{t_l} &= \begin{cases} 1 & (t_l = 0) \\ -2\alpha + 1 & (t_l = 1) \end{cases} \\ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} &= \begin{cases} 1 & (\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle = 0 \bmod 2) \\ -2\alpha + 1 & (\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle = 1 \bmod 2) \end{cases}\end{aligned} \qquad \cdots（５２）$$

【０１２１】

また、式（５３）に示す通り、上述した２－ｎｏｒｍの性質により、２－ｎｏｒｍの評価関数Ｆを、一様分布に関する確率変数Ｓ、盗聴者Ｅｖｅの持つ情報に関する確率変数Ｓｅを用いることで、

【０１２２】

【数５３】

$$||P_U - P_{S_e}||_2 = \frac{1}{\sqrt{2^m}} \sqrt{\sum_{\boldsymbol{t} \in \mathbb{F}_2^m} |\phi_U(\boldsymbol{t}) - \phi_{Se}(\boldsymbol{t})|^2} =: F(\phi_U, \phi_{Se}) \qquad \cdots（５３）$$

【０１２３】

として定義する。本実施形態の一例として行う数値実験では、二元対称通信路ＢＳＣのビット反転確率αを０．０～０．５の範囲で動かして２－ｎｏｒｍの評価関数Ｆの挙動を見る。

また、上述した１－ｎｏｒｍと２－ｎｏｒｍとの関係から、式（５４）が成立する。

【０１２４】

【数５４】

$$F \leq ||P_U - P_{S_e}||_1 \leq \sqrt{2^m} \cdot F \qquad \cdots（５４）$$

【０１２５】

［確率変数Ｓｅの特性関数の算出アルゴリズム］

上述した通り、式（５２）を用いることで、式（５５）を計算できることを述べた。

【０１２６】

【数５５】

$$\prod_{l=m}^{n-1} \left\{ (1-\alpha) + \alpha(-1)^{\langle \boldsymbol{t}, \boldsymbol{h}_l \rangle} \right\} \qquad \cdots（５５）$$

【０１２７】

しかしこのままでは１つの入力ベクトルｔにつきｎ－ｍ＝ｋ回の内積計算を行う必要がある。この節では、式（５５）についてｋ回の内積計算を高速化する方法を考える。計算機上では、F^m_2上の内積は積をＡＮＤでとり、それらの結果をＸＯＲを用いて足し算する操作に帰着される。これを用いると以下の手順を適用することで、内積計算の高速化が可能になる。

【０１２８】

手順１：変数ｔｅｍｐを０に初期化する。

手順２：ｆｏｒ　ｌｏｏｐ：ｌ＝ｍ，…，ｎ－１｛

手順３：　ｔ、ｈｌをビット列とみなして、$temp1 = (t)_2 \mathrm{AND} (h_l)_2$を計算する。

手順４：　ｔｅｍｐ１の１の部分をカウントし、ｔｅｍｐ２に格納する。

手順５：　ｔｅｍｐ２＝１ｍｏｄ２の場合、ｔｅｍｐをインクリメントする。｝

手順６：ｔｅｍｐを繰り返し回数ｋ′として返す。

【０１２９】

この手順により、式（５５）の値は、式（５６）によって与えられる。ここで、ビット列の１が立っている部分をカウントするアルゴリズムは、一般にｐｏｐｕｌａｔｉｏｎ　ｃｏｕｎｔアルゴリズム（ｐｏｐｃｎｔ）と呼ばれている。ｐｏｐｃｎｔは式（５７）のように定義される。

【０１３０】

【数５６】

$$(-2\alpha + 1)^{k'} \qquad \cdots（５６）$$

【０１３１】

【数５７】

$$\mathrm{popcnt}(\boldsymbol{t}) := \mathrm{weight}((\boldsymbol{t})_2) \qquad \cdots（５７）$$

【０１３２】

また、式（５２）の前半の$t_l = 1$となる部分の積についても入力ベクトルｔの１が立っている部分をカウントし、これを繰り返し回数として設定すればよい。以上から数値実験アルゴリズムを以下のようにまとめる。

【０１３３】

手順　１：二元対称通信路ＢＳＣのビット反転確率をαとする。

手順　２：$H_2 = [(h_m)_{10}, \cdots, (h_{n-1})_{10}]$を乱数を用いて生成する。

手順　３：ｆｏｒ　ｌｏｏｐ：α＝０．０，…，０．５｛
手順　４：　ｔｅｍｐ２を０．０で初期化する。
手順　５：　ｆｏｒ　ｌｏｏｐ：（ｔ）$_{10}$＝０，…，$2^{m}-1$｛
手順　６：　　ｓ＝φＵ（（ｔ）$_{10}$）
手順　７：　　ｔｅｍｐ１＝ｐｏｐｃｎｔ（（ｔ）$_{10}$）
手順　８：　　ｆｏｒ　ｌｏｏｐ：ｌ＝ｍ，…，ｎ－１｛
手順　９：　　　ｔｅｍｐ１＝ｔｅｍｐ１＋｛ｐｏｐｃｎｔ（（ｔ）$_{10}$ＡＮＤｈ$_{l}$）ｍｏｄ２｝｝
手順１０：　　$s_e=(-2\alpha+1)^{temp1}$
手順１１：　　ｔｅｍｐ＝｜ｓ－s_e｜^{2}
手順１２：　　ｔｅｍｐ２＝ｔｅｍｐ２＋ｔｅｍｐ｝
手順１３：　αとＲｏｏｔ（ｔｅｍｐ１）／Ｒｏｏｔ（2^{m}）をプロットする。｝

【０１３４】

なお、ここでは、上述のアルゴリズムうち、手順１０において行う（－２α＋１）のべき乗を式（５８）に示すようにして計算している。

【０１３５】

【数５８】

$$(-2\alpha+1)^{N}=\exp\left[N\log(-2\alpha+1)\right] \qquad \cdots(58)$$

【０１３６】

ただし、式（５８）においてビット反転確率α＝０．５の時（－２α＋１）＝０となるので、ｌｏｇ（－２α＋１）＝－∞となってしまい計算することができない。そのため、ビット反転確率α＝０．５は除外して考えることにする。

【０１３７】

［（ｎ，ｋ）符号の性能］

（ｎ，ｋ）符号がよい性能を持つということは、コセット符号化の乱数レートとＢＳＣの通信路容量が一致するビット反転確率αで、送信者Ａｌｉｃｅの持つメッセージと盗聴者Ｅｖｅの持つ情報の相関がなくなることである。まず、ビット反転確率αについての条件を式（５９）に示す。

【０１３８】

【数５９】

$$1-h(\alpha)=\frac{k}{n} \qquad \cdots(59)$$

【０１３９】

式（５９）は、ｎとｋとを固定するとαについての方程式と見ることができる。式（５９）の左辺と右辺の交点を求めることを考え、これを図示すると、図１８のようになる。

【０１４０】

図１８は、（ｎ，ｋ）符号の乱数レートとビット反転確率αとの関係の一例を示す図である。ここで、線Ｌ４は、乱数レート（この一例では、ｋ／ｎ）を示す。また、Ｌ５は、１－ｈ（α）を示す。求めたいビット反転確率αが取りうる範囲は、０．０～０．５であると仮定する。（ｎ，ｋ）符号の乱数レート（すなわち、ｎ及びｋ）を固定して、数（５４）を満たすビット反転確率αを方程式の解を求めるアルゴリズムを用いて数値的に求めればよい。方程式の解を求める代表的な数値解法としてニュートン法や二分法が考えられるが、今回は二分法を用いて求めた値を採用することにする。念の為、求めた数値解をグラフにプロットすることで本当に求めたかった値かどうかを再確認しておく。これを用いてプロットした値が図１８の線Ｌ３である。この値を（ｎ，ｋ）符号のビット反転確率の理論値α_{BSC}とし、理論値α_{BSC}付近で評価値Ｆのとる値が小さい程（ｎ，ｋ）符号の性能がよいと定義する。数値実験の基準として、２－ｎｏｒｍの評価において、理論値

α_{BSC}付近で評価値Ｆの値が高々10^{-3}の定数倍程度であれば評価値Ｆが十分に０に近いと判断し、よい（ｎ，ｋ）符号を選択できたと仮定する。１－ｎｏｒｍの評価においても、（2^m）の平方根と評価値Ｆとの積が高々10^{-2}の定数倍程度であれば評価値Ｆが十分に０に近いと判断し、よい（ｎ，ｋ）符号を選択できたと仮定する。さらに、２－ｎｏｒｍの評価および１－ｎｏｒｍの評価の両方を満たす（ｎ，ｋ）符号を完全秘匿性に近い性能を持つ符号と定義する。

【０１４１】

［数値計算のためのパラメータの生成］

（ｎ，ｋ）符号の性能を見るために、プロットする（ｎ，ｋ）の組について考える。ここで、性能のよい符号を構成するためには、ｍをどれだけ増やせばよいかという問題がある。

【０１４２】

従来手法によると、相互情報量Ｊ（Ｓ；Ｓ′）を直接計算していたため、ｍの値を小さく固定したり、メッセージの入力を制限したりすることで、パラメータに制約条件を与えていた。

本実施形態においては、相互情報量を直接計算していないため計算量を削減できることから、パラメータの生成にも工夫ができる。数値実験アルゴリズム上2^m個の入力が必要なため、ｍが大きい場合の計算時間増大が懸念される。そこで、乱数レートを固定した時のｍの値の変化に注目することで、ｍを大きくとらずに計算する方法を考えた。

【０１４３】

図１９は、乱数レートとｍのサンプルとの関係の一例を示す図である。この図１９に示すように、乱数レートが決まれば式（５９）を満たす（ｎ，ｋ）の組みを複数生成できることがわかる。ｉが大きくなればなる程ｍの値は大きくなるのでｍが大きい場合と小さい場合との比較が可能というのが、この方法のメリットである。このことから、ｎを固定してｋを逐次動かして考えるよりも効率がよい。この方法を用いれば、乱数レートが同じ符号を探索することでｍが大きい場合の性能とほぼ同じ性能を持つ符号が存在するかどうかを調べることができる。よって、ｍを比較的小さくしても同様の性能を持っているかどうかを確認することができる。

【０１４４】

ここまで、前提事項と本実施形態の概要について説明した。次に、上述した計算手順によって検査行列Ｈの評価を行う評価装置の一例について説明する。

【０１４５】

［評価装置の構成］

図１は、本実施形態の評価装置１０の機能構成の一例を示す図である。評価装置１０は、一様特性関数算出部１１０と、ノイズ特性関数算出部１２０と、評価値算出部１３０とを備える。また、評価装置１０は、ビット反転確率αと、検査行列Ｈと、入力ベクトルｔとを取得する取得部（不図示）を備える。ここで、ビット反転確率αとは、盗聴通信路Ｅのビット反転確率である。検査行列Ｈとは、盗聴通信路符号化方式における公開パラメータである。入力ベクトルｔとは、確率変数Ｓｅの確率分布を多変数離散フーリエ変換した関数の入力ベクトルである。ここで、確率変数ＳｅをノイズベクトルＳｅともいう。ノイズベクトルＳｅとは、盗聴通信路Ｅを介して取得される盗聴者受信ビット列Z^nと検査行列Ｈとから得られる盗聴者推定メッセージｓ′に含まれる、ビット反転確率αに基づくノイズを示すビット列である。

【０１４６】

これら各パラメータのうち検査行列Ｈ及び入力ベクトルｔは、入力ベクトル・検査行列の縦ベクトル成分算出部２０によって算出される。なお、この一例では、評価装置１０と入力ベクトル・検査行列の縦ベクトル成分算出部２０とが別の装置であるとして説明するが、評価装置１０が、入力ベクトル・検査行列の縦ベクトル成分算出部２０を備えていてもよい。

【０１４７】

一様特性関数算出部１１０は、上述した式（４６）に示すように、入力ベクトルｔに基づいて、一様分布の特性関数である一様特性関数φＵ（ｔ）を算出する。

【０１４８】

ノイズ特性関数算出部１２０は、上述した式（３０）に示すように、入力ベクトルｔと、検査行列Ｈの縦ベクトル成分h_iと、ビット反転確率αとに基づいて、ノイズベクトルＳｅの確率分布の特性関数であるノイズ特性関数φＳｅ（ｔ）を算出する。

なお、ノイズ特性関数φＳｅ（ｔ）が、検査行列Ｈの縦ベクトル成分h_iに基づいて算出されるのは一例であって、ノイズ特性関数φＳｅ（ｔ）は、検査行列Ｈの横ベクトル成分に基づいて算出されてもよい。

【０１４９】

評価値算出部１３０は、ノイズ特性関数算出部１２０が算出するノイズ特性関数φＳｅ（ｔ）と、ビット反転確率αとに基づいて、検査行列Ｈの評価値Ｆ（φＵ，φＳｅ）をビット反転確率α毎に算出する。この検査行列Ｈの評価値Ｆ（φＵ，φＳｅ）を、単に評価値Ｆとも記載する。

【０１５０】

ここで、式（５１）及び式（５２）に示したように、ノイズ特性関数φＳｅ（ｔ）は、入力ベクトルｔと検査行列Ｈの縦ベクトル成分h_iとの内積と、ビット反転確率αとによって求められる。評価値算出部１３０は、式（５３）に示したように、入力ベクトルｔと、検査行列Ｈの縦ベクトル成分h_iとの内積を求めることにより、評価値Ｆを算出する。

【０１５１】

また、評価値算出部１３０は、ノイズ特性関数φＳｅ（ｔ）と、一様特性関数算出部１１０が算出する一様特性関数φＵ（ｔ）とのノルムをビット反転確率α毎に検査行列Ｈの評価値Ｆとして算出する。

【０１５２】

また、評価値算出部１３０は、ノイズ特性関数φＳｅ（ｔ）と、一様特性関数φＵ（ｔ）との２ノルムを算出し、算出した２－ｎｏｒｍを１－ｎｏｒｍに変換することにより、評価値Ｆを算出してもよい。

【０１５３】

［評価装置の動作］

次に、図２を参照して、評価装置１０による評価値Ｆの算出手順の一例について説明する。

図２は、本実施形態の評価装置１０の評価値Ｆを算出する概略動作の一例を示す図である。

（ステップＳｔ１０）評価装置１０の取得部（不図示）は、検査行列Ｈの縦ベクトル成分h_iを取得する。

（ステップＳｔ２０）評価装置１０の取得部（不図示）は、入力ベクトルｔを取得する。

（ステップＳｔ３０）評価装置１０は、ビット反転確率αを更新する。ここで、評価装置１０は、ビット反転確率αを０．０～０．５の範囲で所定の増分だけ値を増加させることにより、ビット反転確率αを更新する。例えば、評価装置１０は、ビット反転確率α＝０．０を初期値として０．１ずつ増加させながらビット反転確率αが０．５に達するまで、ステップＳｔ４０～ステップＳｔ９０の処理を繰り返し実行する。

【０１５４】

（ステップＳｔ４０）一様特性関数算出部１１０は、ステップＳｔ２０において取得された入力ベクトルｔに基づき、一様特性関数φＵ（ｔ）を算出する。

（ステップＳｔ５０）ノイズ特性関数算出部１２０は、ステップＳｔ１０において取得された縦ベクトル成分h_i及びステップＳｔ２０において取得された入力ベクトルｔに基づき、ノイズ特性関数φＳｅ（ｔ）を算出する。ここで、図３を参照して、ノイズ特性関数φＳｅ（ｔ）の算出手順の詳細について説明する。

【０１５５】

図３は、本実施形態のノイズ特性関数算出部１２０によるノイズ特性関数φＳｅ（ｔ）の算出手順の一例を示す図である。

（ステップＳｔ５１０）変数ｔｅｍｐ及び変数ｌを初期化する。

（ステップＳｔ５２０）入力ベクトルｔ、縦ベクトル成分h_lをいずれもビット列とみなして、入力ベクトルｔと縦ベクトル成分h_lとの論理積を算出する。

（ステップＳｔ５３０）ビット列のうちステップＳｔ５２０において算出された論理積が「１」であるビット列の数を計数する。

（ステップＳｔ５４０）ステップＳｔ５３０において計数された結果を２で除した余り（剰余）が「１」である場合には、変数ｔｅｍｐをインクリメントする。

（ステップＳｔ５５０）変数ｌが（ｎ－１）に達しているか否かを判定する。変数ｌが（ｎ－１）に達していない（ステップＳｔ５５０；ＮＯ）場合には、変数ｌをインクリメントして（ステップＳｔ５６０）、処理をステップＳｔ５２０に戻す。変数ｌが（ｎ－１）に達している場合（ステップＳｔ５５０；ＹＥＳ）には、処理をステップＳｔ５７０に進める。

（ステップＳｔ５７０）ノイズ特性関数φＳｅ（ｔ）＝（－２α＋１）^{temp}として、ノイズ特性関数φＳｅ（ｔ）を算出する。

【０１５６】

（ステップＳｔ６０）図２に戻り、評価値算出部１３０は、ステップＳｔ４０において算出された一様特性関数φＵ（ｔ）と、ステップＳｔ５０において算出されたノイズ特性関数φＳｅ（ｔ）とに基づいて、評価値Ｆを算出する。

（ステップＳｔ７０）評価装置１０は、横軸をビット反転確率α、縦軸を評価値Ｆとして評価値Ｆをプロットする。

ここで、評価装置１０は、入力ベクトルｔをビット列とみなした場合の、すべての成分について評価値Ｆを算出し（ステップＳｔ８０）、評価値Ｆのプロットを繰り返す。また、評価装置１０は、ビット反転確率αが０．５に達するまでビット反転確率αを更新して（ステップＳｔ９０）、評価値Ｆのプロットを繰り返す。この評価装置１０による評価値Ｆのプロットの一例を図４及び図５に示す。

【０１５７】

［評価装置による評価結果の一例］

図４は、本実施形態の評価装置１０による評価値Ｆのプロットの一例（その１）を示す図である。図５は、本実施形態の評価装置１０による評価値Ｆのプロットの一例（その２）を示す図である。この一例において、図４には、Ｔ（ＢＳＣ）＝０．５としたときの（ｎ，ｋ）＝（１０，５），（４０，２０），（６０，３０）についての実験結果のグラフをプロットした。図５には、Ｔ（ＢＳＣ）＝０．５としたときの（ｎ，ｋ）＝（２０，１０），（３０，１５），（５０，２５），（６０，３０）についての実験結果のグラフをプロットした。いずれも、グラフは縦軸を２－ｎｏｒｍの評価値Ｆとし、横軸を二元対称通信路ＢＳＣのビット反転確率αとしている。なお、符号の性能をチェックするために、これらの図の線Ｌ１によって理論値α_{BSC}をプロットした。また，理論値α_{BSC}付近の評価値Ｆの差をわかりやすくするため、理論値α_{BSC}付近のｎの値と評価値Ｆとの関係を図６に示す。

【０１５８】

図６は、本実施形態の理論値α_{BSC}付近の評価値Ｆの一例を示す図である。これらのデータから、理論値α_{BSC}付近の評価値Ｆが（ｎ，ｋ）＝（６０，３０）で約1.449×10^{-3}になっているため、２－ｎｏｒｍにおいて（ｎ，ｋ）＝（６０，３０）の場合、上述した（ｎ，ｋ）符号の条件を満たした。この結果からｍ＝ｎ－ｋ＝３０くらいであれば検査行列Ｈの評価として十分と判断し、（ｎ，ｋ）＝（４０，１０）とすることで再度実験を行った。（ｎ，ｋ）＝（４０，１０）とした時の結果を図７に示す。

【０１５９】

図７は、本実施形態において（ｎ，ｋ）＝（４０，１０）とした場合の評価値Ｆの一例を示す図である。同図の場合、理論値α_{BSC}付近の評価値Ｆが約3.233×10^{-3}

であった。よって、（ｎ，ｋ）＝（４０，１０）とした場合において、（ｎ，ｋ）＝（６０，３０）とした場合と同様の結果が得られたといえる。

【０１６０】

図８は、本実施形態において（ｎ，ｋ）＝（６０，３０）とした場合の評価値Ｆの一例を示す図である。２－ｎｏｒｍにおいて（ｎ，ｋ）＝（６０，３０）の場合に、よい性能を持つ検査行列Ｈを構成できた。このため、この結果を用いて横軸は二元対称通信路ＢＳＣのビット反転確率αを、縦軸はＲｏｏｔ（2^{30}）・Ｆとしてプロットした。なお、ここでＲｏｏｔ（2^{30}）とは、2^{30}の平方根である。１－ｎｏｒｍの評価においては、グラフの縦軸と横軸との対応が非常にわかりづらいため、観察したいＲｏｏｔ（2^{30}）・Ｆの値に線Ｌ２を引くことにする。

【０１６１】

（ｎ，ｋ）＝（６０，３０）において、２－ｎｏｒｍの評価については理論値α_{BSC}付近で評価値Ｆが０に近い値をとったのにも関わらず、１－ｎｏｒｍの評価においては、理論値α_{BSC}付近のＲｏｏｔ（2^{30}）・Ｆの値が約４７．４６６であった。これでは、Ｒｏｏｔ（2^{30}）・Ｆ→０とはいえないため、１－ｎｏｒｍの評価に関して（ｎ，ｋ）＝（６０，３０）では適さないことがわかる。

【０１６２】

２－ｎｏｒｍでは、ｍ＝ｎ－ｋ＝３０とした場合、理論値α_{BSC}付近で評価値Ｆが０に近づくことがわかったので、ｍ＝３０とした場合に、Ｒｏｏｔ（2^{30}）・Ｆ→０となるような（ｎ，ｋ）符号を探索することにする。一般にｎが大きい時に大数の法則の効果が出てくるので、今回はｎ＝４００として再実験を行った。上述した実験結果で、２－ｎｏｒｍの評価に関してｍ＝３０程度とれば評価値Ｆが０に十分近づくことがわかったため（ｎ，ｋ）＝（４００，３７０）で実験を行った。

【０１６３】

図９は、本実施形態において（ｎ，ｋ）＝（４００，３７０）とした場合の評価値Ｆの実験結果の一例を示す図である。同図においては、横軸を二元対称通信路ＢＳＣのビット反転確率αとして、縦軸を評価値Ｆにとってプロットしている。

図１０は、本実施形態において（ｎ，ｋ）＝（４００，３７０）とした場合の評価値Ｆの実験結果の一例を示す図である。横軸を二元対称通信路ＢＳＣのビット反転確率αとして、縦軸をＲｏｏｔ（2^{30}）・Ｆでプロットしたグラフである。なお、本節においてグラフの縦軸と横軸の対応をわかりやすくするため、Ｒｏｏｔ（2^{30}）・Ｆについては上述と同様に観察したいＲｏｏｔ（2^{30}）・Ｆの値に線Ｌ２を引くことにする。

【０１６４】

数値実験の結果（ｎ，ｋ）＝（４００，３７０）においてαＢＳＣ付近の値が、Ｆ＝｜｜ＰＳ－ＰＳｅ｜｜２　１．６３６×１０－６であった。さらに、この両辺にＲｏｏｔ（2^{30}）をかけると、Ｒｏｏｔ（2^{30}）・Ｆ　０．０５４となった。よって、（ｎ，ｋ）＝（４００，３７０）の場合、上述した（ｎ，ｋ）符号の基準を満たすため、本実施形態で定義する完全秘匿性に近い性能を持つ（ｎ，ｋ）符号を選択できた。この場合、ファネス型不等式の右辺に｜｜ＰＳ－ＰＳｅ｜｜１＝Ｒｏｏｔ（2^{30}）・Ｆ　０．０５４を代入すると、約１．８４７という値が得られた。

【０１６５】

［変形例］

以上示した数値実験で用いた方法は、二元対称通信路ＢＳＣのビット反転確率αの刻み幅（増分）ごとに２－ｎｏｒｍの評価値Ｆの計算を行っていた。評価値Ｆの計算において、入力が2^{m}個ある。よって、ビット反転確率αの刻み幅（増分）ごとに2^{m}回のループが必要であった。以降では、2^{m}回のループを削減する演算手順について説明する。

まず、一様分布に関する一様特性関数φＵ（ｔ）と盗聴者の持つ情報に関するノイズ特性関数φＳｅ（ｔ）の入力がともに零ベクトル０ならば、φＵ（０）＝φＳｅ（０）＝１が成立することより、式（６０）が成り立つ。

【０１６６】

【数６０】

$$|\phi_U(\mathbf{0}) - \phi_{S_e}(\mathbf{0})|^2 = 0 \qquad \cdots (60)$$

【０１６７】

以下、Ｋ：＝Ｆ$^{m}{}_{2}$－｛０｝とすると、２－ｎｏｒｍの評価値Ｆを計算する際の総和では、ｔ∈Ｋとして一般性を失わない。また、ｔ∈Ｋに対して、式（６１）及び式（６２）が成り立つ。

【０１６８】

【数６１】

$$1 \leq \mathrm{popcnt}(\boldsymbol{t}) \leq m \qquad \cdots (61)$$

【０１６９】

【数６２】

$$0 \leq \sum_{l=m}^{n-1} \{\mathrm{popcnt}(\boldsymbol{t} \ \mathrm{AND} \ \boldsymbol{h}_l) \bmod 2\} \leq k \qquad \cdots (62)$$

【０１７０】

よって、式（６３）が成り立つ。

【０１７１】

【数６３】

$$1 \leq \mathrm{popcnt}(\boldsymbol{t}) + \sum_{l=m}^{n-1} \{\mathrm{popcnt}(\boldsymbol{t} \ \mathrm{AND} \ \boldsymbol{h}_l) \bmod 2\} \leq n \qquad \cdots (63)$$

【０１７２】

このことを利用すると格納領域ｎのリストｂに総乗の回数を格納することで、２^{m}回のループをビット反転確率αの刻み幅ごとに実行する必要は無くなるため、１回のみ２^{m}回のループを実行するだけで済む。この前処理アルゴリズムを以下にまとめる。

【０１７３】

手順１：格納領域ｎのリストｂを０で初期化する。
手順２：ｆｏｒ　ｌｏｏｐ：（ｔ）$_{10}$＝１，…，２^{m}－１｛
手順３：　ｊ＝ｐｏｐｃｎｔ（（ｔ）$_{10}$）
手順４：　ｆｏｒ　ｌｏｏｐ：ｌ＝ｍ，…，ｎ－１｛
手順５：　　ｉｆ　ｐｏｐｃｎｔ（（ｔ）$_{10}$　ＡＮＤ　（ｈ$_{l}$）$_{10}$）＝１ｍｏｄ２｛
手順６：　　ｊ＝ｊ＋１　｝｝
手順７：　ｂ［ｊ］をインクリメントする。｝

【０１７４】

この前処理アルゴリズムを適用することによって、式（６４）の逆像でＫをｎ個の部分集合に分割できる。すなわち、式（６５）となるので、式（６６）が成り立つ。

【０１７５】

【数６４】

$$f(\boldsymbol{t}) := \mathrm{popcnt}(\boldsymbol{t}) + \sum_{l=m}^{n-1} \{\mathrm{popcnt}(\boldsymbol{t} \ \mathrm{AND} \ \boldsymbol{h}_l) \bmod 2\} \qquad \cdots (64)$$

【０１７６】

【数６５】

$$\mathbb{K} = K_1 \cup \cdots \cup K_j \cup \cdots \cup K_n$$
$$K_j \cap K_\beta = \emptyset \quad (j \neq \beta) \qquad \cdots (65)$$
$$\#K_j = \mathrm{b[j]}$$

【０１７７】

【数６６】

$$\sum_{\mathrm{j}=1}^{n} \mathrm{b[j]} = \#\mathbb{K} = 2^m - 1 \qquad \cdots (66)$$

【０１７８】

このことから、２－ｎｏｒｍの評価値Ｆは、式（６７）のように書き直せる。

【０１７９】

【数６７】

$$F(\phi_{S_e}) = \frac{1}{\sqrt{2^m}} \sqrt{\sum_{t \in \mathbb{K}} |\phi_{S_e}(t)|^2} = \frac{1}{\sqrt{2^m}} \sqrt{\sum_{t \in \mathbb{K}} \{(-2\alpha+1)^{f(t)}\}^2}$$
$$= \frac{1}{\sqrt{2^m}} \sqrt{\sum_{t \in \mathbb{K}} (-2\alpha+1)^{2f(t)}} = \frac{1}{\sqrt{2^m}} \sqrt{\sum_{\mathrm{j}=1}^{n} \mathrm{b[j]}(-2\alpha+1)^{2\mathrm{j}}}$$
$$\cdots (67)$$

さらに、ビット反転確率α＝０の場合には、評価値Ｆの定義に直接、α＝０を代入することで、ノイズ特性関数φＳｅ（ｔ）は、式（６８）として表される。

【０１８０】

【数６８】

$$F(\phi_{S_e}) = \frac{\sqrt{2^m - 1}}{\sqrt{2^m}} \qquad \cdots (68)$$

【０１８１】

ビット反転確率α＝０．５の場合についても、評価値Ｆの定義に直接代入することで、ノイズ特性関数φＳｅ（ｔ）は、式（６９）として表される。

【０１８２】

【数６９】

$$F(\phi_{S_e}) = 0 \qquad \cdots (69)$$

【０１８３】

また、式（７０）に示すｐａｒｉｔｙ関数も用いることとする。

【０１８４】

【数７０】

$$\mathrm{parity}(\boldsymbol{t}) := \begin{cases} 1 & (\mathrm{popcnt}(\boldsymbol{t}) = 1 \bmod 2) \\ 0 & (\mathrm{popcnt}(\boldsymbol{t}) = 0 \bmod 2) \end{cases} \quad \cdots (70)$$

【０１８５】

上述した考察を加味した上で、数値実験アルゴリズムを以下にまとめ直す。

【０１８６】

手順１　：二元対称通信路ＢＳＣのビット反転確率をαとする。
手順２　：$H_2 = [(h_m)_{10}, \cdots, (h_{n-1})_{10}]$を、乱数を用いて生成する。
手順３　：格納領域ｎのリストｂ［］を０で初期化する。
手順４　：ｆｏｒ　ｌｏｏｐ：（ｔ）$_{10}$＝１，…，2^m-1｛
手順５　：　ｊ　＝　ｐｏｐｃｎｔ（（ｔ）$_{10}$）
手順６　：　ｆｏｒ　ｌｏｏｐ：ｌ＝ｍ，…，ｎ－１
手順７　：　　ｉｆ　ｐａｒｉｔｙ（（ｔ）$_{10}$　ＡＮＤ　（h_l）$_{10}$）＝１｛
手順８　：　　ｊ＝ｊ＋１｝｝
手順９　：　ｂ［ｊ］をインクリメントする。｝
手順１０：ｆｏｒ　ｌｏｏｐ：α＝０．０，…，０．５｛
手順１１：　ｔｅｍｐ１を０．０で初期化する。
手順１２：　ｉｆ　α＝０．０　ｏｒ　α＝０．５｛
手順１３：　　ｉｆ　α＝０．０｛
手順１４：　　ｔｅｍｐ１＝2^m-1｝｝
手順１５：　ｅｌｓｅ｛
手順１６：　　ｔｅｍｐ４を０．０で初期化する。
手順１７：　　ｆｏｒ　ｌｏｏｐ：ｊ＝１，…，ｎ｛
手順１８：　　ｉｆ　ｊ＝１｛
手順１９：　　ｔｅｍｐ３＝２＊ｌｏｇ（－２α＋１）
手順２０：　　ｔｅｍｐ４＝ｔｅｍｐ３｝
手順２１：　　ｅｌｓｅ｛
手順２２：　　ｔｅｍｐ４＝ｔｅｍｐ４＋ｔｅｍｐ３｝
手順２３：　　ｉｆ　ｂ［ｊ］≠０｛
手順２４：　　ｔｅｍｐ２＝ｂ［ｊ］＊ｅｘｐ［ｔｅｍｐ４］
手順２５：　　ｔｅｍｐ１＝ｔｅｍｐ１＋ｔｅｍｐ２｝｝｝
手順２６：　Ｒｏｏｔ（ｔｅｍｐ１）／Ｒｏｏｔ（2^m）をプロットする。｝

【０１８７】

この変形例における評価装置１０による評価値Ｆの算出手順の一例について、より具体的に説明する。

図１１は、本実施形態の変形例に係る評価装置１０の評価値Ｆを算出する概略動作の一例を示す図である。

（ステップＳｔ１００）評価装置１０の取得部（不図示）は、検査行列Ｈの縦ベクトル成分h_lを取得する。

（ステップＳｔ１１０）評価装置１０の取得部（不図示）は、入力ベクトルｔを取得する。

（ステップＳｔ１２０）評価装置１０は、評価値Ｆを算出する。ここで、図１２を参照して、評価値Ｆの算出手順の詳細について説明する。

【０１８８】

図１２は、本実施形態の変形例に係る評価装置１０による評価値Ｆの算出手順の一例を示す図である。評価装置１０が備えるコンピュータが動作主体となって、以降の各ステップＳｔを処理する。

（ステップＳｔ２１０）格納領域ｎのリストｂ（ｂ［ｊ］の各要素）を初期化する。
（ステップＳｔ２２０）入力ベクトルｔをビット列とみなして、「１」であるビット列の数を計数する。
（ステップＳｔ２３０）入力ベクトルｔ及び縦ベクトル成分h_lをいずれもビット列とみなして、入力ベクトルｔと縦ベクトル成分h_lとの論理積のパリティを式（７０）により算出する。パリティが「１」である場合（ステップＳｔ２３０；ＹＥＳ）には、変数ｊをインクリメントする。
（ステップＳｔ２４０）変数ｌが（ｎ－１）に達しているか否かを判定する。変数ｌが（ｎ－１）に達していない（ステップＳｔ２４０；ＮＯ）場合には、変数ｌをインクリメントして（ステップＳｔ２６０）、処理をステップＳｔ２３０に戻す。変数ｌが（ｎ－１）に達している場合（ステップＳｔ２４０；ＹＥＳ）には、処理をステップＳｔ２７０に進める。
（ステップＳｔ２７０）リストｂ［ｊ］をインクリメントする（リストｂの要素の値を１増加させる）。
（ステップＳｔ２８０）入力ベクトルｔのすべての成分について算出したか否かを判定する。入力ベクトルｔのすべての成分について算出していない場合（ステップＳｔ２８０；ＮＯ）には、処理をステップＳｔ２２０に戻す。入力ベクトルｔのすべての成分について算出した場合（ステップＳｔ２８０；ＹＥＳ）には、処理をステップＳｔ２９０に進める。

【０１８９】

（ステップＳｔ２９０）ビット反転確率α及び変数ｊを初期化する。
（ステップＳｔ３００）変数ｔｅｍｐ１を初期化する。
（ステップＳｔ３１０）ビット反転確率αの値によって処理を切り替える。具体的には、ビット反転確率α＝０の場合には、処理をステップＳｔ２３０に進める。ビット反転確率α＝０．５の場合には、処理を終了する。ビット反転確率α＞０かつ＜０．５の場合には、処理をステップＳｔ３４０に進める。
（ステップＳｔ３２０）ビット反転確率α＝０の場合、変数ｔｅｍｐ１に（2^m-1）を代入して、ビット反転確率αをインクリメントし（ステップＳｔ３３０）、処理をステップＳｔ３００に戻す。
（ステップＳｔ３４０）変数ｔｅｍｐ４を初期化する。
（ステップＳｔ３５０）変数ｊ＝１であるか否かを判定する。変数ｊ＝１である場合には、変数ｔｅｍｐ３＝２＊ｌｏｇ（－２α＋１）を求め（ステップＳｔ３６０）、求めた変数ｔｅｍｐ３を変数ｔｅｍｐ４に代入する（ステップＳｔ３７０）。変数ｊ＝１でない場合には、変数ｔｅｍｐ３と変数ｔｅｍｐ４との和を変数ｔｅｍｐ４に代入する（ステップＳｔ３８０）。
（ステップＳｔ３９０）リストｂ［ｊ］≠０であるか否かを判定する。リストｂ［ｊ］≠０でない（つまり、リストｂ［ｊ］＝０である）場合には、変数ｊをインクリメントして（ステップＳｔ４４０）、処理をステップＳｔ３５０に戻す。リストｂ［ｊ］≠０である場合には、処理をステップＳｔ４００に進める。
（ステップＳｔ４００）リストｂ［ｊ］＊ｅｘｐ［ｔｅｍｐ４］を求め、求めた値を変数ｔｅｍｐ２に代入する。
（ステップＳｔ４１０）変数ｔｅｍｐ１と変数ｔｅｍｐ２との和を変数ｔｅｍｐ１に代入する。
（ステップＳｔ４２０）変数ｊがｎに達しているか否かを判定する。変数ｊがｎに達していない場合には、変数ｊをインクリメントして（ステップＳｔ４４０）、処理をステップＳｔ３５０に戻す。変数ｊがｎに達している場合には、処理をステップＳｔ４３０に進める。
（ステップＳｔ４３０）Ｒｏｏｔ（ｔｅｍｐ１）／Ｒｏｏｔ（2^m）を算出し、算出した結果を、ビット反転確率αについての評価値Ｆとして出力する。

【０１９０】

上述ではＫの分割を考えていたが、理論的にはＫの分割というよりもF^m_2の分割である。ここでは、ｆ（ｔ）＝０⇔ｔ＝０と０≠∈Ｋ（ここで、０≠∈Ｋの記号は、０（ゼロ）がＫの要素でないことを示す。）から、Ｋをｎ分割した。F^m_2の分割を考える際は、０∈F^m_2（このF^m_2はビット列を示す。）からF^m_2のｎ＋１分割を考える必要がある。よって、２－ｎｏｒｍの評価値Ｆの計算の大部分はF^m_2が分割された集合の要素数をカウントするという問題に帰着されることがわかる。上述した変形例の数値実験アルゴリズムを用いて（ｎ，ｋ）＝（６０，２０）について横軸を二元対称通信路ＢＳＣのビット反転確率α、縦軸を２－ｎｏｒｍの評価値Ｆとしてプロットした結果を図１３に示す。

【０１９１】

図１３は、本実施形態の変形例のアルゴリズムによる評価値Ｆの実験結果の一例を示す図である。上記パラメータで理論値α_{BSC}付近の評価値ＦについてＦ＝｜｜ＰＳ－ＰＳｅ｜｜$_2$　３．６３６×１０$^{-5}$であるため、２－ｎｏｒｍの評価については上述した基準を満たしている。ここで、｜｜Ａ｜｜$_2$との表現は、Ａの２－ｎｏｒｍを示す。１－ｎｏｒｍの評価については、両辺にＲｏｏｔ（２^{40}）をかけることにより、Ｒｏｏｔ（２^{40}）・Ｆ　３８．１３１であるため、１－ｎｏｒｍの評価については不適切なパラメータである。

改良後（変形例）のアルゴリズムは、改良前のアルゴリズムに比べ、計算時間が減少した。上述した（ｎ，ｋ）＝（６０，２０）（すなわち、ｍ＝ｎ－ｋ＝４０）において、改良前のアルゴリズムの場合、実験環境において約１週間経過しても計算が終わらなかったが、改良後のアルゴリズムの場合、改良前と同一の実験環境において約４時間半で計算が終わった。さらに、（ｎ，ｋ）＝（４００，３７０）の場合、改良前のアルゴリズムであると約２日半かかる計算が、改良後であると、改良前と同一の実験環境において約４分半で計算できた。

【０１９２】

以上説明したように、本実施形態の評価装置１０は、ノイズ特性関数φＳｅ(ｔ)の算出にあたり、式（３０）に示す多変数離散フーリエ級数を利用している。ここで、式（３０）の指数部の演算について、体F_2の演算としてｍｏｄ２の剰余演算を行う。この手順を採用することにより、入力ベクトルｔの離散点を2^m個だけ計算すれば、ノイズ特性関数φＳｅ（ｔ）を求めることができる。すなわち、本実施形態の評価装置１０によれば、盗聴通信路符号化における符号化レートの評価値を、実用的な手順により求めることができる。

【０１９３】

また、本実施形態の評価装置１０は、例えば、１変数のｚ変換から逆変換により確率分布を求めることをしない。本実施形態の評価装置１０は、逆変換を行わずに直接フーリエ変換領域における2^m個の離散点を計算することにより、一様特性関数φＵ（ｔ）とノイズ特性関数φＳｅ(ｔ)との２ノルムを直接求める。

【０１９４】

また、本実施形態の評価装置１０は、式（３６）に示す、１ノルムと２ノルムの関係式を利用することにより、盗聴者Ｅｖｅの持つ確率変数Ｓｅと一様分布Ｕの１ノルムの評価を、上述した２ノルムによる演算を経由することで行っている。すなわち、本実施形態の評価装置１０は、一様特性関数φＵ（ｔ）とノイズ特性関数φＳｅ(ｔ)との２ノルムを求めた後、式（３６）の関係を用いて一様分布Ｕとノイズ確率変数Ｓｅとの１ノルムの評価を行う。さらに、式（３５）に示す、ファネス型不等式を利用することにより、盗聴者Ｅｖｅの持つ確率変数Ｓｅのエントロピーの評価を行う。

【０１９５】

また、本実施形態の評価装置１０は、ベクトルにおける１の数を汎用関数であるｐｏｐｃｎｔ（式（５７））によって算出することにより、演算の高速化を図っている。

【０１９６】

また、検査行列Ｈの評価においては、ビット反転確率αを０．０から０．５までの範囲で様々に変えて評価値Ｆを算出する。ここで、ビット反転確率αを様々に変えて評価値Ｆ

を算出する場合、計算オーダーがＯ（２^{m}）になる演算部分が生じる。本実施形態の評価装置１０は、ビット反転確率αを０．０から０．５まで変化させた場合であっても、計算オーダーがＯ（２^{m}）になる演算部分（すなわち、計算負荷が大きい演算部分）を、１回のみに済ませるアルゴリズムによって評価値Ｆを算出する。

したがって、本実施形態の評価装置１０は、従来手法に比べて演算を高速化することができる。

【０１９７】

以上、本発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更を加えることができる。上述した各実施形態に記載の構成を組み合わせてもよい。

【０１９８】

なお、上記の実施形態における各装置が備える各部は、専用のハードウェアにより実現されるものであってもよく、また、メモリおよびマイクロプロセッサにより実現させるものであってもよい。

【０１９９】

なお、各装置が備える各部は、メモリおよびＣＰＵ（中央演算装置）により構成され、各装置が備える各部の機能を実現するためのプログラムをメモリにロードして実行することによりその機能を実現させるものであってもよい。

【０２００】

また、各装置が備える各部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより、制御部が備える各部による処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【０２０１】

また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであってもよく、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであってもよい。

【符号の説明】

【０２０２】

１０…評価装置、２０…入力ベクトル・検査行列の縦ベクトル成分算出部、１１０…一様特性関数算出部、１２０…ノイズ特性関数算出部、１３０…評価値算出部、Ｆ…評価値

【図１】

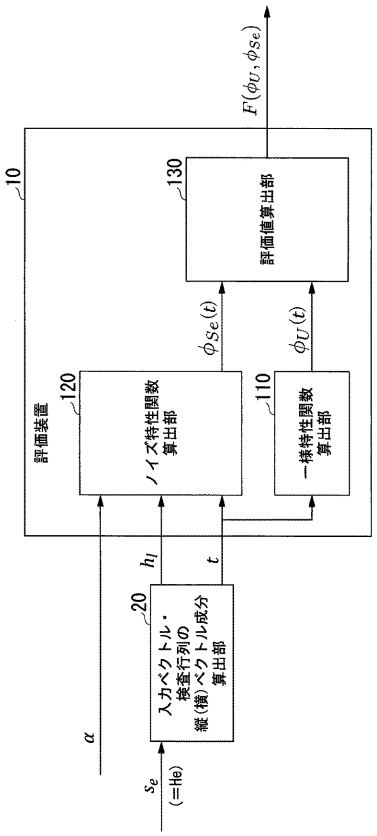


図１

【図２】

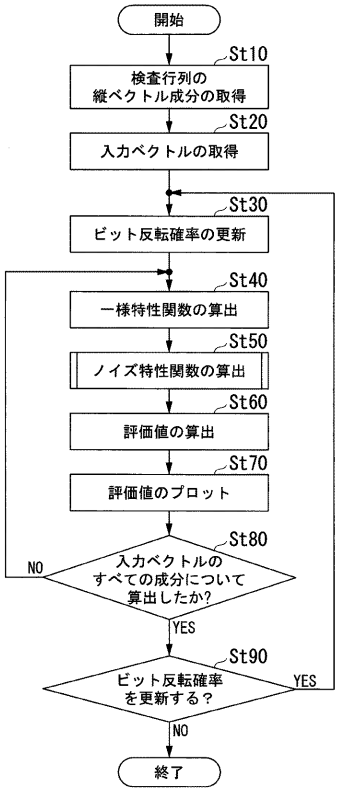


図２

【図３】

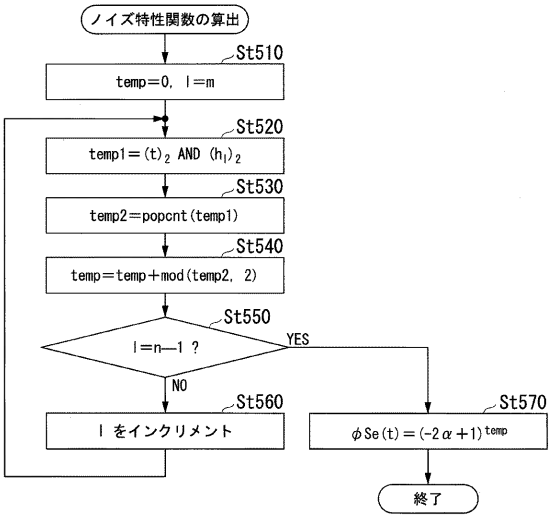


図３

【図４】

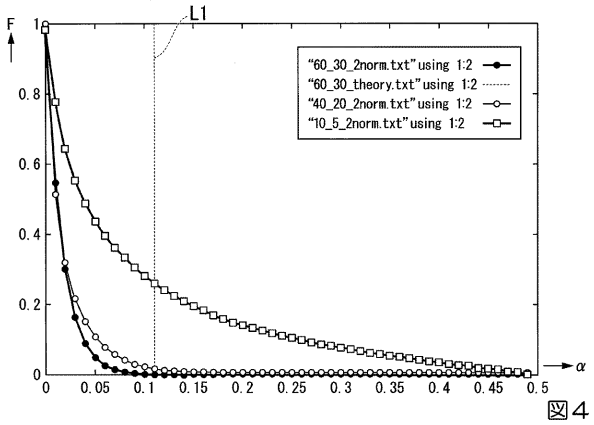


図４

【図５】

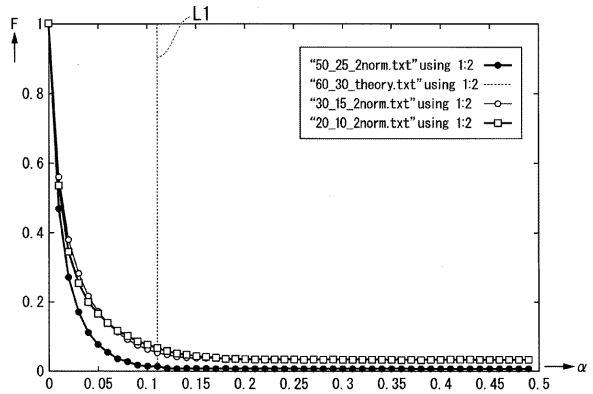


図５

【図６】

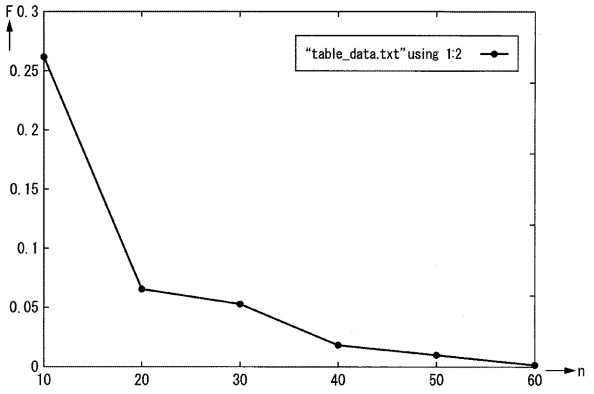


図６

【図７】

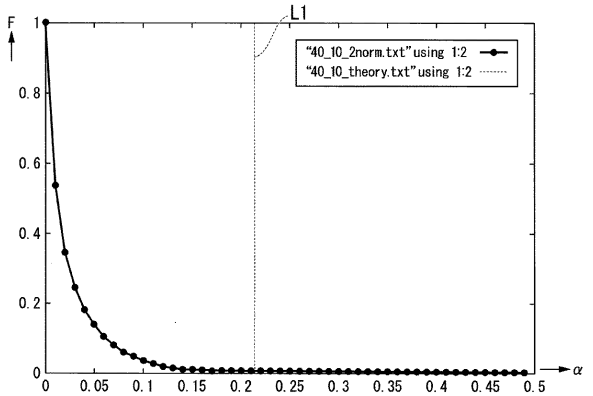


図７

【図８】

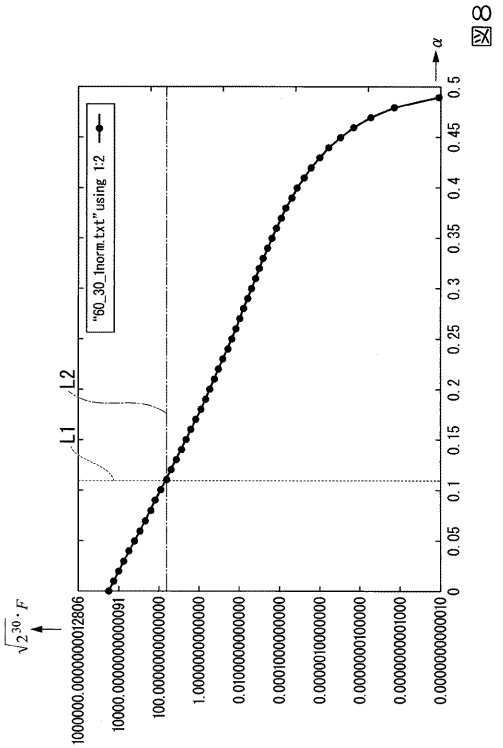


図８

【図９】

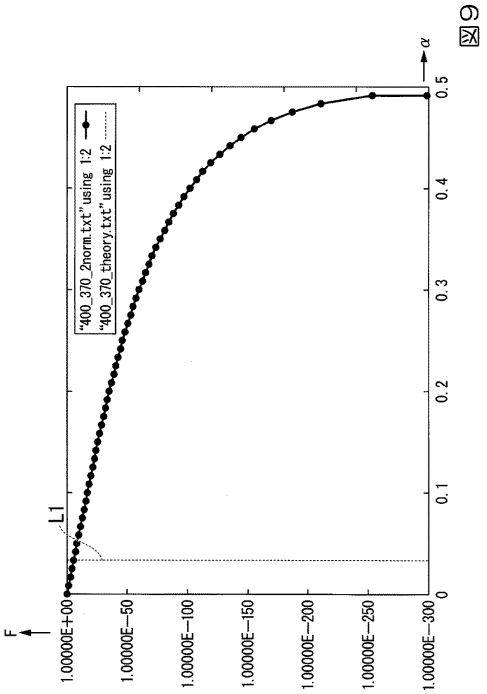


図９

【図１０】

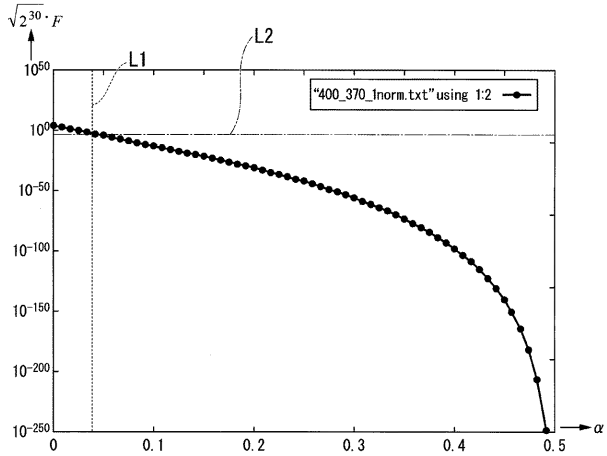


図１０

【図１１】

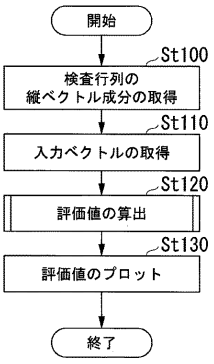


図１１

【図１２】

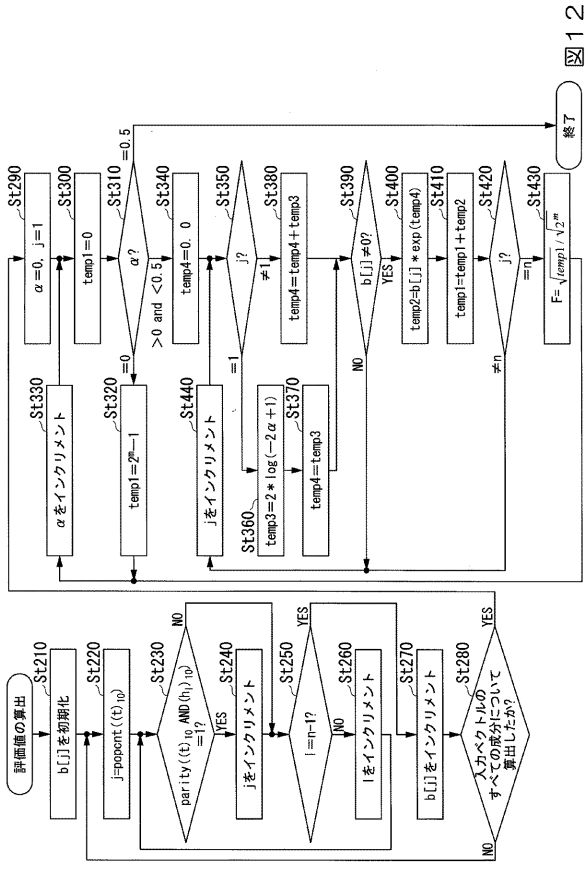


図１２

【図１３】

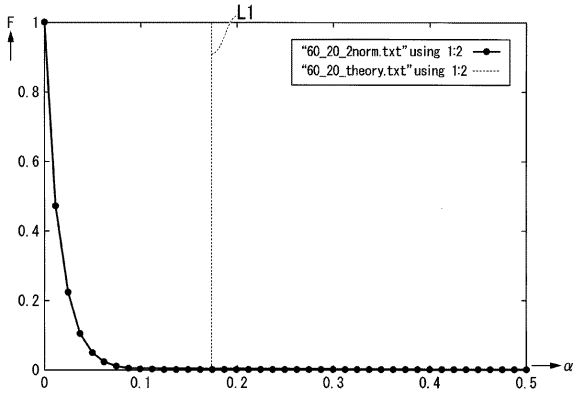


図１３

【図１４】

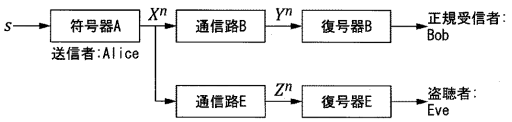


図１４

【図１５】

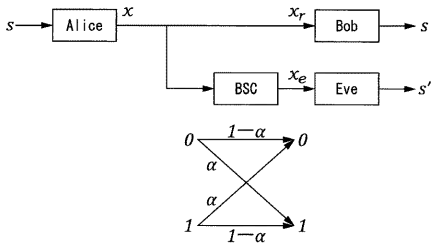


図１５

【図１６】

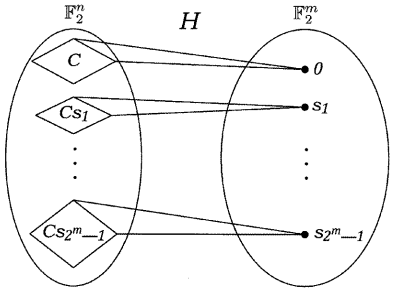


図１６

【図１７】

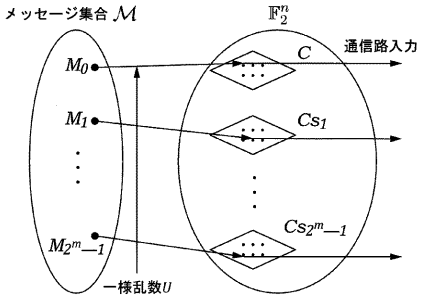


図１７

【図１８】

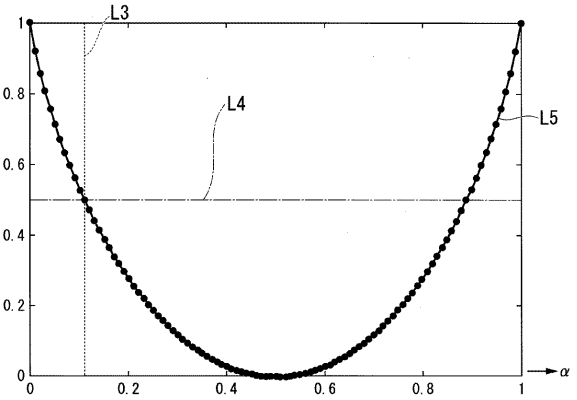


図１８

【図１９】

インデックス	乱数レート：$R_U=k/n$	k	n	m=n−k
1	0.5	5	10	5
2		10	20	10
3		15	30	15
4		20	40	20
5		25	50	25
6		30	60	30
⋮		⋮	⋮	⋮
i		5i	10i	5i

図１９