k-結託に安全なネットワークコーディングの提案

石下 寿美代† 宮地 充子†‡§

†北陸先端科学技術大学院大学
923-1211 石川県能美市旭台 1-1
s1410008, miyaji@jaist.ac.jp

‡大阪大学大学院工学研究科電気電子情報工学専攻
565-0871 大阪府吹田市山田丘 2-1

§独立行政法人科学技術振興機構 CREST
332–0012 埼玉県川口市本町 4–1–8 川口センタービル

あらまし ISIT2013 において, Nihar らは隣接するノードの識別情報を用いて各ノードにシェアを含む情報を伝送することができ, (k-1) 個のノードの結託に対して安全な SNEAK プロトコルを提案した. しかし, このプロトコルでは全ノードが対等であり, かつデータ入手の為に再通信が必要であるという問題点がある. 本研究では, この SNEAK を発展させ, 中間ノードと受信ノードに区別して受信ノードのみが再通信せずにデータを復元でき, かつ k-結託に強いスキームの提案および考察を行う.
キーワード：ネットワークコーディング, 秘密分散法, 耐故障性

Secure network coding against k-collude adversary

Sumiyo Ishige† Atsuko Miyaji †‡§

†Japan Advanced Institute of Science and Technology.
1-1 Asahidai, Nomi, Ishikawa 923-1211, Japan
s1410008, miyaji@jaist.ac.jp

‡Graduate School of Engineering, Osaka University
2-1 Yamadaoka, Suita, Oosaka 565-0871, Japan
§JST CREST
Kawaguchi Center Building 4–1–8, Honcho, Kawaguchi-shi, Saitama, 332–0012 Japan

Abstract ISIT2013, Nihar et al proposed SNEAK protocol that can transmit the information of share to each nodes using the identifying information of adjacent nodes, and secure against (k-1) collusion. We considered the problem of this scheme is that all nodes treated as equal and they need to re-communicate to get data. In this paper, we proposed a implemented scheme that try to distinguish all nodes into intermediate nodes and receiver node and only receiver nodes can recover the data without re-communicating and secure against k-collude adversary.
Keyword: Network Coding, Secret Sharing, Fault-Tolerant

1 はじめに

送信ノード-受信ノード間のネットワークにおいて, 攻撃者による盗聴に対しても安全に情報を伝送することを考える. Agrawal[1] らは中間ノードが符号化を行うことによりメッセージ（秘密）を秘匿し, 送信ノードと受信ノード間の通信を安全に行うことができるネットワークコーディングを提案した. このネットワークコー

ディングは情報量的安全性により, エッジに流れている情報自体から秘密に関するどんな部分情報についても漏洩することがないという特徴をもつが, 一方でノードやエッジの盗聴や結託により秘密の復元に充分な情報が集まると露呈するという危険性がある．1979 年に Shamir により提案された (n, k) 閾値秘密分散法はネットワークコーディングと同じく情報量的安全性に基づいた情報分散共有法である．主に分散ストレージなどサーバと直接接続しているようなトポロジにおいて主に研究が行われている．1993 年 D.Dole らは [2] において直接接続していないネットワーク上のノードに対して秘密を伝送する SMT プロトコルを提案した．ネットワークにおいて (n, k) 閾値秘密分散法を用いて秘密 s を伝送するためには, 中間ノードを経由してシェアを受け取る必要がある．しかし, シェアを直接送信してしまうと他のノードへ秘密の復元に十分な数のシェアを与えることになるため, ディーラーは乱数を用いてシェアを秘匿する．秘匿したシェアおよび対応する乱数は独立した経路で各ノードに伝送されるので, 他のノードにシェアを与えることなく自身のシェアを得ることができる．2011 年 Nihar らは分散ストレージにおける故障ノード修復のための最適な再生成符号を提案 [6] し, この研究を元に SNEAK プロトコル [3] を提案した．この SNEAK プロトコルは SMT の問題点を改善したものではあったが, 中間ノードおよびレシーバー (受信) ノードが同等なものとして扱われ, レシーバーノードが秘密を復元するためには再度中間ノードと通信を行わなければならないという問題があった．そこで本稿ではこの SNEAK プロトコルを元に, レシーバーノードが再通信をすることなくシェアおよび秘密を復元できる方法についての提案を行う．

本稿の構成は次の通りである．まず, 2 章では本稿で使用する表記や主な定義について説明し, 3 章では既存研究の紹介を行う．次に, 4 章で本稿で提案する方式についての説明を行い．5 章で結論および今後の課題について述べる．

2 準備

2.1 表記

ここでは本稿で用いる表記について示す.

- G : 非巡回ネットワーク
- D : ディーラー
- R : レシーバーノード
- e : エッジ
- n : G を構成するノードの個数
- s : ディーラーが保持する $\mathbb{F}_q$ 上の秘密
- t_i : ノード i のシェア
- $N(j)$: ノード $j \in n$ からの入力エッジを持つ隣接ノードの集合
- $L(j)$: ノード $j \in n$ への出力エッジを持つ隣接ノードの集合
- ψ_i : ノード i に割り当てられている符号ベクトル $\{1, i, i^2, \cdots i^{m-1}\}$
- Ψ : Vandermode 行列

2.2 定義

ここで本稿に関連する主な定義について示す.

定義 2.1 (k-connected dealer) $(n+1)$ のノードを持つネットワーク G において, ディーラーを除く各 n ノードが

- ディーラーからの直接入力エッジを持つ.
- ディーラーからノードまで k 本の辺素パスを持つ.

のどちらかを満たすとき, *k-connected dealer condition* を満たすネットワークであるとする.

定義 2.2 (d-propagating dealer) $(n+1)$ のノードを持つネットワーク G において, ディーラーを除くすべての n ノード

- ディーラーからの直接入力エッジを持つ.

- 少なくとも d 個のノードからの入力エッジをもつ

のどちらかを満たすとき, *d-propagating dealer condition* を満たすネットワークであるとする.

補題 2.1 すべてのネットワーク G において (n,k) 閾値分散を実現するには, G が *k-connected dealer condition* を満たすネットワークである必要がある.

3 既存研究

3.1 SMT

1993 年 D.Dole らは [2] において SMT プロトコルを提案した. SMT プロトコルは次のステップで秘密 s から作成したシェア $\{t_i\}_{i=1}^{n}$ を各ノードに伝送する. また, SMT プロトコルにおいて, ネットワーク G は k-connected dealer condition を満たす.

1. シェアの作成
   一様ランダムに選択した乱数 r を用いて, すべてのノード i に対するシェアを作成する.

$$t_i = s + ir_1 + i^2 r_2 + \cdots + i^{k-1} r_{k-1}$$

2. ディーラー
   ディーラーは乱数 $r'_{1,1}, \cdots, r'_{i,k}$ を用いてシェアを次のように秘匿する.

$$T_i = t_i + r'_{1,1} + \cdots + r'_{i,k}$$

   ディーラーはすべてのノードのシェアを含む情報 T_i および乱数 $r_{1,1}, \cdots, r_{i,k}$ を, 独立した経路に一度に送信する.

3. 各ノード
   各ノード i は自身に属する情報 T_i および $r'_{1,1}, \cdots, r'_{i,k}$ を保持し, 次ノードのシェアおよび乱数を独立した経路で送信する. 受け取った情報から, ノード i はシェア t_i を得ることができる.

この SMT プロトコルにおける通信量は次のように表される. $|N(D|$ を $j \in N(D)$ であるノード数とする. この時, n 個のノードを保持するネットワーク G に対し, SMT が要する通信量は

$$\Gamma_{SMT}(G) = |N(D)| + \sum_{i \notin N(D)} \min_{w \geq k} \Big[\frac{w}{w-k+1} \times e_w(D \to i) \Big]$$

である. ここで, $e_w(D \to i)$ をディーラーおよびノード i へ至る w 本の辺素パス (独立した経路) の平均経路長とする.

3.2 SNEAK

2013 年 Nihar らは SMT を改良した SNEAK を提案した [3]. このプロトコルにおいて, ネットワーク G は d-propagating dealer condition を満たす. ここで SNEAK で用いられる表記について示す.

- s_A : $s_A = s_{d-k+1}$ であるスカラ
- $\boldsymbol{s_B}$: $s_B = [s_1 \cdots s_{d-k}]$ である
  長さ $(d-k)$ のベクトル
- $\boldsymbol{r_a}$: 長さ $(k-1)$ である乱数ベクトル
- R_b : $\frac{k(k-1)}{2}$ 成分が乱数である
  $(k-1) \times (k-1)$ 対称行列
- R_c : $(k-1)(d-k)$ 成分が乱数である
  $(d-k) \times (k-1)$ 行列
- M : スカラ s_A および小行列 $\boldsymbol{s_B}, \boldsymbol{r_a}, R_b, R_c$ により構成される対称行列

$$M = \begin{bmatrix} s_A & \boldsymbol{r_a}^T & \boldsymbol{s_B}^T \\ \boldsymbol{r_a} & R_b & {R_c}^T \\ \boldsymbol{s_B} & R_c & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \end{matrix} \begin{matrix} \underbrace{} \\ 1 \end{matrix} \begin{matrix} \underbrace{} \\ k-1 \end{matrix} \begin{matrix} \underbrace{} \\ d-k \end{matrix}$$

- t_i : 長さ $(d-k+1)$ のベクトルで表される
  各ノード $i (1 \leq i \leq n)$ のシェア t_i

$$t_i^T = \psi_i^T \begin{bmatrix} s_A & \boldsymbol{s_B}^T \\ \boldsymbol{r_a} & {R_c}^T \\ \boldsymbol{s_B} & 0 \end{bmatrix}$$

ディーラーは次のステップで秘密 s から作成したシェア $\{t_i\}_{i=1}^{n}$ を各ノードに伝送する.

1. ディーラー
   すべての $j \in N(D)$ に対し, 長さ d のベクトル $\psi_j^T M$ を送信する.
2. ノード $\ell \in N(D)$
   ディーラーから $\psi_\ell^T M$ を受け取る. ノード ℓ はすべての $j \in N(\ell)$ に対し, 内積 $\psi_\ell^T M \psi_j$ を計算し, 次のノードに伝送する.
3. ノード $\ell \notin N(D)$
   d 本のエッジ $\{e_1, \cdots e_d\}$ から受け取った情報をそれぞれ $\{\sigma_1, \cdots, \sigma_d\}$ とする. ノード $\ell \notin N(D)$ は
   $$v^T = [\sigma_1, \cdots, \sigma_d]^T [\psi_{e_1} \cdots \psi_{e_d}]^{-1}$$
   を計算する. その後, $j \in L(\ell)$ であるノードに $v^T \psi_j$ を計算し伝送する.

SNEAK における通信量は G のすべてのノードに対して $\frac{d}{d-k+1}$ のデータを得る必要があるため, 次のように表すことが出来る.

$$\Gamma_{SNEAK}(G) = n\frac{d}{d-k+1}$$

3.3 Product Matrix

再生成符号とは分散ストレージ上の故障ノード内にあるシェアやデータを修復する目的で提案された符号である. この再生成符号の構成方法は, まずストレージサイズ α を最小化して構成する最小ストレージ再生成符号 (MSR) と, まず修復バンドワイズ β を最小化して構成する最小バンドワイズ再生成符号 (MBR) がある. Nihar らは [6] において, この MSR および MBR を最適に構成する方法についての提案を行った. ここでは特に SNEAK と関連の深い MBR のシェア復元について紹介する.
まず, MBR 再生成符号に用いられる表記について示す.

- B : $u_i \in \mathbb{F}_q^B$ であるデータファイル
- f : 故障ノード
- h : ヘルパーノード $\{h_j \mid j = 1, ..., d\}$
- d' : シェアを復元するために故障ノードが任意にアクセスするノードの個数
- k' : B を復元するために故障ノードが任意にアクセスするノードの個数
- S : 上三角成分行列が $\{u\}_{i=1}^{B}$ から独立に選択された ${}_{k'+1}C_2$ 個成分からなる $(k' \times k')$ 対称行列
- T : S で選択されなかったデータを成分とする $(k' \times (d' - k'))$ 行列
- M' : S および T を用いて表される対称行列
$$M\text{'} = \begin{bmatrix} S & T \\ T^T & 0 \end{bmatrix}$$
- t_i' : 各ノード i が保持するシェア $t_i' = \psi_i M$

MBR のシェア復元では, 故障ノード f によるシェアの復元はつぎのようにして行われる.

1. 故障ノード f
   任意の d' 個のノード集合 $\{h_j \mid j = 1, ..., d'\}$ を選択してアクセスする.
2. ヘルパーノード h
   故障ノードに次の情報を送信する.
   $$\psi_{h_j}^T M \psi_f$$
3. 故障ノード f
   ヘルパーノードから情報を受け取った故障ノードは $(d' \times d')$ 修復行列 Ψ_{repair} を作成する.
   $$\Psi_{repair} = \begin{bmatrix} \psi_{h_1}^T \\ \vdots \\ \psi_{h_d'}^T \end{bmatrix}$$
   この逆行列 Ψ_{repair}^{-1} を, 受け取った情報に左から掛け合わせることで故障ノードが失ったシェアを復元することができる.

3.4 問題点の考察

SMT プロトコルでは, ディーラーは各ノード i のシェア t_i および対応する乱数 $r'_{i,1}, \cdots, r'_{i,\ell}$ を送信する際, 各ノードが安全にシェアを保持できるようにシェアおよび乱数を独立した経路で伝送する. よって, すべてのノードはネットワークトポロジの全体を事前に知っている必要がある. [4] で提案された SNEAK では, 中間ノードが受け取った情報を再利用することにより SMT よりも低い通信量でシェアを伝送することができた. しかし, このプロトコルでは中間ノードとレシーバーノードを区別なく同等なものとして扱っており, レシーバーノードが秘密の復元に必要な量のシェアを集めるためには再度 $k-1$ 個のノードと通信を行う必要がある. そのため, レシーバーノードが秘密を復元して効率よく通信を行える方式になっていないと考える. もっとも簡易な方法としては $j \in L(R)$ であるノード j がシェアを添付することであるが, 攻撃者によるシェア盗聴の危険性を考えると安全とはいえない.

4 提案方式

前章の問題点を解決するため, 本稿では各レシーバーノードに $k-1$ 個のミラーノードを想定することでレシーバーノードが再通信を行わなくとも秘密の復元に十分なシェアを得ることのできる方式についての提案を行う. 本提案では次のようなシステムモデルを想定する.

4.1 システムモデル

ディーラーおよび n 個のノードにより構成される非巡回ネットワーク G を考える. このネットワーク G は, ある変数 $d(\geq k)$ に対して d-propagating dealer condition を満たし, 以下に定義されるミラーノードをもつ.

定義 4.1 (ミラーノード $R^m_{i,j}$) ネットワーク G におけるレシーバーノードを $R_{i,1}$ とする. このとき, 各レシーバーノードはそれぞれ $k-1$ 個のミラーノード $R^m_{i,j} (j = 2, \cdots, k)$ を持つ.

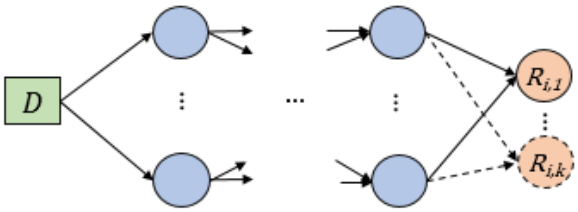

図 1: ミラーノード

各ノードはプロトコルには従うが, 秘密 s を得ることができそうな情報を保持することが出来るものとする.

4.2 提案方式

4.2.1 ディーラー初期設定

ディーラーはまず, 各ノード n に対し $(n \times d)$ の Vandermonde 行列 Ψ を構成する. この行列 Ψ の i 行は各ノード i に割り当てられている次のような符号ベクトルである.

$$\psi_i = \{1, i, i^2, \cdots i^{d-1}\}$$

次に, ディーラーは秘密 s およびその他の乱数 $\boldsymbol{r_a}$, R_b, R_c を用いて $(d \times d)$ 対称行列 M を構成する.

4.2.2 伝送アルゴリズム

ネットワーク G 内のノードは次のステップに沿ってシェアを含む情報を伝送する.

1. ディーラー
   すべての $j \in N(D)$ に対し, 長さ d のベクトル $\psi_j^T M$ を送信する.
2. ノード $\ell \in N(D)$
   ディーラーから $\psi_\ell^T M$ をそれぞれ受け取る. ノード $j \in N(\ell)$ の符号ベクトルを用いて内積 $\psi_\ell^T M \psi_j$ を演算した結果をノード j に送る.
3. ノード $\ell \notin N(D)$
   2. にて $L(\ell)$ である d 個のノード $\{i_{\ell,1}, \cdots, i_{\ell,d}\}$ から受け取った情報をそれぞれ $\{\sigma_{\ell,1}, \cdots, \sigma_{\ell,d}\}$

とする.
ノード $\ell \notin N(D)$ は

$$\boldsymbol{v}^T = \begin{bmatrix} \psi_{i_{\ell,1}}^T \\ \vdots \\ \psi_{i_{\ell,d}}^T \end{bmatrix}^{-1} \begin{bmatrix} \sigma_{\ell,1} \\ \vdots \\ \sigma_{\ell,d} \end{bmatrix} \tag{1}$$

を計算して自身のシェアを得る. その後ノード $j \in N(\ell)$ の符号ベクトルを用いて内積 $\boldsymbol{v}^T\psi_j$ を演算した結果をノード j に送る.

4. ノード $\ell \in L(R_{i,1})$
まず 3. より $\boldsymbol{v}_\ell^T$ を得る.
ノード ℓ は, レシーバーノード $R_{i,1}$ およびミラーノード $R_{i,j}^m, (j = 2, ..., k)$ の符号ベクトルを用いて, 内積を演算した結果

$$\boldsymbol{\sigma}_\ell = \left[\boldsymbol{v}^T\psi_{R_{i,1}}, \boldsymbol{v}^T\psi_{R_{i,2}^m}, \cdots, \boldsymbol{v}^T\psi_{R_{i,k}^m}\right]$$

をレシーバーノード $R_{i,1}$ に送る.

5. レシーバーノード $R_{i,1}$
$\ell \in L(R_{i,1})$ であるノード $\{i_{\ell,1}, \cdots, i_{\ell,d}\}$ から受け取った情報をそれぞれ $[\boldsymbol{\sigma}_{\ell,1}, \cdots, \boldsymbol{\sigma}_{\ell,d}]^T$ とする. レシーバーノード $R_{i,1}$ は各列ベクトルに対して (1) 式を用いることで k 個のシェアを得る. このようにして得たシェアから, 秘密 s を求めることが出来る.

4.2.3 例

次のような $n = 6, k = 2, d = 2$ であるネットワークにおいて, エンドノード $R_{1,1}$ が k 個のシェアを得る過程を示す.

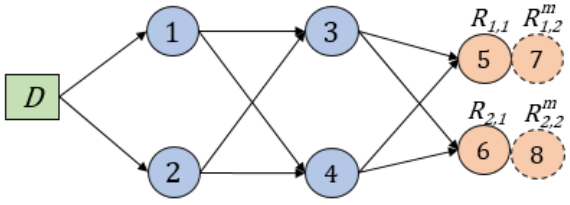

図 2: $n = 6, k = 2, d = 2$ のネットワーク

まず, ディーラーは次のような $(d \times d)$ 対称行列 M を構成する.

$$M = \begin{bmatrix} s & r_a \\ r_a & R_b \end{bmatrix}$$

本提案プロトコルに沿って計算を行うと, 4. においてノード $\ell = \{3, 4\} \in L(R_{1,1})$ は

$$\boldsymbol{v}_3 = [s + 3r_a \quad r_a + 3R_b]$$
$$\boldsymbol{v}_4 = [s + 4r_a \quad r_a + 4R_b]$$

を得る. ノード $\ell = \{3, 4\}$ は, レシーバーノード $R_{1,1}$ およびミラーノード $R_{1,2}^m$ の符号ベクトルを用いて $\boldsymbol{v}_3^T\psi_{R_{1,1}}, \boldsymbol{v}_3^T\psi_{R_{1,2}}, \boldsymbol{v}_4^T\psi_{R_{1,1}}, \boldsymbol{v}_2^T\psi_{R_{1,2}}$ を演算した結果

$$\boldsymbol{\sigma}_3 = \begin{bmatrix} (s + 5r_a) + 3(r_a + 5R_b) \\ (s + 7r_a) + 3(r_a + 7R_b) \end{bmatrix}^T$$
$$\boldsymbol{\sigma}_4 = \begin{bmatrix} (s + 5r_a) + 4(r_a + 5R_b) \\ (s + 7r_a) + 4(r_a + 7R_b) \end{bmatrix}^T$$

をレシーバーノード $R_{1,1}$ に送る. レシーバーノードは, 受け取った情報 $[\boldsymbol{\sigma}_3, \boldsymbol{\sigma}_4]$ の各列ベクトルを用いて次の計算を行い, 2 つのシェアを得る.

$$\begin{bmatrix} \psi_3^T \\ \psi_4^T \end{bmatrix}^{-1} \begin{bmatrix} (s + 5r_a) + 3(r_a + 5R_b) \\ (s + 5r_a) + 4(r_a + 5R_b) \end{bmatrix} = \begin{bmatrix} s + 5r_a \\ r_a + 5R_b \end{bmatrix}$$
$$\begin{bmatrix} \psi_3^T \\ \psi_4^T \end{bmatrix}^{-1} \begin{bmatrix} (s + 7r_a) + 3(r_a + 7R_b) \\ (s + 7r_a) + 4(r_a + 7R_b) \end{bmatrix} = \begin{bmatrix} s + 7r_a \\ r_a + 7R_b \end{bmatrix}$$

レシーバーノード $R_{1,1}$ はこのようにして得た 2 つのシェアから秘密 s を復元できる.

4.3 正当性

次の定理では提案した伝送方式において確かに各ノードがシェアを受け取ることができ, かつレシーバーノードにおいて受け取ったシェアから秘密 s を復元できることを示す. 定理および証明は [4] に基づく.

定理 4.1 (シェアの伝送) すべてのノード i は $\psi_i^T M$ を復元し, シェア t_i を得ることが出来る.

(証明)
証明は帰納法により行う．すべてのノード i が $\psi_i^T M$ を復元でき, かつ通信プロトコルに沿って他のノード $j \in N(\ell)$ に情報を伝送したならば, その情報は $\psi_i^T M \psi_j^T$ で表されると仮定する．
ノード 1 を考える．ノード 1 はディーラーに直接接続しているので, $\psi_1 M$ をディーラーから受け取る．さらに, 通信方式により, ノードは $\psi_1^T M \psi_j$ を隣接ノード $j \in N(1)$ に伝送する．
次に, ディーラーと直接接続していない $(\ell-1)$ までのノードに対し, 仮定が真であるとする．このときノード i は少なくとも d 個のノード $\{j_1, \cdots, j_d \subseteq [i-1]\}$ から次を計算した結果を受け取る必要がある．

$$\begin{bmatrix} \sigma_1 \\ \vdots \\ \sigma_d \end{bmatrix} = \begin{bmatrix} \psi_{j_1}^T \\ \vdots \\ \psi_{i_d}^T \end{bmatrix} M\psi_i$$

$\psi_{j_1}^T, \cdots, \psi_{j_d}^T$ は $(d \times d)$Vandertmonde 行列であることから逆行列が存在する．これを左から掛けて

$$\begin{bmatrix} \psi_{j_1}^T \\ \vdots \\ \psi_{i_d}^T \end{bmatrix}^{-1} \begin{bmatrix} \sigma_1 \\ \vdots \\ \sigma_d \end{bmatrix} = M\psi_i (= \boldsymbol{v})$$

ここで, M は対称行列であることから,

$$\boldsymbol{v}^T = \psi_i^T M^T = \psi_i^T M$$

を得る．通信プロトコルにより, ノード i はノード $j \in N(i)$ に

$$\boldsymbol{v}^T \psi_j = \psi_i^T M^T \psi_j$$

を伝送する．これにより任意のノード i に対し仮定が成り立つので, すべてのノード $i \in [n]$ は $\psi_i^T M$ を復元し, 自身のシェア t_i を得ることが出来る．

定理 4.2 (k secret recovery) 任意の k 個のシェアから秘密を一意に復元することができる．

(証明)
$I \subseteq [n]$ を秘密の復元に用いる k 個のノードの集合とし, Ψ_I を $\{\psi_i^T\}_{i \in I}$ からなる $(k \times d)$ 行列であるとする．また, Ψ_I' を Ψ_I の最初の k 列からなる小行列とする．このとき, シェアは次のように表すことが出来る．

$$\Psi_I \begin{bmatrix} {\boldsymbol{s_B}}^T \\ {R_c}^T \\ 0 \end{bmatrix} = \Psi' \begin{bmatrix} {\boldsymbol{s_B}}^T \\ {R_c}^T \end{bmatrix}$$

Ψ' は正則行列であることから, 逆行列が存在する．この逆行列 Ψ'^{-1} を左から掛けることにより, 秘密を復元できる．

5 結論

本稿では, Nihar[3] らの提案した SNEAK の問題点を改善し, ミラーノードを想定することでレシーバーノードが再通信することなく秘密の復元に必要なシェアを得ることができる方式の提案を行った．この提案により, ディーラーとレシーバーノード間において安全に情報を伝送することができる．今後の課題として, ネットワーク内にレイヤーを設け, 各レイヤーで少なくとも k 個のノードが失われていなければエンドノードまで安全に秘密を伝送できる耐故障性のある通信方式を検討する．

謝辞

本研究は JSPS 科研費 15K00183, 15K00189 の助成を受けました．

参考文献

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R.-W. Yeung, “Network information flow”, IEEE Trans. on Inform. Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.

[2] D. Dolev, C. Dwork, O. Waarts, and M. Yung, “Perfectly secure message transmission”, Journal of the ACM, vol. 40, no. 1, pp. 17-47, 1993.

[3] N. B. Shah, K. V. Rashmi, and K. Ramchandran, “Secure network coding for distributed secret sharing with low communication cost”, in Proc. IEEE International Symposium on Information Theory (ISIT), Jul. 2013.

[4] Nihar B. Shah, K. V. Rashmi and Kannan Ramchandran, Fellow, IEEE "Distributed Secret Dissemination Across a Network",arXiv:1207.0120v5 [cs.CR] 22 Oct 2014

[5] Zhaohui Tang, Hoon Wei Lim, and Huaxiong Wang "Revisiting a secret sharing approach for network code", ProveSec2012.

[6] K. V. Rashmi, N. B. Shah, and P. V. Kumar, “Optimal exact-regenerating codes for the MSR and MBR points via a product-matrix construction”, IEEE Trans. Inf. Th., Aug. 2011.