修士論文審査用資料

盗聴者に対して安全なネットワーク符号化

数理情報学専攻 46219 原田 邦彦
指導教員 山本 博資 教授

2006 年 2 月 7 日

概要

盗聴者に対して安全なネットワーク符号化は，$r = h - k$ のもとに，受信者が長さ h の情報を得ることができるとき，盗聴者が任意の k 本以下の辺を流れる情報を盗聴をすることができるとしても，情報量的に安全に長さ r の秘密情報 S^r を伝送することができるように考えられたものである．盗聴者に対して安全なネットワーク符号化における既知の研究は，盗聴者が $j(k < j < h)$ 本の辺から情報を盗聴したとき， S^r の一部である S^{h-j} が漏洩してしまうかもしれず，完全に安全ではない．本稿では強いランプ型秘密分散法の概念に基づき，盗聴者が $j(k < j < h)$ 本の辺から情報を盗聴したとしても S^{h-j} が完全に安全となる strongly k-secure な符号の必要十分条件を示し，さらに符号化に十分な各 S_i のアルファベットの条件を示す．

1 はじめに

ネットワークにおいて複数の点の間で，情報を誤りなく伝送する問題を考える．ネットワークの各辺を通信路とみなせば，ネットワークはインターネットなどの通信路ネットワークをよくモデル化している．この問題に対して，Ahlswede-Cai-Li-Yeung [1] は，ネットワークの各点で符号化が許される場合を考え，伝送可能な情報量の上限を与え，そのような符号化をネットワーク符号化と呼んだ．

Cai-Yeung [2] や Feldman-Malkin-Servedio-Stein [3] は盗聴者が通信路から情報を盗聴することを考え，盗聴される通信路の本数があるしきい値以下ならば情報量的に完全に安全であるネットワーク符号の必要十分条件を与えた．しかし，これらの手法はしきい値以上の通信路の盗聴に対する安全性を考慮していない．そこで，本稿では強いランプ型しきい値秘密分散法 [6] の概念を応用し，しきい値以上の通信路を流れる情報の盗聴に対して強いランプ型の安全性を保証するような符号化の必要十分条件を与える．さらに，そのような符号化が存在する有限体アルファベットサイズを与える．

2 ネットワーク符号化

点集合を V，辺集合を $E \subseteq V \times V \times \mathbb{N}$ で表したとき，ネットワークは有向グラフ $G = (V, E)$ で表される．各辺はそれぞれ，その通信路の性能を表す容量を持つが，本稿では単位容量とする．単位容量とは，要素数 q の有限体を $\mathbb{F}_q$ としたとき，各辺（各通信路）は単位時間に $\mathbb{F}_q$ の要素を 1 つだけ誤りなく伝送できることを意味する．本稿で扱うネットワークは，有向閉路が存在しないこと (acyclic) を仮定する．

今, 単一の情報源点 (source node) $s \in V$ と, 受信点 (sink node) の集合 $T \subset V$ を持つネットワークで，情報源点から全ての受信点に同一のメッセージ $X^n = (X_1, X_2, \ldots, X_n)$ を伝送する問題を扱う．この問題をマルチキャストと呼ぶ．ここで，各 X_i はアルファベット $\mathcal{X} = \mathbb{F}_q$ の値をとるものとし，無記憶な一様分布に従うものとする．ネットワーク符号化は，各点において符号化が許される場合を考える．マルチキャストにおけるネットワーク符号化において，全ての受信点に単位時間で伝送できるメッセージ長 n が，式 (1) で定義される h に対して，$n \leq h$ であることが符号存在の必要十分条件であることが示されている [1].

$$h = \min_{t \in T} \text{max-flow}(s, t). \tag{1}$$

ここで，記号 max-flow(s, t) は，s–t 間の最大流を表す．また，等号を達成する符号化は線形符号のみで十分である [5]. 本稿では $n = h$ を達成する線形ネットワーク符号化を考える．つまり，各点における符号化が，点の得た情報の線形結合であらわされる場合である．このとき，各辺を流れる情報は入力の情報 X^h の線形結合として表すことができる．辺 e を流れる情報を $X^h b(e)$ として表せるようなベクトル $b(e)$ を符号化ベクトルと呼ぶと，線形ネットワーク符号化は各辺にこの符号化ベクトルを以下の条件を満足するように割り当てることである．

- ある点を始点とする辺に割り当てられる符号化ベクトルは，その点を終点とする辺に割り当てられた符号化ベクトルの線形結合である．
- 受信点を終点とする辺に割り当てられた符号化ベクトルのなす空間は h 次元である．

このとき，全ての辺の符号化ベクトルを横に並べた行列を Z とする．Z の構成アルゴリズムは Jaggi-Sanders-Chou-Tolhuizen [4] などに従う．

3 strongly k-secure な符号化法

必ずしも盗聴者に対して安全とは限らないような線形のネットワーク符号 Z が与えられているものとする．今，長さ $r \leq h$ の秘密情報 S^r を盗聴者に対して安全に伝送することを考える．ここで，盗聴者は Z を完全に知っているものとし，暗号化は公開の情報 M を用いて行う．任意の辺集合 $A \subset E$ に対して，その要素に対応する符号化ベクトルを並べた行列を Z_A で表すことにする．X^h に線形変換 M^{-1} を施して $X^h M^{-1}$ をネットワークに流すときに，S^r が盗聴者に対して安全になるような，2 つのしきい値型の安全特性を次に定義する．なお，$H(\cdot)$ はエントロピー関数である．

定義 1 (k-secure) $\text{rank} Z_A \leq k$ を満たす任意の A について正則行列 M が次の等式を満足する．

$$H(S^r | X^h M^{-1} Z_A) = H(S^r). \tag{2}$$

定義 2 (strongly k-secure) 正則行列 M が k-secure であり，かつ $k \leq \text{rank} Z_A < h$ を満たす任意の A について次式

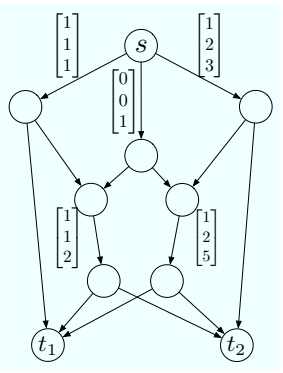

図 1　strongly k-secure

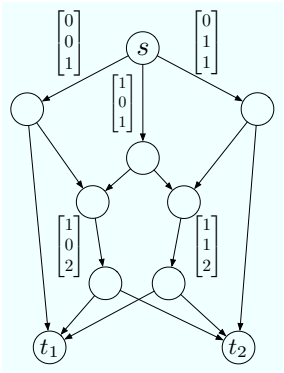

図 2　non-strongly k-secure

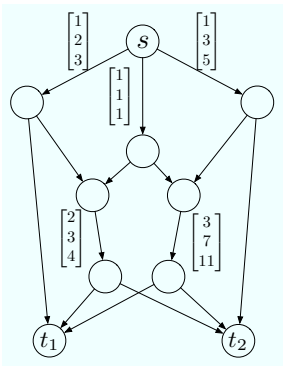

図 3　$k = l = 0$ で strongly k-secure

を満たす.

$$H(S_{i_1},S_{i_2},\ldots,S_{i_{h-\mathrm{rank}Z_A}}|X^hM^{-1}Z_A) = \frac{h-\mathrm{rank}Z_A}{r}H(S^r), \quad (3)$$
$$\forall S_{i_1},S_{i_2},\ldots,S_{i-h-\mathrm{rank}Z_A} \in \{S_1,\ldots,S_r\}.$$

k-secure な線形変換 M は $r \le h-k$ ならば十分に大きな有限体上に存在することが示されている [2, 3]. いま, $X^h = (S_1, S_2, \ldots, S_r, R_1, R_2, \ldots, R_l), r+l = h, l \ge k$ として, X^hM^{-1} をネットワークに伝送することを考えるとき, M が strongly k-secure となる必要十分条件は次の定理で与えられる.

定理 1 $r \le h-k$ ならば, 十分に大きな有限体上に strongly k-secure な線形変換 M が存在する. また, M が strongly k-secure であることと, $0 \le j < r$ を満たす任意の j について, Z 中の任意の最大 $k+j$ 個の線形独立な列ベクトルと, M の最初の r 列のうちの任意の $r-j$ 個の列ベクトルが線形独立であることは同値である.

例 1 図 1 に $r = 2, h = 3, l = k = 1$ のときの strongly k-secure な符号構成例を示す. 図 2 は比較のために同じ条件のもと strongly でない k-secure な符号構成例をしめしたものである. 各辺に示されたベクトルは $X^3 = (S_1, S_2, R_1)$ のどのような線形結合が流れているかを示すものである. Non-strongly の場合は $[1,0,2]^{\mathrm{T}}, [1,1,2]^{\mathrm{T}}$ に対応する辺の盗聴から S_2 の値が陽に漏洩してしまうが, strongly の場合は漏洩しない.

また, strongly k-secure ならば, $k = l = 0$ においても, 安全性に意味を持つ. 図 3 の例では, 任意の 1 本の盗聴に対して任意の 2 シンボルが安全であり, 任意の 2 本の盗聴に対して任意の 1 シンボルが安全な符号となっている.

表 1　有限体のサイズの評価

	$k < l, k = \mathrm{o}(\lvert E\rvert)$	$k < l, k = \Theta(\lvert E\rvert)$
k-secure	$(k+1)^{\frac{1}{l-k}}\lvert E\rvert^{\frac{k}{l-k}}$	$2^{\Omega\left(\frac{k}{l-k}\right)}$
strongly k-secure	$(k+r)^{\frac{1}{l-k}}2^{\frac{r}{l-k}}\lvert E\rvert^{\frac{k+r}{l-k}}$	$2^{\Omega\left(\frac{k}{l-k}\left(1+\frac{r}{\lvert E\rvert}\right)\right)}$

4　符号化が存在する有限体アルファベットのサイズ

前節まで, 十分に大きな有限体を仮定し, その上での符号化の議論を行った. しかしながら, 実用上の観点からは, 有限体のサイズは可能な限り小さいことが望まれる. 文献 [4] などによれば, $q \ge |T|$ が線形ネットワーク符号を構成可能な十分条件であるが, 盗聴者に対する安全性を確保しようとすれば, 制約条件が増えることからより大きなサイズの有限体が必要になると言うことができる. そこで, 本研究では, strongly k-secure な線形変換 M が存在する有限体のサイズを評価した. この結果を表 1 に示す. k-secure については, 文献 [3] による. なお, $k = l$ の際には, k-secure のとき, $|E|^{\Omega\left(\sqrt{\frac{k}{\log k}}\right)}$ という非常に大きな有限体が必要なことが示されている. Strongly k-secure の場合は未解決であるが, これよりも大きなものが必要なことは言うまでもない. $l > k$ にとるのが実用上は良いといえるだろう. また $k = \Theta(|E|)$ のとき, k-secure なものと strongly k-secure なものがほとんどかわらない有限体上に存在することに着目されたい. また, 一般の $\mathcal{A} = \{A_1, \ldots, A_{|\mathcal{A}|}\}$ の盗聴に対して安全な符号化が存在する有限体は, $q \ge |\mathcal{A}|^{\frac{1}{l-k+1}}$ で十分であることを見積もった. これは, $l = k$ のとき, Cai-Yeung [2] の結果に一致するものである.

5　まとめと今後の課題

本稿では, 盗聴者に対しての強い意味での安全性として strongly k-secure な線形変換 M を定義し, その必要十分条件を与えた. さらに, 符号化が存在するのに十分な有限体のサイズを評価した.

今後の課題としては, strongly k-secure な符号化が $k = l$ で存在するための有限体のサイズを評価し, よりタイトなサイズを求めることが必要である. その他, 異なる安全性条件のもとでの符号化の構成や, マルチキャスト以外の問題に対しての考察が必要であろう.

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] N. Cai and R. W. Yeung, "Secure network coding," in *IEEE ISIT'02*, Lausanne, Switzerland, June 2002, p. 323.

[3] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," in *42nd Ann. Allerton Conf. on Comm., Control, and Comp.*, 2004.

[4] S. Jaggi, P. Sanders, P. A. Chou, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. on Inform. Theory*, vol. 51, no. 6, pp. 1973–1982, June 2005.

[5] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. on Inform. Theory*, vol. 49, no. 2, pp. 371–381, February 2003.

[6] 山本博資, "(k, L, n) しきい値秘密分散システム," **電子通信学会論文誌**, vol. J68-A, no. 9, pp. 945–952, September 1985.