Vol.2015-CSEC-70 No.7
Vol.2015-SPT-14 No.7
2015/7/2

余剰ネットワークを用いた安全なネットワーク符号化

藤本竜矢[†1]　　岩村惠市[†2]

概要：マルチキャスト通信を行う際の最大通信レートは最大フロー最小カット定理により与えられ，ネットワーク符号化を用いるとこれを達成可能である．また，送信する秘密情報の安全性の向上も可能である．この安全性に関して，ネットワーク中のt本のパスが盗聴された場合，秘密情報に関しての一切の情報が漏れないネットワーク符号を，t-secure なネットワーク符号と呼ぶ．t-secure なネットワーク符号を構成するために，送信ノードにおいて秘密情報とは別に乱数をt個以上生成し送信データを構成する必要があるため，送信レートは低下する．本稿では，マルチキャスト通信において最大フローの達成とは無関係にある残余ネットワークを利用することで，送信レートを低下させずに，通信路の盗聴に関して部分的にt-secure な安全性を達成可能な手法を示す．
キーワード：線形ネットワーク符号化，部分的安全性，安全なネットワーク符号化

Secure network coding using the remaining network

TATSUYA FUJIMOTO[†1]　IWAMURA KEIICHI[†2]

Abstract：The maximum communication rate in multicast network is given by the max-flow min-cut theorem and is achieved by using network coding. Network coding also enable to improve the secrecy of transmit information. For safety, the wiretapper can get no information from message on arbitrary t　paths in the network. This is called t-secure network codes. In order to construct a t-secure network codes, the transmission data is necessary to be constituted of the secret message and t random numbers in the source node. Therefore transmission rate is lowered. In this paper, we use the remaining network which is independent of maximum flow of multicast communication. Without lowering the transmission rate, we can achieve partially t-secure network code against wiretapping on the communication network.
キーワード：linear network coding，partial secrecy，secure network coding

1. はじめに

近年，通信の高速化は重要性が非常に高くなっている．通信の高速化を達成するために，プロトコルから改良する手法が検討されている．この手法のひとつにネットワーク符号化があげられる．

従来のネットワークにおいて，中継ノードは受信したデータを複製し隣接ノードへの転送のみを行う．ネットワーク符号化では，中継ノードは複数の受信したデータを演算･符号化し，符号化したデータを隣接ノードへ送信する．これにより，マルチキャスト通信における理論上の最大通信レートの達成が可能となる．

ネットワーク符号化は Ahlswede らによってその理論が確立された[1].

中継ノードにおいて線形演算を行うネットワーク符号化は線形ネットワーク符号と呼ばれ，Li らにより最大フロー(2.1 節)を達成するのに十分であることが示されている[4]．ネットワーク符号化を用いる際には，符号ベクトルと呼ばれる係数が必要となるが，これを確定的方法で割り当てる手法が Jaggy ら[2]によって提案された．また，各中継ノードで自律分散的に符号ベクトルを決定する方式をランダムネットワーク符号化と呼び[5]，ネットワーク構造が時間的変化する際に用いられる．本稿では前者を使用する．

ネットワーク符号化において，Cai らは秘密分散を利用することで任意のパスの盗聴に対して情報量的に安全なネットワーク符号化を示した[3].

ネットワーク中のt本の独立なパスの盗聴に対して安全なネットワーク符号をt-secure なネットワーク符号と呼ぶ[7]．また，原田らは[6]において，t-secure な符号ベクトル割り当てアルゴリズムを提案した．

これらは，送信ノードにおいて秘密情報とは別に乱数をt個以上生成し送信データを構成する必要があるため，送信レートは低下する．これに関して余剰ネットワークを同時に利用することで，ユニキャスト通信において秘密情報を効率よくt-secure 送信する手法が[9]で示された．これは，ネットワーク中の全てのノードが乱数を発生できるものとして，安全性の向上を図っている．また，[10]においては，マルチキャスト通信において，ネットワーク中の余剰なリソースから送信ノードとすべての受信ノードへ向かうパスを用いて安全性の向上を図っている．しかし，これらの方式を用いた場合，秘密情報の送信の際に行う操作が増える．例えば，送信ノードから秘密情報を送出する際には，ネットワーク中の余剰リソースにおいて乱数を生成し，その乱数を送信ノードが受け取っている必要がある．

そこで本稿では，別のアプローチを用いて秘密情報の送信をより安全にする手法を提案する．具体的には，送信ノ

†1 東京理科大学
Tokyo University of Science
†2 東京理科大学
Tokyo University of Science

ードからネットワーク中の中継ノードへと向かう，残余ネットワークを用いることで，マルチキャスト通信において，部分的にt-secure なネットワーク符号とする確定的手法について考察する．以降，2 章においてネットワーク符号化についての概要を示す．3 章で提案手法について示す．その後，4 章において安全性について考察する．

2. ネットワーク符号化

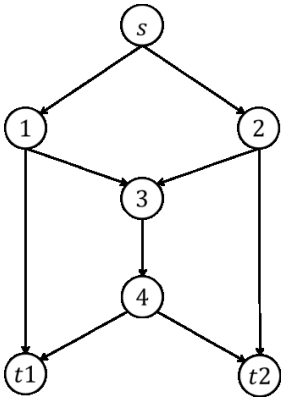
2.1 マルチキャスト通信と最大フロー

ユニキャスト通信における送信ノードから受信ノードへの最大フローは，最大フロー最小カット定理により与えられる．最大フローは，送信ノードsから受信ノードtへの単位時間あたりの流量のうち最大となるものであり，最小カットは，ネットワーク中のすべてのノードを，送信ノードsを含む集合$\mathcal{S}$と受信ノードtを含む集合$\mathcal{T}$にカットしたときのカットエッジの容量が最小となるものである．最大フロー最小カット定理は，最小カットが最大フローと等しくなるというものである．

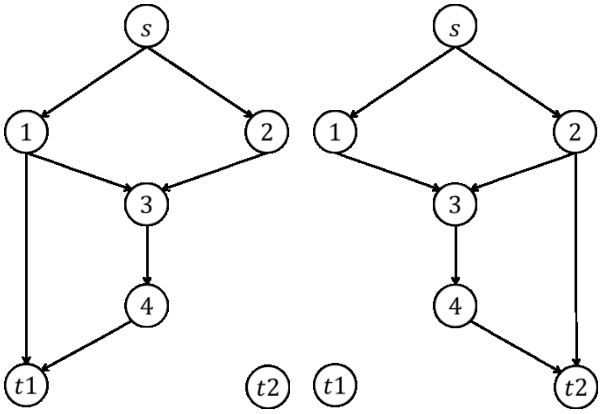
次に，ネットワークを介して一つの送信ノードから，複数の受信ノードへ同時に情報を送信するマルチキャスト通信について考える．中継ノードが入力されるデータの複製を可能とすると，マルチキャスト通信における最大フローは送信ノードから各受信ノードへのユニキャスト通信における最大フローのうち最小の値となる．図 1(a)のネットワークにおいて，各受信ノード$t1, t2$へユニキャストする際のネットワークはそれぞれ図 1(b)，図 1(c)である．各エッジの容量を 1 とすると，最小カットの容量は共に 2 であるため，最大フローは共に 2 である．そのため，送信ノードsから各受信ノード$t1, t2$へマルチキャストする際の最大フローは 2 となる．

2.2 ネットワーク符号化

中継ノードにおいて複数経路から受信したデータの符号化を行い，中継ノードの出力を決定する技術をネットワーク符号化と呼ぶ[1]．図 2 に図 1 のネットワークにおいてマルチキャスト通信を行う例を示す．各エッジの容量は 1 とする．このとき，ネットワークにおいて送信ノードsから受信ノード$t1, t2$へのマルチキャスト通信の最大フローは 2 である．送信ノードからのデータは$\{s \to 1 \to t1\}$及び$\{s \to 2 \to 3 \to 4 \to t1\}$を通って受信ノード$t1$へ伝送され，$\{s \to 1 \to 3 \to 4 \to t1\}$及び$\{s \to 2 \to t2\}$を通って受信ノード$t2$へ伝送される．従来の通信ネットワークの場合，送信ノードから送出したデータ$x1, x2$はパス$\{3 \to 4\}$において，どちらか一方のみしか送信することができない．このため，最大フロー2 を達成できない．一方，ネットワーク符号化を用いると$x1$と$x2$を受信したノード 3 は，これらの排他的論理和$x1 + x2$を演算(符号化)し次のノードへと送信する．受信ノード$t1$は$x1$と$x1 + x2$を受け取り，受信ノード$t2$は$x2$と$x1 + x2$を受け取るため，それぞれ$x1$と$x2$の復元可能となる．すなわち，ネットワーク符号化によりこのネットワークにおける最大フローでのデータ送信が可能となる．

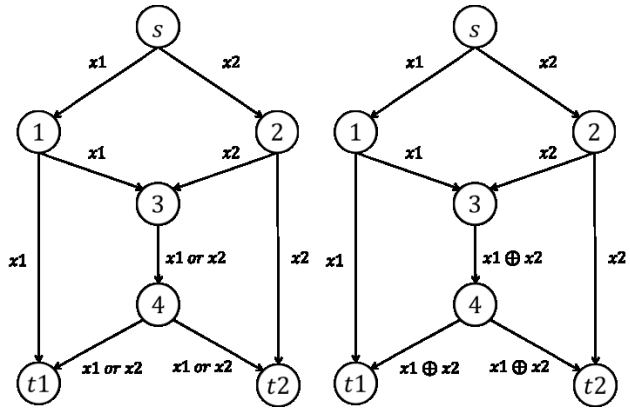


(a)ネットワーク構造



(b) $t1$へユニキャスト　　(c) $t2$へユニキャスト

図 1 各受信ノードへユニキャスト



(a)通常のマルチキャスト　　(b)ネットワーク符号化

図 2 マルチキャストネットワーク

2.3 線形ネットワーク符号

通信ネットワークは有向グラフ$G = (V, E)$によって表される．ここでV,Eはネットワーク上のすべてのノードとエッジの集合である．任意のネットワークにおいて，中継ノードへの入力の線形結合による符号化によりそのネットワ

ークにおける最大フローを達成可能であることが，[4]に示されている．各辺$e \in E$は誤りなく有限体GF_q上の 1 情報$Y(e)$を伝達する．送信ノードから送信する情報を$X^h = (x_1, x_2, \cdots, x_h)$とする．$h$はマルチキャスト通信における最大フローである．このとき，ネットワーク上の各辺を流れる情報が$x_1, x_2, \cdots, x_h$の線形結合となるものを，線形ネットワーク符号という．

各辺を流れる情報$Y(e)$は$x_1, x_2, \cdots, x_h$線形結合となっているため, 各辺にk次元の列ベクトル$b(e)$が与えられているものとして，$Y(e) = X^h b(e)$と表すことができる．ここで$b(e)$は符号ベクトルと呼び，これを各辺に割り当てることで線形ネットワーク符号の構成が可能である．図 3 は，図 2(b)を符号ベクトルで表したものである．

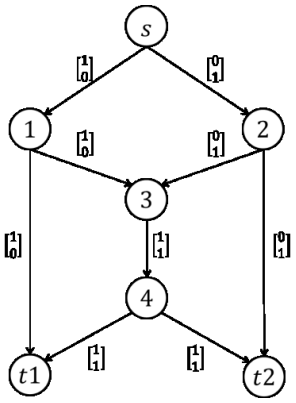


図 3 符号ベクトル

2.4 符号ベクトルの割り当て方法

Jaggy らは，[2]において 2.3 節で示した符号ベクトルの確定的割り当て方法を示した．この方法は最大フローhでの送信が可能である．$f_{\leftarrow}^{t}(e)$をf^t上のエッジeの直前のエッジとする．また，$P(e)$はエッジeの直前のエッジの集合とする．アルゴリズムは以下のとおりである．

I. 仮想ノードs'をグラフ$G = (V, E)$に追加し，s'からsへh本のパス$\{e_1, \ldots, e_h\}$を追加する．各受信ノードについてs'からh本の辺疎パスf^tを探索する．

II. s'から出るh本のパス$C_t = \{e_1, \ldots, e_h\}$にそれぞれ符号ベクトル$b(e_i) = \left[0^{i-1}, 1, 0^{h-i}\right]^T$を割り当てる．また，$B_t = \{b(e_1), \ldots, b(e_h)\}$とする．

III. $v \in V$を位相的順序で選び、f^t上のパスeについて以下を行う．

(a)以下を満たす$b(e)$を決定し，割り当てる．

全てのtについて

$b(e) = \sum_{p \in P(e)} m_p(e) b(p)$

$\left(B_t \setminus \left\{b\left(f_{\leftarrow}^{t}(e)\right)\right\}\right) \cup \{b(e)\}$が線形独立

(b)各$t \in T(e)$に対して

$C_t = (C_t \setminus \{f_{\leftarrow}^{t}(e)\}) \cup \{e\}$

$B_t = \left(B_t \setminus \left\{b\left(f_{\leftarrow}^{t}(e)\right)\right\}\right) \cup \{b(e)\}$

以上によって割り当てられた符号ベクトルはf^tそれぞれについて線形独立となるように割り当てられるため，受信ノードでのh個の送信情報を復元可能なものとなっている．

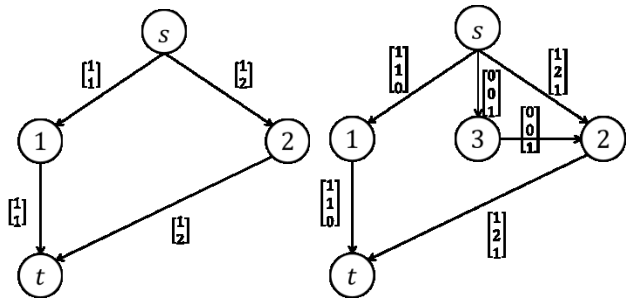
3. 提案手法

S.Jaggy らの方式[2]によって割り当てた符号ベクトルにより最大フローhでマルチキャスト通信が可能であるが，ネットワーク中には最大フローに必要なノードとパス以外に使用していないノードとパスが存在する．本節では、これらを利用し，安全に情報を送信する手法を提案する．

3.1 余剰ネットワークを利用する

ネットワーク上には最大フローでの秘密情報の送信に最低限必要なネットワーク以外に，余剰のパスおよびノードが存在する．送信ノードからこれらを利用して乱数を挿入可能なものについて考察し，秘密情報を安全に送信する手法を提案する．

図 4 にユニキャスト通信において余剰ネットワークを用いて安全性の向上が可能となる例を示す．



(a) (b)
図 4 余剰ネットワークの利用(ユニキャスト通信)

図 4 のネットワークは最大フロー2 のネットワークである．最大フローを達成するためには$\{s \to 1 \to t\}$，$\{s \to 2 \to t\}$の 2 本のパスがあれば十分である．ここで，送信ノードsから秘密情報$X^2 = (x_1, x_2)$を送信する場合について考える．図 4(a)ではネットワーク上のどの 1 エッジを盗聴されたとしても，秘密情報同士の線形結合値が漏れる．図 4(b)では余剰ネットワーク$\{s \to 3 \to 2\}$を用いる．送信ノードから，秘密情報と乱数である(x_1, x_2, r_1)を送信する．$\{s \to 3 \to 2\}$を用いて乱数をノード 2 に乱数r_1送信することで，$\{s \to 2\}$上のパスに流れる情報を乱数r_1を含ものすることができる．そのため，$\{s \to 2\}$上のパスを盗聴された場合秘密情報に関して何も漏れることはない．すなわち，送信ノードsからノード 2 までのネットワークは 1-secure なネットワークとなっている．

次に受信ノードが複数の場合の例を図 5 に示す．

Vol.2015-CSEC-70 No.7
Vol.2015-SPT-14 No.7
2015/7/2

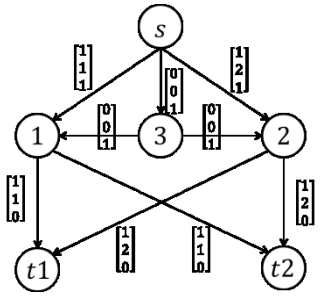


図 5　余剰ネットワークの利用(マルチキャスト通信)

図 5 のネットワークにおいても先のユニキャスト通信と同様の安全性が保障できる．このように，送信ノードにおいて乱数を付加し，中継ノードにおいて乱数の打消しを行うことで，盗聴に関して安全性を向上させることが可能である．

以下，本章での秘密情報$S=(s_1,\cdots,s_h)$は最大フローhで送信されるものとする．次節において送信ノードと受信ノードにおいて，予め情報を共有せずに送信ノードから余剰ネットワークを利用して乱数を送信することで安全性の向上を図る手法をついて述べる．

3.2 提案手法

ネットワークは非循環有向グラフ$G=(V,E)$であるとする．送信ノードから各受信ノードへh本の独立なパスが存在し，各パスは有限体GF_q上の 1 シンボルを送信することができる．

アルゴリズム 1(使用できる余剰ネットワークの決定)

I. 送信ノードは各受信ノード$t\in T$に達する独立なh本のルート$f^t=(p_{t,1},\cdots,p_{t,h})$を探索する． $f^t(e)$はルートf^t上のエッジeの始点ノードを表す．
II. 全てのノードを送信ノードから順に位相的順序に並べ，この際，位相的順序が同じノードには同じ順序を割り当て，すべての受信ノードを同じ位相的順序に設定する．
III. $F=\bigcup_{t\in T}f^t$とする．
IV. 順序付けられたノードを送信ノードsを含む集合$\mathcal{S}$とすべての受信ノードTを含む集合$\mathcal{T}$にカットする．カットする際は集合$\mathcal{S}$が最も大きくなるものから順に選択していく．$\mathcal{S}=\{s\}$なった場合 VII へ進む．
V. 選択したカットに$c\in C$ついて，$u\in\mathcal{S}$, $v\in\mathcal{T}$である，すべてのパス$(u,v)\in E$の始点ノードuについて，送信ノードsからすべてのノードuへFと辺素なパスを用いて，マルチキャストする最大フローがa_cであるとき，ノードuは送信ノードで生成した乱数をa_c個打ち消すことができるノードとなる．送信ノードからすべてのノードuへのFと辺素であるルートを$f^u=(p_{u,1},\cdots,p_{u,a_c})$とする．
VI. $F=F\cup f^u$とする．IV へ戻る．
VII. 送信ノードは$a=\sum_{c\in C}a_c$個の乱数を送信可能である．

アルゴリズム 2(余剰ネットワークへの符号ベクトルの割り当て)

アルゴリズム 1 について，カットは選択した順に$c_1,c_2,\cdots,c_j$であり，各カットにおけるuへは$a_{c_1},a_{c_2},\cdots,a_{c_j}$個の乱数が送信可能であるとする．

I. 余剰ネットワークを用いて送信ノードはa個の乱数を生成，送信可能であるとする．
II. アルゴリズム 1 で選択したカット$c_1,c_2,\cdots,c_j$におけるu余剰ネットワーク上のルートf^uに Jaggy らの方式に沿って，符号ベクトルを決定する．
   - c_jにおけるuへは，a_{c_j}個の乱数送信するため，$h+1\le i\le h+a_{c_j}$行がそれぞれ決定した符号ベクトルでそれ以外の部分が 0 となる符号ベクトルとなる．
   - c_{j-1}におけるuへは，a_{c_j}個の乱数送信するため，$h+a_{c_j}+1\le i\le h+a_{c_j}+a_{c_{j-1}}$行がそれぞれ決定した符号ベクトルでそれ以外の部分が 0 となる符号ベクトルとなる．
   ⋮
   - c_1におけるuへは，a_{c_j}個の乱数送信するため，$h+a_{c_j}+a_{c_{j-1}}+\cdots+a_{c_2}+1\le i\le h+a$行がそれぞれ決定した符号ベクトルでそれ以外の部分が 0 となる符号ベクトルとなる．

アルゴリズム 3(f^t上のパスへの符号ベクトルの割り当て)

I. 2.4 節の Jaggy らの方式に沿って予めf^t上のパスへ符号ベクトルを割り当てておく．
II. 仮想ノードs'をグラフ$G=(V,E)$に追加し，s'からsへa本のパス$\{e_1,\dots,e_a\}$を追加する．$h+1\le i\le h+a$，$b(e_i)=\left[0^{i-1},1,0^{h-i}\right]^T$を割り当てる．また，$B_t=\{b(e_1),\dots,b(e_a)\}$とする．
III. $v\in V$を位相的順序で選び、f^t上のパスeについて以下を行う．乱数がa_c個含まれるエッジについて，任意のa_c本のエッジに割り当てられる符号ベクトル乱数を$\left[0^{i-1},1,0^{h+a_c-i}\right]^T(1\le i\le h)$と線形独立にとる条件を加えて以下を行う．
   - 通常の中継ノードの場合

   (a)以下を満たす$b(e)$を決定し，割り当てる．

   全てのtについて

   $b(e)=\sum_{p\in P(e)}m_p(e)b(p)$

   $\left(B_t\setminus\left\{b\left(f^t_{\leftarrow}(e)\right)\right\}\right)\cup\{b(e)\}$が線形独立 k

   (b)各$t\in T(e)$に対して

   $C_t=(C_t\setminus\{f^t_{\leftarrow}(e)\})\cup\{e\}$

   $B_t=\left(B_t\setminus\left\{b\left(f^t_{\leftarrow}(e)\right)\right\}\right)\cup\{b(e)\}$

- 乱数を打ち消し可能な中継ノードの場合

(a)以下を満たす$b(e)$を決定し割り当てる．

全てのtについて

$b(e) = \sum_{p \in P(e)} m_p(e) b(p)$

$\left(B_t \setminus \left\{b\left(f_{\leftarrow}^{t}(e)\right)\right\}\right) \cup \{b(e)\}$が線形独立

$b(e)$の打ち消す乱数に対応する行を 0

(b)各$t \in T(e)$に対して

$C_t = (C_t \setminus \{f_{\leftarrow}^{t}(e)\}) \cup \{e\}$

$B_t = \left(B_t \setminus \left\{b\left(f_{\leftarrow}^{t}(e)\right)\right\}\right) \cup \{b(e)\}$

IV. 符号ベクトル$b(e) = [0^{h+a}]$となった時点で終了し，残りのパスには$[0^{h+a}]$を割り当てる．

V. 予め割り当てられている符号ベクトルとの和をとり新たな符号ベクトルとする．

例)

図 5 のネットワークに余剰ネッワークを用いて符号ベクトルを割り当てる．

アルゴリズム 1 を用いる．送信ノードは各受信ノードに達する独立な 2 本のルートを探索する．$t1$について$\{s \to 1 \to t1\}$，$\{s \to 2 \to t1\}$であり，$t2$について$\{s \to 1 \to t2\}$，$\{s \to 2 \to t2\}$となる．

全てのノード$\{s, 1,2, t1, t2\}$の位相的順序付けを行う．$order1 = s$，$order2 = 1,2$，$order3 = t1, t2$となる．カットc_1は$\mathcal{S} = \{s, 1,2\}$，$\mathcal{T} = \{t1, t2\}$であり，すべての始点ノード$u = 1,2$ へ送信ノードsからf^uを用いてマルチキャストする最大フローは 1 でありノード$u = 1,2$は送信ノードで生成した乱数を$a_{c_1} = 1$個消去可能となる．

アルゴリズム 2 を用いる．$i = 3$であり，$b(s', s) = [0,0,1]^T$をとなり，これを元に送信ノードsから各受信ノード$u = 1,2$まで符号ベクトルを割り当てる．すなわち，図 6 のようになる．

アルゴリズム 3 を用いる．$i = 3$であり，$b(s', s) = [0,0,1]^T$となり，順に$b(s,1) = [0,0,1]^T$，$b(s,2) = [0,0,1]^T$，$b(1,t1) = [0,0,1]^T$，$b(2,t1) = [0,0,1]^T$，$b(1,t2) = [0,0,1]^T$，$b(2,t2) = [0,0,1]^T$となる．すなわち，乱数部分は図 7 のようになる．Jaggy らの方式により予め割り当てられた符号ベクトルとの和をとることで，全体として図 5 のような符号ベクトルが割り当てられる．

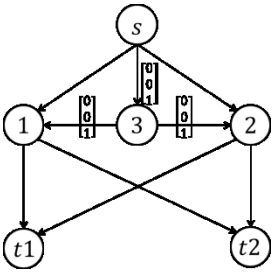


図 6 余剰ネットワークへの符号ベクトル割り当て

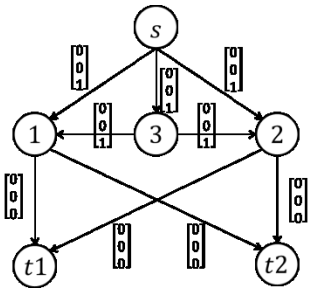


図 7 符号ベクトルの割り当て(乱数部分)

4. 安全性について

提案手法により割り当てた符号ベクトルを用いて，送信ノードから秘密情報及び，中継ノードで打ち消される乱数を送信する場合，ネットワーク中の乱数がt個含まれる領域において，盗聴されるt個の独立なパスからは秘密情報に関して何も漏れない．すなわち，ネットワーク中の一部分についてt-secure となるようなネットワーク符号となっていることが分かる．また，送信ノードから送信する情報を秘密情報$S = (s_1, \cdots, s_h)$から，秘密情報s_1と乱数$r_1, \cdots, r_{h-1}$を含む$S' = (s_1, r_1, \cdots, r_{h-1})$とし，既存の安全なネットワーク符号化を利用することで，ネットワーク上一部分では最大で$h + t - 1$-secure なネットワーク符号とすることができる．

5. おわりに

本稿では，最大フローを達成しつつ余剰ネットワークを利用して，乱数を送信ノードから生成し送信，中継ノードで打ち消すことで通信路の盗聴に関して部分的にt-secure な安全性を達成可能な手法を示した．本手法は既存の安全なネットワーク符号化手法と組みわせることでさらに安全性の向上を図ることが可能である．今後の課題としては，本手法を用いるのに適した余剰ネットワークが，ネットワーク中にどの程度存在するのか検証する必要があると考えている．

謝辞　熱心にご教授くださった先生方及び研究室の皆様に感謝申し上げます.

参考文献

1) R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W.-H. Yeung, “Network information flow,” IEEE Trans. Inf. Theory, vol. IT-46, pp. 1204-1216, Apr. 2000.
2) S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen. Polynomial time algorithms for multicast network code construction. IEEE Trans. Inf. Theory, 2003.
3) N. Cai, and R. W. Yeung, “Secure network coding,” in Proc, IEEE Int. Symp. Inf. Theory. (ISIT), Lausanne, Switzerland, June 2002, p. 323.
4) S. Li and R. W. N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, pp. 371-381, 2003
5) T. Ho, M. Medard, and R. Koetter, “A Random Linear Network Coding Approach to Multicast” IEEE Trans. Inf. Theory. Vol. 52, pp.4413-4430
6) K. Harada and H. Yamamoto, “Strongly secure linear network coding,” IEICE Trans. Fundamentals, vol. E91-A, No. 10 October 2008.
7) N. Cai, R. W. Yeung, “Secure Network Coding on a Wiretap Network” IEEE Trans. Inf. Theory, vol. 57, no. 1, January 2011
8) W. Huang, T. Ho, M. Langberg, and J. Kliewer, “On secure network coding with uniform wiretap sets,” in IEEE NetCod, 2013.
9) T. Cui, T. Ho, and J. Kliewer, “On secure network coding with uniform wiretap sets,” IEEE Trans. Inf. Theory, vol. 59, pp. 166-176, 2013
10) 久保祐樹, 山本博資, “補助ノードを用いた安全な線形ネットワーク符号構成多項式アルゴリズム,” The 33rd Symposium on Information Theory and its Applications (SITA2010)Matsushiro, Nagano, Japan, Nov. 30 Dec. 3, 2010