The 29th Symposium on Information Theory
and Its Applications (SITA2006)
Hakodate, Hokkaido, Japan, Nov. 28 – Dec. 1, 2006

セキュアネットワーク符号化アルゴリズム
— 条件付き正則行列の構成アルゴリズム (I) —
A note on secure network coding algorithms

栗原正純*
KURIHARA, Masazumi

Abstract— In this paper we propose algorithms for constructing secure network codes. Secure network codes are based on a concept of a secure sharing scheme in cryptography. It is known that a secure network code can be constructed by using a conditional regular matrix based on secure sharing scheme for a given linear network code. But a non-trivial and concrete method to find such a conditional regular matrix has not been known clearly. We propose algorithms to find the conditional regular matrix and estimate the time and space complexities of the algorithms.

Keywords— Network coding, secure network coding, coding algorithms, secure sharing scheme

1 まえがき

2002 年に Cai and Yeung[1] により定式化された線型ネットワーク符号におけるセキュアなネットワーク符号化は，暗号理論における秘密分散法の概念に基づく．彼らの発表の後，ランプ型秘密分散法も含めたセキュアなネットワーク符号化に関連する幾つかの研究が行われている [3, 4, 5, 6] ．特に，線型ネットワーク符号が既に与えられている場合，セキュアなネットワーク符号化を実現させるには，ランプ型も含めて秘密分散符号化に従うセキュア変換行列を用いて情報源からの情報シンボルを変換した後，ソースノードから送信すればよいことが知られている [1, 3, 4, 6] ．その秘密分散符号化に従うセキュア変換行列の条件とは，山本 [2] により与えられたランプ型秘密分散法の条件に従えば十分であることが分かっている．

本稿では，ランプ型秘密分散符号化を実現するためのセキュア変換行列を条件付き正則行列ということにする．そして，その条件付き正則行列を求めるアルゴリズムを提案し，符号化を行なう有限体のサイズとアルゴリズムの時間と領域の計算量を評価することを目的とする．

本稿の構成は，以下の通りである．2 では，本稿で用いる線型代数の準備をする．3 では，与えられたベクトル系列の基底を構成するアルゴリズムを与える．このアルゴリズムは，次節に示すランプ型秘密分散符号化に従う条件付き正則行列を求めるアルゴリズムの前処理を実行するアルゴリズムに利用される．4 では，ランプ型秘密分散符号化に従う条件を満たす条件付き正則行列を求める問題を設定し，その解法となるアルゴリズムを提案する．そして，アルゴリズムの計算量について評価する．5 では，前節までに示した条件付き正則行列およびその構成アルゴリズムを用いて，ランプ型秘密分散符号化およびセキュアネットワーク符号化を構成できることを述べる．6 は，結論である．

2 準備

本節では，本稿で用いる線型代数の準備をする．有限体 $\mathbf{F}_q$ 上の線型空間 V の空でない部分集合 $S = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ から生成される V の部分空間を $\langle S\rangle = \langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\rangle := \{\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_n\boldsymbol{x}_n | \alpha_1, \ldots, \alpha_n \in \mathbf{F}_q\}$ と表す．

線型空間 V を有限体 $\mathbf{F}_q$ 上の h 次元線型空間 $\mathbf{F}_q^h$ とする．V の元を列ベクトル $\boldsymbol{x} = (x_1, \ldots, x_h)^T \in \mathbf{F}_q^h$ と表す．ここで，記号 T はベクトルの転置を表す記号である．V の 2 つの元 $\boldsymbol{x}, \boldsymbol{y}$ に対し，内積を $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, \boldsymbol{x}) := \boldsymbol{x}^T\boldsymbol{y} = \sum_{i=1}^h x_i y_i$ と定義する．

定理 1 $h \times h$ 単位行列を E と記す．h 次元正方行列 X に対し，$XY = E$ となる h 次元正方行列 Y が存在すれば X は正則である．$YX = E$ となる Y の存在を仮定しても同様である． ∎

3 基底構成アルゴリズム I

3.1 問題設定 I

はじめに，列ベクトル $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_h$, および, $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_h \in \mathbf{F}_q^h$ を用いた 2 個の $h \times h$ 行列 X と Y を，それぞれ

$$X = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_h)^T, \quad (1)$$
$$Y = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_h) \quad (2)$$

と定義する．ここで，行列 X に関しては，列ベクトル $\boldsymbol{x}_i$ を転置し，行ベクトルとしていることに注意する．また，$h \times h$ 単位行列を E と記す．そして，添字の整数を要素とする添字集合に $I(\subseteq \{1, \ldots, h\})$ を用いる．

本節の問題として，空でない任意の部分集合 $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\} \subset \mathbf{F}_q^h$ に対し，以下の条件を満たす行列 X, Y と添字集合 I を求める問題を考える．

条件 2 以下の式 (3) と (4) が成り立つ．

$$\langle G\rangle = \langle\{\boldsymbol{y}_i | i \in (\{1, \ldots, h\} \setminus I)\}\rangle, \quad (3)$$
$$XY = E. \quad (4)$$

定理 1 より，式 (4) が成り立つならば，Y は正則行列であるから，$\boldsymbol{y}_1, \ldots, \boldsymbol{y}_h$ は線型独立で $\mathbf{F}_q^h$ の基底である．したがって，式 (3) が成り立つならば，$\dim\langle G\rangle = h - |I|$ であり，$\{\boldsymbol{y}_i | i \in (\{1, \ldots, h\} \setminus I)\}$ は $\langle G\rangle$ の基底となる．

以上より，本節で設定する問題を以下に示す．

問題 1 任意に与えられた空でない部分集合 $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\} \subset \mathbf{F}_q^h$ に対し，条件 2 を満たす Y, X, I を求めよ． ∎

3.2 アルゴリズム I

問題 1 を解く一方法を以下に示す．

アルゴリズム 1 (Algorithm I)

Input : $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\}$
Output: Y, X, and I

Initial: $X = Y := E$, $I := \{1, 2, \ldots, h\}$, and $k := 1$.
Step 1) Input: $G = \{\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_n\}$.
Step 2) if $^\exists j \in I$ such that $(\boldsymbol{g}_k, \boldsymbol{x}_j) \neq 0$, then goto 3), else goto 5).

* 〒 182-8585 電気通信大学情報通信工学科． Dept. of Infor. and Comm. Eng., Univ. of Electro-Comm., Tokyo, 182-8585 Japan. E-mail: kuri@ice.uec.ac.jp

Step 3) for some j such that $(\boldsymbol{g}_k, \boldsymbol{x}_j) \neq 0$,

$$\begin{aligned} \boldsymbol{y}_j &:= \boldsymbol{g}_k \\ \boldsymbol{x}_j &:= (\boldsymbol{y}_j, \boldsymbol{x}_j)^{-1}\boldsymbol{x}_j \\ \boldsymbol{x}_i &:= \boldsymbol{x}_i - (\boldsymbol{y}_j, \boldsymbol{x}_i)\boldsymbol{x}_j \text{ for all } i = 1, \ldots, h \text{ s.t.} i \neq j \\ I &:= I \setminus \{j\} \end{aligned}$$

Step 4) if $I = \emptyset$, then goto 6), else goto 5).
Step 5) $k := k + 1$. if $k > n$, then goto 6), else goto 2).
Step 6) Output: X, Y, and I and halt. ∎

以下に，アルゴリズムの出力データ X, Y, I が条件 2 を満たすことを示そう．

補題 3 (Lemma 5 in [8]) $XY = E$ が成り立つと仮定する．ある列ベクトル $\boldsymbol{g} \in \mathbf{F}_q^h$ とある添え字 $j \in \{1, \ldots, h\}$ に対し，$(\boldsymbol{g}, \boldsymbol{x}_j) = 0$ であると仮定する．このとき，$\boldsymbol{g} = \sum_{\substack{i=1 \\ i \neq j}}^{h} c_i \boldsymbol{y}_i$ と表すことができる．ここで，$c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_h \in \mathbf{F}_q$ である．すなわち，$\boldsymbol{g}$ は $h-1$ 個の $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{j-1}\boldsymbol{y}_{j+1}, \ldots, \boldsymbol{y}_h$ に線型従属である． ∎

補題 3 から以下の系が得られる．

系 4 $XY = E$ が成り立つと仮定する．列ベクトル $\boldsymbol{g} \in \mathbf{F}_q^h$ に対し，添字集合 $\{1, \ldots, h\}$ を次のように I_1 と I_2 に直和分割する．

$$\begin{aligned} I_1 &:= \{j \in \{1, \ldots, h\} \mid (\boldsymbol{g}, \boldsymbol{x}_j) = 0\}, \\ I_2 &:= \{j \in \{1, \ldots, h\} \mid (\boldsymbol{g}, \boldsymbol{x}_j) \neq 0\}. \end{aligned}$$

このとき，$\boldsymbol{g} = \sum_{i \in I_2} c_i \boldsymbol{y}_i$ と表すことができる． ∎

補題 5 (Lemma 6 in [8]) アルゴリズム 1 Step 3 にて，更新して得られる $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_h$ および $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_h$ を成分とする行列 Y と X は $XY = E$ を満たす． ∎

定理 6 アルゴリズム 1 は，与えられた G に対し，条件 2 を満たす X, Y, I を出力することが可能である． ∎

定理 7 アルゴリズム 1 の時間と領域の計算量は，それぞれ $O(h^2 n)$ と $O(h^2)$ である． ∎

Remark 8 アルゴリズム 1 において出力される行列 X と Y は $XY = E$ を満たす．したがって，定理 1 より，行列 X は Y の逆行列である． ∎

4 条件付き正則行列の構成アルゴリズム IIb

4.1 問題設定 IIb

空間 $\mathbf{F}_q^h$ の空でない部分集合 G_ℓ の濃度を $|G_\ell| = r_\ell$ と表し，その各要素の列ベクトルを $G_\ell = \{\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}\}$ と表す．そして，そのような N 個の異なる部分集合 $G_1, \ldots, G_N$ からなる集合を $\mathcal{G} = \{G_1, \ldots, G_N\}$ とする．集合 $\mathcal{G}$ に対し，以下の仮定をする．

仮定 9 集合 $\mathcal{G}$ の各要素 G_ℓ, $\ell = 1, \ldots, N$ に対し，以下が成り立つ．

1) $r_\ell < h$,
2) rank $[\boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}] = r_\ell$. ∎

このとき，次の条件を満たす行列 F を求める問題を考える．列ベクトル $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_h \in \mathbf{F}_q^h$ を成分とする $h \times h$ 行列 F を

$$F := [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_h] \tag{5}$$

とする．そして，正整数 r を $r < h$ を満たすものとする．

条件 10 仮定 9 を満たす集合 $\mathcal{G}$ に対し，行列 F は，次の 2 つの条件を満たす．

1) rank $F = h$,
2) 各 G_ℓ, $\ell = 1, \ldots, N$ に対し，以下が成り立つ．

2-1) $r_\ell \leq r$ の場合:

$$\text{rank}[\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}] = h - r + r_\ell. \tag{6}$$

2-2) $r_\ell > r$ の場合: 任意の $h - r_\ell$ 個の要素 $\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}} \in \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{h-r}\}$ に対し，以下が成り立つ．

$$\text{rank}[\boldsymbol{f}_{i_1}, \ldots, \boldsymbol{f}_{i_{h-r_\ell}}, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,r_\ell}] = h. \tag{7}$$

この条件 10 は山本 [2] により与えられたランプ型秘密分散法の条件に従っている．以上より，本節で設定する問題を以下に示す．

問題 2 仮定 9 を満たす集合 $\mathcal{G} = \{G_1, \ldots, G_N\}$ に対し，条件 10 を満たす $h \times h$ 行列 $F = [\boldsymbol{f}_1, \ldots, \boldsymbol{f}_h]$ を求めよ． ∎

4.2 アルゴリズム IIb

問題 2 を解く一方法を示す前に，集合 $\mathcal{G} = \{G_1, \ldots, G_N\}$ の各要素集合 G_ℓ に対し，以下のような幾つかの記号を定義する．まず，各 ℓ に対し，正整数 d_ℓ を

$$d_\ell := \begin{cases} 1 & (r_\ell \leq r) \\ \binom{h-r}{h-r_\ell} & (r_\ell > r) \end{cases} \tag{8}$$

と定義する．各 ℓ に対し，集合 $\{1, \ldots, h-r\}$ の部分集合 $B_\ell^{(1)}, \ldots, B_\ell^{(d_\ell)}$ と，それら全体からなる集合 $\mathcal{B}_\ell$ を以下のように定義する．

$$\begin{aligned} \mathcal{B}_\ell &= \{B_\ell^{(1)}, \ldots, B_\ell^{(d_\ell)}\}, && (9) \\ B_\ell^{(k)} &\subseteq \{1, \ldots, h-r\}, && (10) \\ |B_\ell^{(k)}| &= \begin{cases} h-r & (r_\ell \leq r) \\ h-r_\ell & (r_\ell > r) \end{cases} && (11) \\ B_\ell^{(i)} &\neq B_\ell^{(j)} \quad \text{if } i \neq j && (12) \end{aligned}$$

ただし，$k = 1, \ldots, d_\ell$. すなわち，集合 $\{1, \ldots, h-r\}$ から $h - r_\ell$ 個 (または $h - r$ 個) の要素を取り出す組合せの集合が $B_\ell^{(1)}, \ldots, B_\ell^{(d_\ell)}$ であり，それら全体を要素とする集合が $\mathcal{B}_\ell$ である．集合 $\mathcal{B}_\ell$ の要素に順序を付ける方法については文献 [9] のアルゴリズム f および f^{-1} を参照．特に，$r_\ell \leq r$ となる場合は，$\mathcal{B}_\ell = \{B_\ell^{(1)}\}$, $B_\ell^{(1)} = \{1, \ldots, h-r\}$, $|B_\ell^{(1)}| = h - r$ となる．求める正則行列 F に対応させて，$N+1$ 番目として以下のものを定義する．

$$\begin{aligned} \mathcal{B}_{N+1} &= \{B_{N+1}^{(1)}\}, && (13) \\ B_{N+1}^{(1)} &= \{1, \ldots, h-r\}, && (14) \\ |B_{N+1}^{(1)}| &= h - r. && (15) \end{aligned}$$

また，各集合 G_ℓ をアルゴリズム 1 に入力し，得られる出力 X, Y, I を X_ℓ, Y_ℓ, I_ℓ と表すことにする．この 1 組の (X_ℓ, Y_ℓ, I_ℓ) に対し，d_ℓ 個の組 $(X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)})$, $k = 1, \ldots, d_\ell$ を考える．$h \times h$ 行列 $X_\ell^{(k)}, Y_\ell^{(k)}$ の各成分ベクトルは，列ベクトル $\boldsymbol{x}_{\ell,1}^{(k)}, \ldots, \boldsymbol{x}_{\ell,h}^{(k)}$ と $\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h}^{(k)} \in \mathbf{F}_q^h$ により以下のように表されるものとする．

$$\begin{aligned} X_\ell^{(k)} &= (\boldsymbol{x}_{\ell,1}^{(k)}, \ldots, \boldsymbol{x}_{\ell,h}^{(k)})^T, && (16) \\ Y_\ell^{(k)} &= (\boldsymbol{y}_{\ell,1}^{(k)}, \ldots, \boldsymbol{y}_{\ell,h}^{(k)}) && (17) \end{aligned}$$

すべての k に対し，$X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)}$ の初期値を以下のようにする．

$$\begin{aligned} X_\ell^{(k)} &= X_\ell, && (18) \\ Y_\ell^{(k)} &= Y_\ell, && (19) \\ I_\ell^{(k)} &= I_\ell. && (20) \end{aligned}$$

また，求める正則行列 F に対応させる $X_{N+1}^{(1)}, Y_{N+1}^{(1)}, I_{N+1}^{(1)}$ の初期値は，以下のようにする．

$$X_{N+1}^{(1)} = Y_{N+1}^{(1)} = E, \tag{21}$$

$$I_{N+1}^{(1)} = \{1, \ldots, h\}. \tag{22}$$

したがって，以下に示すアルゴリズム 2 の中で扱う行列 X, Y や添字集合 I に関する個数は，共に以下に示す L 個になる．

$$L := \sum_{\ell=1}^{N+1} d_\ell \tag{23}$$

ただし，$d_{N+1} = 1$ とする．

それぞれの組 $(X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)})$ には，添字集合 $B_\ell^{(k)}$ が付随する．具体的に，$B_\ell^{(k)}$ がどのように $(X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)})$ に係わるのかを以下に記す．例えば，$(h, r) = (6, 2)$ とする．また，$r_\ell = 3$ とすると，$d_\ell = 4$ となる．そして，$B_\ell^{(1)} = \{1, 2, 3\}$, $B_\ell^{(2)} = \{1, 2, 4\}$, $B_\ell^{(3)} = \{1, 3, 4\}$, $B_\ell^{(4)} = \{2, 3, 4\}$ とすると，$\mathcal{B}_\ell = \{B_\ell^{(1)}, B_\ell^{(2)}, B_\ell^{(3)}, B_\ell^{(4)}\}$ となる．このとき，組 $(X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)})$ を更新して，最終的には条件 10 の 2) を満たすことを考える．そのために，添字集合 $B_\ell^{(k)}$ は，最終的な行列 $Y_\ell^{(k)}$ の列ベクトル成分として含まれるベクトル $\boldsymbol{f}_i$ の添字集合に対応し，以下のような対応関係をもたせることを目的に用意するものである．

$$\begin{aligned}
Y_\ell^{(1)} \leftrightarrow B_\ell^{(1)} &\leftrightarrow \{\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,3}\},\\
Y_\ell^{(2)} \leftrightarrow B_\ell^{(2)} &\leftrightarrow \{\boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_4, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,3}\},\\
Y_\ell^{(3)} \leftrightarrow B_\ell^{(3)} &\leftrightarrow \{\boldsymbol{f}_1, \boldsymbol{f}_3, \boldsymbol{f}_4, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,3}\},\\
Y_\ell^{(4)} \leftrightarrow B_\ell^{(4)} &\leftrightarrow \{\boldsymbol{f}_2, \boldsymbol{f}_3, \boldsymbol{f}_4, \boldsymbol{g}_{\ell,1}, \ldots, \boldsymbol{g}_{\ell,3}\}.
\end{aligned}$$

さらに，各 $\ell = 1, \ldots, N+1$ に対し，以下の集合を定義する．各整数 $m \in \{1, \ldots, h-r\}$ に対し，

$$D_\ell(m) := \{k \in \{1, \ldots, d_\ell\} | m \in B_\ell^{(k)} \text{ for } B_\ell^{(k)} \in \mathcal{B}_\ell\} \tag{24}$$

とする．このとき，

$$|D_\ell(m)| = \begin{cases} 1 & (r_\ell \le r) \\ \binom{h-r-1}{h-r_\ell-1} & (r_\ell > r) \end{cases} \tag{25}$$

が成り立つ．つまり，$D_\ell(m)$ の濃度は m の値に依存しない．そして，以下の関係が成り立つ．

$$\frac{d_\ell}{|D_\ell(m)|} = \begin{cases} 1 & (r_\ell \le r) \\ \frac{h-r}{h-r_\ell} & (r_\ell > r) \end{cases} \tag{26}$$

以下に問題 2 を解くアルゴリズムを示す．

アルゴリズム 2 (Algorithm IIb)

Input : $X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)}$ for all $\ell = 1, \ldots, N$ and $k = 1, \ldots, d_\ell$
Output : $X_{N+1}^{(1)}, Y_{N+1}^{(1)}, I_{N+1}^{(1)}$

Initial: $h_2 := h - r$, $X_{N+1}^{(1)} = Y_{N+1}^{(1)} := E$, $I_{N+1}^{(1)} := \{1, \ldots, h\}$, and $m := 1$.

Step 1) Input: $X_\ell^{(k)}, Y_\ell^{(k)}, I_\ell^{(k)}$ for all $\ell = 1, \ldots, N$ and $k = 1, \ldots, d_\ell$

Step 2) for each $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$,

$$i_\ell^{(k)} = i_{\ell,m}^{(k)} := \min I_\ell^{(k)} \tag{27}$$

Step 3) Choose $\alpha_\ell^{(k)} \in \mathbf{F}_q$ for all $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$, and set

$$\boldsymbol{f} = \boldsymbol{f}_m := \sum_{\ell=1}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)} \tag{28}$$

Step 4) if $(\boldsymbol{f}, \boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)}) \neq 0$ for all $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$, then goto 5), else goto 3).

Step 5) for each $\ell = 1, \ldots, N+1$ and $k \in D_\ell(m)$,

$$\begin{aligned}
\boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)} &:= \boldsymbol{f}\\
\boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)} &:= (\boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)}, \boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)})^{-1} \boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)}\\
\boldsymbol{x}_{\ell, i}^{(k)} &:= \boldsymbol{x}_{\ell, i}^{(k)} - (\boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)}, \boldsymbol{x}_{\ell, i}^{(k)}) \boldsymbol{x}_{\ell, i_\ell^{(k)}}^{(k)}\\
&\qquad \text{for all } i = 1, \ldots, h \text{ s.t.} i \neq i_\ell^{(k)}\\
I_\ell^{(k)} &:= I_\ell^{(k)} \setminus \{i_\ell^{(k)}\}
\end{aligned}$$

Step 6) $m := m + 1$. if $m > h_2$, then goto 7), else goto 2).

Step 7) Output: $X_{N+1}^{(1)}$, $Y_{N+1}^{(1)}$, and $I_{N+1}^{(1)}$ and halt. ∎

定理 11 アルゴリズム 1 と 2 を用いることで，仮定 9 を満たす与えられた集合 $\mathcal{G}$ に対し，条件 10 を満たす正則行列 F を求めることが可能である．ここで，アルゴリズム 2 の出力 $Y_{N+1}^{(1)}$ を F とする． ∎

Remark 12 アルゴリズム 2 Step 3 において，式 (28) の $\boldsymbol{f}_m$ を構成する際，係数 $\alpha_\ell^{(k)}$, $\ell = 1, \ldots, N+1$, $k \in D_\ell(m)$ を (一様) ランダムに選び出すことにする．このとき，添字集合 $\{1, \ldots, N+1\}$ の中から 1 個の数字 p_1 を選び出し，さらに，集合 $D_{p_1}(m)$ の中から 1 個の数字 p_2 を選び出す．そして，添字の順序対 (p_1, p_2) に対応する項を式 (28) の右辺から抜き出し，以下のように表す．

$$\begin{aligned}
\boldsymbol{f}_m &= \alpha_{p_1}^{(p_2)} \boldsymbol{y}_{p_1, i_{p_1}^{(p_2)}}^{(p_2)} + \sum_{\substack{k \in D_{p_1}(m)\\ k \neq p_2}} \alpha_{p_1}^{(k)} \boldsymbol{y}_{p_1, i_{p_1}^{(k)}}^{(k)}\\
&\quad + \sum_{\substack{\ell=1\\ \ell \neq p_1}}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)}
\end{aligned} \tag{29}$$

一方，順序対 (p_1, p_2) に対応する正則行列 $Y_{p_1}^{(p_2)}$ の列ベクトル $\boldsymbol{y}_{p_1,1}^{(p_2)}, \ldots, \boldsymbol{y}_{p_1,h}^{(p_2)}$ は $\mathbf{F}_q^h$ の基底にもなるから，式 (29) の右辺の第 2 項と 3 項を以下のように一意に表すことができる．

$$\begin{aligned}
&\sum_{\substack{k \in D_{p_1}(m)\\ k \neq p_2}} \alpha_{p_1}^{(k)} \boldsymbol{y}_{p_1, i_{p_1}^{(k)}}^{(k)} + \sum_{\substack{\ell=1\\ \ell \neq p_1}}^{N+1} \sum_{k \in D_\ell(m)} \alpha_\ell^{(k)} \boldsymbol{y}_{\ell, i_\ell^{(k)}}^{(k)}\\
&= \sum_{i=1}^{h} \beta_{p_1,i}^{(p_2)} \boldsymbol{y}_{p_1,i}^{(p_2)}
\end{aligned} \tag{30}$$

ここで，$\beta_{p_1,1}^{(p_2)}, \ldots, \beta_{p_1,h}^{(p_2)} \in \mathbf{F}_q$ である．したがって，ベクトル $\boldsymbol{f}_m$ は以下のように表すことができる．

$$\boldsymbol{f}_m = (\alpha_{p_1}^{(p_2)} + \beta_{p_1, i_{p_1}^{(p_2)}}^{(p_2)}) \boldsymbol{y}_{p_1, i_{p_1}^{(p_2)}}^{(p_2)} + \sum_{\substack{i=1\\ i \neq i_{p_1}^{(p_2)}}}^{h} \beta_{p_1,i}^{(p_2)} \boldsymbol{y}_{p_1,i}^{(p_2)} \tag{31}$$

このとき，ベクトル $\boldsymbol{f}_m$ と $\boldsymbol{x}_{p_1, i_{p_1}^{(p_2)}}^{(p_2)}$ の内積が $(\boldsymbol{f}_m, \boldsymbol{x}_{p_1, i_{p_1}^{(p_2)}}^{(p_2)}) = 0$ となるのは，$\alpha_{p_1}^{(p_2)}$ の値が $\alpha_{p_1}^{(p_2)} = -\beta_{p_1, i_{p_1}^{(p_2)}}^{(p_2)}$ となる場合だけである．式 (28) の項の総数は，以下に示す M 個になる．

$$M := \sum_{\ell=1}^{N+1} |D_\ell(m)| \tag{32}$$

そして，式 (28) の係数である M 個の $\alpha_\ell^{(k)} \in \mathbf{F}_q$ の選び方の全体は q^M 通りある．一方，順序対 (p_1, p_2) に対し，$(\boldsymbol{f}_m, \boldsymbol{x}_{p_1, i_{p_1}^{(p_2)}}^{(p_2)}) =$

0 となる M 個の $\alpha_\ell^{(k)} \in \mathbf{F}_q$ の選び方は q^{M-1} 通りある．したがって，M 個の $\alpha_\ell^{(k)} \in \mathbf{F}_q$ をランダムに選んだ場合に，$(\boldsymbol{f}_m, \boldsymbol{x}^{(p_2)}_{p_1,i^{(p_2)}_{p_1}}) = 0$ となる確率は $q^{M-1}/q^M = 1/q$ である．

いま，有限体の大きさについて，$|\mathbf{F}_q| = q > 2M$ を仮定する．このとき，ランダムに選び出した M 個の $\alpha_\ell^{(k)} \in \mathbf{F}_q$ に対し，$(\boldsymbol{f}_m, \boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell}) = 0$ となる $\ell \in \{1,\ldots,N+1\}$ かつ $k \in D_\ell(m)$ の順序対 (ℓ,k) が存在する確率はたかだか M/q であり，$M/q < 1/2$ となる．すなわち，Step 3 にて構成した $\boldsymbol{f}_m$ が Step 4 の条件を満たすことができず，失敗する確率が $1/2$ より小さいことを示している． ∎

Remark 13 アルゴリズム 2 Step 3 における列ベクトル $\boldsymbol{f}_m$ の構成を以下のように変更しても，Remark 12 と同様の議論と結論が導かれることを述べる．

まず，アルゴリズム 2 の中で，各 m の値の段階における Step 2 において選ばれた $i_\ell^{(k)}$, $\ell = 1,\ldots,N+1$, $k \in D_\ell(m)$ を要素とする集合を

$$I(m) := \{i_\ell^{(k)} | \ell = 1,\ldots,N+1,\ k \in D_\ell(m)\} \tag{33}$$

と定義する．このとき，いずれの $i_\ell^{(k)}$ も集合 $\{1,\ldots,h\}$ の要素であるので，$|I(m)| \le h$ が成り立つ．そして，次のようなベクトル $\boldsymbol{f}_m$ を構成することを考える．

$$\boldsymbol{f}_m := \sum_{i \in I(m)} \alpha_i \boldsymbol{e}_i \tag{34}$$

ここで，$\boldsymbol{e}_i \in \mathbf{F}_q^h$ は，第 i 成分が $\mathbf{F}_q$ の単位元で，その他の成分はすべて零元である単位列ベクトルを表す．さらに，$|I(m)|$ 個の α_i, $i \in I(m)$, は，ランダムに選ばれるものとする．このとき，添字集合 $\{1,\ldots,N+1\}$ の中から 1 個の数字 p_1 を選び出し，さらに，集合 $D_{p_1}(m)$ の中から 1 個の数字 p_2 を選び出す．すると，Remark 12 と同様の議論により，$|I(m)|$ 個の $\alpha_i \in \mathbf{F}_q$ をランダムに選んだ場合に，添字の順序対 (p_1,p_2) に対し，$(\boldsymbol{f}_m, \boldsymbol{x}^{(p_2)}_{p_1,i^{(p_2)}_{p_1}}) = 0$ となる確率は $q^{|I(m)|-1}/q^{|I(m)|} = 1/q$ である．そして，$|\mathbf{F}_q| = q > 2M$ を仮定すると，ランダムに選び出した $|I(m)|$ 個の $\alpha_i \in \mathbf{F}_q$ に対し，$(\boldsymbol{f}_m, \boldsymbol{x}^{(k)}_{\ell,i^{(k)}_\ell}) = 0$ となる $\ell \in \{1,\ldots,N+1\}$ かつ $k \in D_\ell(m)$ の順序対 (ℓ,k) が存在する確率はたかだか M/q であり，$M/q < 1/2$ となる． ∎

定理 14 $|\mathbf{F}_q| = q > 2M$ と仮定する．このとき，アルゴリズム 2 の時間と領域の計算量は，それぞれ $O(h^3M)$ と $O(h^2L)$ である．ただし，L, M はそれぞれ式 (23) と (32) により定義された値である． ∎

定理 15 $q > 2M$ と仮定する．このとき，アルゴリズム 1 と 2 を用いて問題 2 を解くための時間と領域の計算量は，それぞれ $O(h^3M)$ と $O(h^2L)$ である． ∎

5 応用 (ランプ型秘密分散符号化，セキュアネットワーク符号化)

正整数の h と r は，$r < h$ を満たすものとする．$h-r$ 個の $S_1,\ldots,S_{h-r} \in \mathbf{F}_q$ を等確率に生起する情報シンボルとする．また，r 個の $R_1,\ldots,R_r \in \mathbf{F}_q$ を一様な乱数シンボルとする．そして，$(S_1,\ldots,S_{h-r},R_1,\ldots,R_r) \in \mathbf{F}_q^h$ という h 次元行ベクトルの順序組を考える．

$\mathbf{F}_q$ 上の $h \times h$ 行列 F を正則行列とする．h 次元空間 $\mathbf{F}_q^h$ の任意の列ベクトル $\boldsymbol{g}$ に対応する符号シンボルを以下のように定義する．

$$W(\boldsymbol{g}) := (S_1,\ldots,S_{h-r},R_1,\ldots,R_r)F^{-1}\boldsymbol{g} \in \mathbf{F}_q \tag{35}$$

いま，次の 2 点を仮定する．集合 $\mathcal{G} = \{G_1,\ldots,G_N\}$ は，仮定 9 を満たすものとする．次に，行列 F は，条件 10 を満たす正則行列とする．このとき，条件 10 はランプ型秘密分散符号化で要求される条件 [2] を示している．そして，各集合 $G_\ell = \{\boldsymbol{g}_{\ell,1},\ldots,\boldsymbol{g}_{\ell,r_\ell}\}$ の各要素列ベクトルに対応する符号シンボルを以下のように表す．

$$W_{\ell,i} = W(\boldsymbol{g}_{\ell,i}) = (S_1,\ldots,S_{h-r},R_1,\ldots,R_r)F^{-1}\boldsymbol{g}_{\ell,i} \tag{36}$$

ただし，$i = 1,\ldots,r_\ell$．このとき，任意の $G_\ell \in \mathcal{G}$ に対し，以下のことが成り立つ．1) $r_\ell \le r$ の場合，

$$H(S_1,\ldots,S_{h-r}|W_{\ell,1},\ldots,W_{\ell,r_\ell}) = H(S_1,\ldots,S_{h-r}) \tag{37}$$

が成り立つ．2) $r_\ell > r$ の場合，任意の $h-r_\ell$ 個の $S_{i_1},\ldots,S_{i_{h-r_\ell}} \in \{S_1,\ldots,S_{h-r}\}$ に対し，

$$H(S_{i_1},\ldots,S_{i_{h-r_\ell}}|W_{\ell,1},\ldots,W_{\ell,r_\ell}) = H(S_{i_1},\ldots,S_{i_{h-r_\ell}}) \tag{38}$$

が成り立つ．式 (37) および (38) は，ランプ型秘密分散符号化で要求される性質 [2] を示している．したがって，本稿で示したアルゴリズム 1 と 2 を用いることで，ランプ型秘密分散符号化を構成することが可能である．同時に，集合 $\mathcal{G}$ の各要素集合 G_ℓ を盗聴されるリンク集合に付随するリンクベクトル集合に対応させることで，セキュアネットワーク符号化を構成することも可能であることも示している [1, 3, 4, 5, 6].

6 むすび

本稿では，ランプ型秘密分散符号化およびセキュアネットワーク符号化を構成可能なアルゴリズムを提案した．そして，符号化を行なう有限体のサイズを $q > 2M$ とした場合，アルゴリズムの時間と領域の計算量がそれぞれ $O(h^3M)$ と $O(h^2L)$ となることを示した．最後に，本原稿に関連した情報がある場合は http://www.coding.ice.uec.ac.jp/に掲示する．

参考文献

[1] N. Cai and R. W. Yeung, “Secure network coding”, IEEE ISIT’02, p.323, June 2002.

[2] 山本博資, “(k,L,n) しきい値秘密分散システム”, IEICE, vol.J68-A No.9, pp.945-952, 1985.

[3] J. Feldman, T. Malkin, R. A. Servedio and C. Stein, “On the capacity of secure network coding”, Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing, Sept. 2004.

[4] K. Bhattad, K. R. Narayanan, “Weakly secure network coding”, First Workshop on Network coding, Theory and Applications, NETCOD2005, Italy, Apr. 2005.

[5] 原田邦彦，山本博資, “強いランプ型しきい値特性を持つ安全なネットワーク符号化法”, Proc. SITA2005, Okinawa, pp.741-744, Nov. 2005.

[6] 原田邦彦，山本博資, “線形ネットワーク符号化に対する強いランプ型秘密分散法”, IEICE Tech. Rep. IT2006-40, pp.31-36, 2006.

[7] 栗原正純, “ネットワーク符号化とある種の線型変換”, IEICE Tech. Rep. IT2006-41, pp.37-42, 2006.

[8] S.Jaggi, *et. al.*, “Polynomial time algorithms for multicast network code construction,” IEEE Trans. on IT, vol. 51, no. 6, pp.1973-1982, June 2005.

[9] 栗原正純, “MDS 符号とその復号法”, IEICE Tech. Rep. IT2003-92, pp.109-114, 2004.