論文の内容の要旨

論文題目：　安全なネットワーク符号化

氏名：　原田 邦彦

Ahlswede-Cai-Li-Yeungによって提案されたネットワーク符号化は，ネットワークの各点で符号化を行える場合を考え，情報を送信する情報源点と情報を受信する受信点の間により多くの情報を伝送するための符号化に関する研究分野である．コンピュータネットワークなど，情報通信網は複数の通信路と通信路を結ぶ節点をネットワークとしてモデル化できる．特に 1 個の情報源点から複数個の受信点へと完全に同一の情報を伝送する通信問題はマルチキャスト通信と呼ばれ，この通信問題に対しては伝送可能な情報量の上限がネットワークフローにおける各受信点に対する最大フローの最小値で与えられることが知られている．また，この上限を達成する符号は線形ネットワーク符号化で構成できることが知られている．以下では，マルチキャスト通信で伝送可能な最大の情報量を h で表す．図 1に，マルチキャスト通信におけるネットワーク符号の一例を示す．例では，点 v_3 において符号化を行うことで，情報源点 s から 2 個の受信点 t_1, t_2 に長さ 2 の情報 (x_1, x_2) の情報伝送を可能にしている．

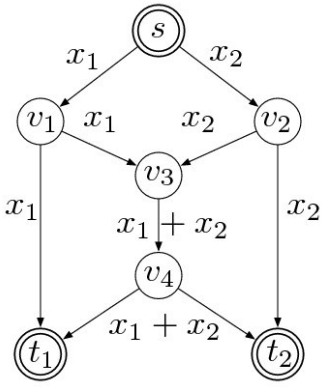

図 1　Ahlswede-Cai-Li-Yeung によるネットワーク符号化の例

一方で，ノンマルチキャスト通信に対する伝送可能な情報量の領域に関しては，ほとんどが未解決問題となっているが，厳密な領域が示されている問題の一つに，1 個の情報源点から 2 個の受信点への一般の通信問題がある．この問題では，2 個の受信点の各々に対する個別情報と両方の受信点に対する共通情報を考えれば十分である．これらの各情報量を $\omega_1, \omega_2, \omega_0$ とする．この領域に含まれる任意の情報量を持つ情報を伝送可能な符号も線形ネットワーク符号化で構成できることが知られている．しかし，既存の研究で示されている符号構成手法は $h = \omega_0 + \omega_1 + \omega_2$ としたマルチキャスト通信問題に帰着する証明的手法で，実用的に使いやすい符号とは言えなかった．

本論文では，ネットワークに盗聴者が介在する場合に，情報を秘匿して伝送可能な線形ネットワーク符号化を扱った．ここでの情報秘匿特性は，情報量的安全性によるものであり，将来にわたって安全であることが保証されない計算量的安全性によるものではない．また，各点があらかじめ暗号化のための共通鍵を秘密に共有している仮定もおかない．本論文の成果を以下にまとめる．

まず，第 3 章では第一に，マルチキャスト通信に対して情報秘匿特性を持つ安全な線形ネットワーク符号を提案した．同じ方向性を持つ先行研究として，長さ r の秘密情報 S^r を伝送するとき，ネットワークの任意の k 本以下の枝を盗聴されても S^r に関する情報が全く漏洩しないという情報秘匿を扱ったものがある．この場合には，$r \le h-k$ であることが秘匿して伝送可能な必要十分条件であることが知られている．本論文では，この情報秘匿特性をweakly k-secureと呼び，これをさらに強めた情報秘匿であるstrongly k-secureを定義した．Strongly k-secureな情報秘匿は，k-secureであり，かつ $j=1,2,\mathrm{K},r-1$ に対して $k+j$ 本の枝を盗聴されても，秘密情報の任意の $r-j$ シンボルが完全に漏洩しない手法である．本論文では，strongly k-secureな情報秘匿を達成できる必要十分条件もまた $r \le h-k$ であることを導出した. 具体的には, この条件が満たされた場合に対して, strongly k-secure な 2 つの符号構成アルゴリズムを示した．1 つは符号構成時に直接安全となるように符号を構成する手法であり, もう 1 つは既存の安全とは限らない線形ネットワーク符号を線形変換することによる手法である．$r \le h-k$ は，非線形符号を用いた場合にも導出できる上界であり，$r > h-k$ を達成できないという意味で，本論文による手法よりも効率の良い符号化手法は存在しない． 図 1の符号例を用いて，weakly 1-secureな情報秘匿とstrongly 0-secureな情報秘匿の 2 つの例を示す．Weakly 1-secure な情報秘匿を行って秘密情報 w を伝送するには，一様乱数情報 p を用意し，$(x_1, x_2) = (w+p, p)$ として伝送すればよい．このとき，任意の 1 本の枝を盗聴されたとしても，（アルファベットサイズが 3 以上であれば）w に関する情報は全く漏洩しない．これに対し，strongly 0-secureに秘密情報 w_1, w_2 を秘匿して伝送するには，$(x_1, x_2) = (w_1+w_2, w_1+2w_2)$ として伝送すればよい．このとき，任意の 1 本の枝が盗聴されたとしても，（アルファベットサイズが 4 以上であれば）w_1, w_2 の線形関係は漏れるが，それぞれの値は全く漏洩することはない．このように，strongly 0-secureな情報秘匿は，$k=0$ の場合でも安全性が意味を失わない符号となる．しかも，この例では，weakly 1-secure に伝送する w と同程度の情報秘匿を達成しながら，strongly 0-secureでは 2 個の秘密シンボルを伝送することができている．

第 3 章では第二に，strongly k-secure な線形ネットワーク符号が存在するために必要な有限体アルファベットサイズを議論した．線形ネットワーク符号はその計算の利便性から，アルファベットとして有限体を用いることが多い．そのサイズは実用上できるだけ小さいことが求められるが，あまり小さくすると符号が構成できなくなってしまう．そこで，符号が存在するために必要なアルファベットサイズを評価する必要がある．符号に課す制約が増えることから，情報秘匿しない場合よりも weakly k-secure に構成する場合の方が，またそれよりも strongly k-secure に構成する場合の方がより大きい有限体を必要とする. 実際に, 有限体のサイズを評価し, この事実を確認した. また, weakly k-secure の場合に対して示されたものと同じように，$h-k$ と r とのギャップを大きくすればするほど指数的に小さな有限体をアルファベットとして用いることができることを示した．

第 3 章では第三に，ネットワークの余剰なリソースを利用して情報秘匿を達成する手法を提案した．Weakly k-secure や strongly k-secure に秘密情報を秘匿して伝送する場合，情報源点と受信点との

間のマルチキャスト通信だけを利用すると，大きくても$r = h - k$の情報量を持つ秘密情報しか伝送することができない．しかし，一般にはこのマルチキャスト通信には利用していない通信リソースが多くある．これを利用して安全なネットワーク符号を構成することを考えた．具体的には，以下のように書ける．元のネットワークの問題にある変換を行った通信問題でのマルチキャスト容量がh'（必ず$h' \geq h$となる）であるとする．このとき，情報量hを持つ秘密情報を weakly $(h'-h)$-secure あるいは strongly $(h'-h)$-secure に秘匿する符号を構成できることを示した．視点を変え，k-secure な情報秘匿のkを固定して考えれば，秘匿して伝送可能な秘密情報量は$r \leq \min(h, h'-k)$である．

第 4 章では，1 個の情報源点から 2 個の受信点に個別情報と共通情報を伝送する問題に対して，その 3 つの情報（各々の受信点に対する個別情報と共通情報）を伝送するルートを完全に分離できる分離符号化が可能なことを，具体的な構成法を示すことにより証明した．分離符号化を用いると，情報量ω_1, ω_2を持つ個別情報はそれぞれ符号化を行わずルーティングで伝送し，情報量ω_0を持つ共通情報は$h = \omega_0$としたマルチキャスト通信で伝送することができる．また，既存手法より符号化を行う点を減すことができ，その結果小さい次元で符号化を行え，符号化の計算量を減すことができる．既存手法による符号化手法には，マルチキャスト通信に対して提案した安全なネットワーク符号をそのまま応用することができなかったが，分離符号化を用いればそのままに適用できることを示した．さらに，安全なネットワーク符号化を含めたさまざまな機能を持つ任意の符号化をそのまま適用可能である．本論文では，この適用を行った場合に対し，符号化の実現のために必要な有限体アルファベットサイズの評価も行った．

以上のように，本論文では既存の手法に比べより強い情報秘匿特性をネットワーク符号に導入し，その効率化を図った．また，既存の手法はマルチキャスト通信にしか応用できない符号であったが，より広い通信のクラスに対して情報秘匿特性を導入することに成功した．