様式 C-19

# 科学研究費補助金研究成果報告書

平成 22 年　5 月 28 日現在

研究種目：基盤研究(C)
研究期間：2007～2009
課題番号：19560384
研究課題名（和文）　オーバーレイ可能な機能的ネットワーク符号化に関する研究

研究課題名（英文）　Research on overlay network coding

研究代表者
桑門　秀典　　(KUWAKADO HIDENORI)
神戸大学・大学院工学研究科・准教授
研究者番号：30283914

研究成果の概要（和文）：ネットワーク符号化は，中継ノードで適切な符号化を行うことで，ネットワークがもつ伝送効率を最大にする技術である．近年，伝送効率の向上だけでなく，様々な機能がネットワーク符号化により実現できることが分かってきた．本研究では，送信者が受信者を動的に選択できる符号化法を提案し，その符号化法が適用できるネットワーク形状を明らかにした．また，本研究では，ネットワーク的計算と並列計算法であるビットスライス計算の類似性に着目し，既知のビットスライス計算の最適性をネットワーク的計算の立場から検討を行った．

研究成果の概要（英文）：Network coding is a method to improve transmission efficiency with encoding of internal nodes.　Recent works on network coding show that network coding is for achieving not only an efficient transmission but also useful functions. This research shows a network code for selecting receivers dynamically without changing encoding rules of internal nodes.　In addition, we study the optimality of a bitslice implementation in the context of network computing. This is based on the similarity of the bitslice implementation and the network computing.

交付決定額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 2007 年度 | 2,200,000 | 660,000 | 2,860,000 |
| 2008 年度 | 600,000 | 180,000 | 780,000 |
| 2009 年度 | 700,000 | 210,000 | 910,000 |
| 年度 | | | |
| 年度 | | | |
| 総　計 | 3,500,000 | 1,050,000 | 4,550,000 |

研究分野：暗号理論
科研費の分科・細目：電気電子工学　通信・ネットワーク工学
キーワード：暗号・セキュリティ　ネットワーク符号化

## １．研究開始当初の背景

インターネットでは，映像配信，音楽配信のようなアプリケーション，つまり，大きなサイズのデータを多人数に同時配信するアプリケーションの需要は日増しに高まっている．しかし，そのようなアプリケーションをクライアント・サーバモデルで実現すると，サーバやネットワークの負荷が過大になる

ことが懸念される．そこで，ネットワーク上に点在する中継ノードにサーバの役割を分散させるP2Pネットワーク技術が期待されている．

理論的には，2000年にAhlswedeらは，中継ノードが入力シンボルを適切に符号化(ネットワーク符号化)して次ノードに送信すると，多人数へ同時配信できるスループットが向上すること及びその限界を示した．2005年にJaggiらがその限界スループットを達成する具体的な符号化法を示した．現在のP2Pアプリケーションにおいては，中継ノードはデータのキャッシュなどの単純な役割しかしていないが，Ahlswedeらと Jaggiら結果は，中継ノードが知的な符号化をすれば，より高速にデータ配信できることを意味している．

現在までに，同時配信できる限界スループットの達成に関しては，理論的には解決済みであり，実装・実用化をする段階にある．次の研究課題は，ネットワーク符号を高機能化することである．高機能化の一例は，盗聴に対する安全性である．Feldmanらは，送信データに事前に適切な線形変換を施せば，既存のネットワーク符号を変更することなく，盗聴に対して安全になることを示した．この結果は，限界スループットを達成する符号化と盗聴に対して安全な符号化は分離できる，ということを示唆している．このことから，研究代表者は，限界スループットを達成する符号化の上に，別の機能を実現する符号化を重ね合わせることができるのではないか，という着想を得た．このような符号化を「機能的オーバーレイネットワーク符号化」と呼ぶことにする．

２．研究の目的

本研究で実現するオーバーレイネットワーク符号化の機能をあげる．

（１）受信者の選択

送信者が送信データに応じて最終的な受信者を動的に選択できる機能．この機能は，有料のデータ配信には必須である．受信者を選択することはルーティングでも実現できるが，ネットワーク符号化を用いれば，より効率良くデータを送信できる見込みがある．

（２）ネットワーク的計算

複数送信者は其々がもつデータをネットワークに入力し，中継ノードが適切な計算を行うことにより，一人の受信者にその計算結果が伝わる機能．これは，一般に，計算結果のデータ量が入力データ量よりも少なくなることに着目し，ネットワーク上で伝送されるデータ量を削減できる見込みがある．

これらの機能を実現する符号化法を一つの独立した層として考案することが，本研究の研究目標である．本研究の独創的な点は，``オーバーレイ''，つまり，限界スループットを達成するネットワーク符号を最下位層とし，その上に異なる機能を実現するネットワーク符号を層として，いくつもオーバーレイする点である．

研究代表者がこれまで行ってきた暗号学的プロトコルの研究では，end-to-endの通信を想定し，中継ノードを一切考慮していなかった．じつは，暗号学的プロトコルの分野では，先にあげた機能の一部は end-to-end の通信では実現できることがすでに示されている．そこで，ネットワーク符号化で示された「中継ノードにおける知的処理」を前提に，暗号学的プロトコルを見直し，その結果をオーバーレイ・ネットワーク符号化として実現する点が本研究の特色である．

異なる機能のネットワーク符号が完全に独立した層として実現できれば，既存のネットワークを変更することなく，必要な機能や新しい機能を自由に追加できるようになり，利便性が向上するとともに，P2P ネットワーク技術への応用が期待できる．

３．研究の方法

（１）「受信者の選択」のための符号化法

最初に，1ビットのデータを二人の受信者に選択的に送信できる符号化を検討する．次に，それを複数ビットに拡張する．その後，受信者の数を増やすような符号化を検討し，この方法で適用可能なネットワークの形状を明らかにする．

（２）「ネットワーク的計算」のための符号化法

この計算法は，研究期間中にNetwork computingとして，Appuswamyらによって提案された．この計算法は，データをビット毎に分割し，ビット毎に演算を行うビットスライス計算と類似している．まず，ネットワーク的計算とビットスライス計算の類似性を検討し，ビットスライス計算のアルゴリズムをネットワーク的計算に応用する．そして，相互の計算法における計算の最適性の議論が相互に適用できないか調べる．

４．研究成果

（１）「受信者の選択」のための符号化法

① 通常の network code

バタフライネットワークと呼ばれる図1の有向グラフを考える． このグラフは，ソース集合(送信者集合)が $\{1\}$ で，シンク集合(受信者集合)が $\{6,7\}$ のネットワークである．ノード1をAlice，ノード6をBob，ノード7を Charlie と呼ぶことにする． このネットワークの辺は，$\{0,1\}$ のシンボルを通信でき，

各ノードは法 2 の加算の演算を行うことができる.

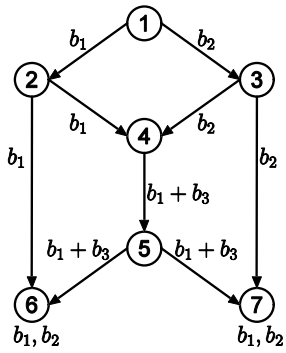


図 1:通常の network code

Bob は, $s_1$ と $s_1 + s_2 \bmod 2$ を受信する. Bob が受信した記号 $(r_{6,1}, r_{6,2})$ は, 下記のように書ける.

$$\begin{pmatrix} r_{6,1} \\ r_{6,2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}, \qquad (1)$$

ここで, 算術演算は, $GF(2)$ の上で行われる. Bob は, 上記の行列の逆行列に $(r_{6,1}, r_{6,2})$ を乗ずると, $(s_1, s_2)$ を得ることができる. 同様に, Charlie が受信した記号 $(r_{7,1}, r_{7,2})$ は下記のように書ける.

$$\begin{pmatrix} r_{7,1} \\ r_{7,2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix}.$$

②受信者の選択ができる network code

Alice は, 通常は Bob と Charlie の両方に同じ情報を送っているが, Alice は, 時々, Bob にのみ, あるいは Charlie のみ情報を送りたい ことがあるとしよう. これを実現する方法の一つは, Alice がノード 2 またはノード 5 に Bob にシンボル を送信しないように依頼することである. それらのノードにそのような依頼をしなくても, Bob または Charlie にだけ情報を送る符号化を以下に示す.

ネットワークの辺が $M_4 = \{0,1,2,3\}$ のシンボルを送信できると仮定する. $M_4$ 上の演算は, 法 4 の乗算で定義される. $M_4$ は群ではないことに注意. 図 2 から分かるように, 通常のネットワーク符号との差異は, ノード 4 の符号化である. ノード 4 の符号化は, 入力シンボル $s_1, s_2 \in M_4$ に対して下記のように定義される.

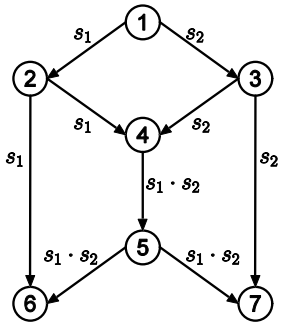


図 2 : 受信者の選択ができる network code

$$E(s_1, s_2) = s_1 \cdot s_2 \bmod 4$$

その他のノードの符号化は, 通常のネットワーク符号と同じである. このネットワーク符号を用いると, Alice は 1 ビットのデータを Bob にだけ, Charlie にだけ, あるいは両方に送るというように, 受信者を選択することができる.

表 1: $s_1$

| $u \diagdown r_1$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 3 |
| 1 | 1 | 3 |

表 2: $s_2$

| $u \diagdown r_1$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 3 |
| 1 | 3 | 1 |

表 3: $s_1 s_2 \bmod 4$

| $u \diagdown r_1$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 3 | 3 |

二つの部分集合 $M_{4,inv}, M_{4,ninv}$ を

$$M_{4,inv} = \{1,3\},\ M_{4,ninv} = \{0,2\},$$

のように定義する. 其々の部分集合の二つの要素は, 其々0 と 1 を表す. Alice が行う符号化の仕方を説明する. まず, Alice が Bob と Charlie の両方に情報を送る場合を考える. Alice は, ランダムビット $r_1$ を選び, $r_2$ as $r_2 = r_1 \oplus b$ を計算する. その後, Alice は, 以下のように $s_1, s_2 \in M_{4,1}$ を選ぶ.

$$s_1 = \begin{cases} 1 & \text{if } r_1 = 0, \\ 3 & \text{if } r_1 = 1. \end{cases}$$

$$s_2 = \begin{cases} 1 & \text{if } r_2 = 0, \\ 3 & \text{if } r_2 = 1. \end{cases}$$

$u$ と $r_1$ が与えられたとき，表 1，表 2，表 3 は，$s_1$，$s_2$，$s_1 s_2 \bmod 4$ の値を表している．Bob は，$s_1$ と $s_1 s_2 \bmod 4$ を受信するので，$s_2$ を復元できる．なぜなら，$M_{4,inv}$ の任意の要素は，法 4 で乗法的逆元をもつ．それゆえ，Bob は，$u$ を知ることができる．同様に，Charlie も $u$ を知ることができる．

表 4：$s_1$

| $u$ ＼ $r_1$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 3 |
| 1 | 1 | 3 |

表 5：$s_2$

| $u$ ＼ $r_1$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 2 |
| 1 | 2 | 0 |

表 6：$s_1 s_2 \bmod 4$

| $u$ ＼ $r_1$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 2 |
| 1 | 2 | 0 |

次に，Alice が Bob だけに 1 ビットのデータ $b$ を送りたい場合を考えよう．Alice は，ランダムビット $r_1$ を選んだ後，$r_2$ as $r_2 = r_1 \oplus b$ を計算する．そして，Alice は，$s_1 \in M_{4,inv}$ と $s_2 \in M_{4,ninv}$ を以下のように選ぶ．

$$s_1 = \begin{cases} 1 & \text{if } r_1 = 0, \\ 3 & \text{if } r_1 = 1. \end{cases}$$

$$s_2 = \begin{cases} 0 & \text{if } r_2 = 0, \\ 2 & \text{if } r_2 = 1. \end{cases}$$

$u$ と $r_1$ が与えられたとき，表 4，表 5，表 6 は，$s_1$，$s_2$，$s_1 s_2 \bmod 4$ の値を示している．Bob は，$s_1$ と $s_1 s_2 \bmod 4$ を受信するので，$s_1$ の乗法的逆元を使って，$s_2$ を $s_2 = s_1^{-1}(s_1 s_2) \bmod 4$ のように計算することができる．よって，Bob は，$u = s_1 \oplus s_2$ を計算して，$u$ を得る．一方，Charlie は，$s_2$ と $s_1 s_2 \bmod 4$ を受信する．しかし，Charlie は，$s_2$ が乗法的逆元を持たないので，$s_1$ を一意に復号できない．つまり，Charlie は，$u$ を知ることができない．逆に，Charlie にだけ情報を送りたい場合にも同様の符号化で可能である．

この符号化は，モノイドの性質を利用した秘密分散法に基づいている．複数ビットの場合やネットワークの形状の一般化については，発表論文を参照してほしい．

（2）「ネットワーク的計算」のための符号化法

前節の network code は，一人の送信者が複数の送信者に同じデータを送信するための符号化である．ネットワーク的計算は，逆に，複数の送信者が異なるデータを送信し，一人の受信者は，それらのデータの関数値のみを受け取るための符号化である．Appuswamy らは，その関数とネットワークの形状から決まる伝送効率(演算効率に相当)の上限を導いた．本研究では，暗号方式の高速実装の一つであるビットスライス計算法とネットワーク的計算 の類似性に着目した．ここでは，関数としてハッシュ関数 TIB3 の非線形置換 S-box に着目し，これのビットスライス計算法の最適性を評価する．

表 7：TIB3 の S-box

| $(x_1, x_2, x_3)$ | 000 | 001 | 010 | 011 |
|---|---|---|---|---|
| $(y_1, y_2, y_3)$ | 110 | 100 | 001 | 111 |

| $(x_1, x_2, x_3)$ | 100 | 101 | 110 | 111 |
|---|---|---|---|---|
| $(y_1, y_2, y_3)$ | 000 | 011 | 101 | 010 |

TIB3 の S-box は，3 ビット入力 3 ビット出力の関数であり，表 7 で定義される．入力を $(x_1, x_2, x_3)$，出力を $(y_1, y_2, y_3)$ とおくと，表 7 は，下記の式で表される．

$$y_1 = \neg x_1 \oplus (x_2 \wedge \neg x_3)$$
$$y_2 = x_3 \oplus (\neg x_1 \wedge \neg x_2)$$
$$y_3 = x_2 \oplus (x_1 \wedge x_3)$$

上式が TIB3 の S-box のビットスライス計算法であり，出力の 1 ビットがビット毎の論理演算のみが計算できることがわかる．

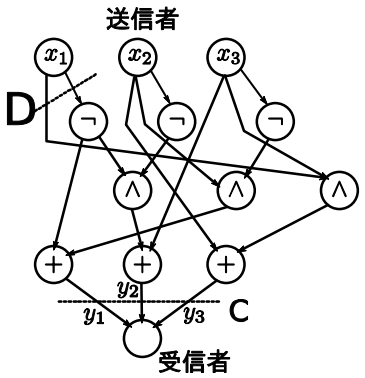


図 3：TIB3 の S-box のネットワーク

このビットスライス計算法をネットワーク的計算とみなすと，図3のような network code になっている．三人の送信者と一人の受信者である． 前節の図とは異なり，ノードが行う演算をノードの中に記している．このように表記することで， 演算回数とノードの数が一致するため，演算回数が視覚的にわかりやすくなる．

このネットワーク的計算の最適性を Appuswamy らの上限と比較すると， その上限に達していることがわかった． この意味で，このビットスライス計算法は，ネットワーク的計算として最適である． しかし，これは，ビットスライス計算法がビット毎の出力を計算 するため，図3中の cut C のような cut が必ず存在するので， 必然的な結果である．そこで，この cut を除いて，ネットワーク的計算として最適性を調べたところ， 図 3 中の cut D のところに冗長な部分があり，最適でないことが分かった． つまり，TIB3 の S-box のビットスライス計算法には冗長な部分があり， 計算回数を削減できる可能性があることを意味する．

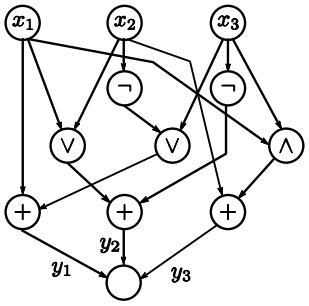


図4：TIB3 の S-box の改良ネットワーク

検討の結果，図4のようにすれば， cut D のところに冗長がなくなることが判明した．図4から逆にビットスライス計算法を導出すると， 下記の式になる．

$$y_1 = x_1 \oplus (\neg x_2 \vee x_3)$$
$$y_2 = \neg x_3 \oplus (x_1 \vee x_2)$$
$$y_3 = x_2 \oplus (x_1 \wedge x_3)$$

元のビットスライス計算法とこのビットスライス計算法が等価であることは， 入力可能なすべての3ビットの入力に対して同じ出力になることは， 実際に計算することで確かめることができる． このビットスライス計算法は，元のビットスライス計算法よりも 1回演算回数が減っているので(図中のノードの数が一つ減っている)． 演算効率が向上している．

発表論文では，最適性の検討過程や他の関数のビットスライス計算法の最適性について検討している．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）

① 桑門秀典，森井昌克，Improved Bitslice Network for Computing the TIB3 S-Box，電子情報通信学会 2010 総合大会講演論文集，査読無，2010，p.130.

② 桑門秀典，森井昌克，S-Box Bitslice Networks as Network Computing，電子情報通信学会技術研究報告，査読無，vol.109，2010，pp.35-38.

③ 桑門秀典，森井昌克，Multi-Bit Revocable Network Coding Scheme For Butterfly-Like Network ， 2008 International Symposium on Information Theory and its Applications，査読有，2008.

④ 桑門秀典，森井昌克，Conditions for Achieving a Revocable Network Coding Scheme，電子情報通信学会技術研究報告，査読無，vol.107，2008，pp.55-58.

〔学会発表〕（計１件）

① 桑門秀典， Indifferentiable Double-Block-Length Compression Function，2007 Hawaii and SITA Joint Conference on Information Theory，2007年5月31日，アメリカ合衆国 ハワイ州.

〔図書〕（計０件）
〔産業財産権〕
○出願状況（計０件）
○取得状況（計０件）
〔その他〕
なし

６．研究組織
(1)研究代表者
桑門 秀典 （KUWAKADO HIDENORI）
神戸大学・大学院工学研究科・准教授
研究者番号：30283914

(2)研究分担者
該当なし

(3)連携研究者
該当なし