様式 C-19

科学研究費補助金研究成果報告書

平成２１年 ３月３１日現在

研究種目：基盤研究（B）
研究期間：２００６年度 ～ ２００８年度
課題番号：１８３６０１７９
研究課題名（和文） マルチユーザ情報理論と暗号理論のネットワーク符号化への展開

研究課題名（英文） Studies towards the Network Coding Theory Based on Multi-user Information Theory and Cryptography

研究代表者
小林 欣吾（Kobayashi Kingo）
電気通信大学・電気通信学部・教授
研究者番号： ２００２９５１５

研究成果の概要：マルチユーザ情報理論と暗号理論の視点から，ネットワーク符号化におけるロバスト性とセキュア性の両立を意識して，線形ネットワーク符号の新しい構成法，ネットワーク誤り訂正符号の復号に関する基本概念の確立と,具体的復号アルゴリズムの提案,および,計算量の評価を行った。さらに，多重アクセス・ブロードキャスト・ネットワークに適するセキュリティ・プロトコル，安全なコンテンツ配信のための電子透かし法等の提案をした。

交付額

（金額単位：円）

	直接経費	間接経費	合 計
２００６年度	4,800,000	1,440,000	6,240,000
２００７年度	4,200,000	1,260,000	5,460,000
２００８年度	3,600,000	1,080,000	4,680,000
総 計	12,600,000	3,780,000	16,380,000

研究分野：工学
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：マルチユーザ情報理論，暗号・情報セキュリティ，ネットワーク符号化，ネットワーク・セキュリティ，安全性解析，電子透かし，ＬＤＰＣ符号，代数幾何符号

１．研究開始当初の背景

1970 年代から 80 年代にかけて衛星通信、深宇宙通信などの実現に深くかかわったマルチユーザ情報理論の理論的成果が、近年急速に発展してきたワイヤレス情報通信、インターネット環境においても適用可能であろうとの期待に裏打ちされて、世紀の変り目にネットワーク符号化という新しい概念が成立した。この概念は、ドイツ・ビーレフェルト大学 Ahlswede 教授らの先駆的な理論成果に基づいており、彼と協力関係にある香港中文大学 Yeung 教授らは線形ネットワーク符号化の研究を行っていた。ネットワーク符号化の生みの親であり，そのアイデアに至る基礎的理論のマルチユーザ情報理論の世界的権威である Ahlswede 教授は IEEE の Information Theory Society の 2008 年度の ShanNo.n 賞を受賞した。研究代表者の小林はビーレフェルト大学の彼が主宰したプロジェクトにも参加し Ahlswede 教授と共同研究も行って来ていた。Yeung 教授，ビーレフェルト大学 Cai 教授らによる，2003 年の線形ネットワーク符号化の論文は，小林も務める IEEE Information Theory Society の Award Committee において 2008 年度の Best Paper Award として採択された。

さらに、共同研究者である米国カリフォルニア大学サンジェゴ校の Wolf 教授、Siegel

教授，Zeger 教授を中心として熱心にネットワーク符号化の研究が推進される機運が高まっていた。2003 年ラトガー大学 DIMACS でネットワーク符号化のワークショップが開催され、情報理論、通信理論、計算機科学の世界的専門家が参加している。2006 年春には，全世界から優れた情報理論，通信理論、計算機科学の若手研究者が集結してきているカリフォルニア大学サンジェゴ校においては，Center of Information Theory and its App.lications という研究センターの開所にあわせて，第一回 ITA(Information Theory and App.lications) Workshop が開催され，全米ばかりでなく世界の一大拠点となろうとしていた。2007 年 9 月に Adelaide で開催された 2007 IEEE International Symposium on Information Theory では，ネットワーク符号化のセッションが多くの若手研究者を集めて熱気のある発表が行われている。このように，ネットワーク符号化の研究は世界的な注目を浴びて来ているただ中にあった。

当該研究は、このような時代的背景において、電通大のマルチユーザ情報理論、符号理論、情報圧縮理論，情報セキュリティの専門家が我が国および世界をリードすべくネットワーク符号化のさらなる展開を計ろうという意図のもとで計画された基盤研究である。

２．研究の目的

ワイヤレス通信環境とインターネットが有機的に結合した現代の情報通信網において、近年ネットワーク符号化が注目を浴びている。この技術的概念は多重アクセス通信路の容量域を決定したことでマルチユーザ情報理論の創始者の一人として知られるドイツ・ビーレフェルト大学の Ahlswede 教授を中心とするグループによって 2000 年に提唱され、それまでインターネットをとおしての情報伝送はパケットデータの複製をのみを中継ステーションで行うマルチキャストしか念頭になかったネットワーク技術者研究者に衝撃を与えた。それは情報理論的発想から自然と帰結される符号化を各中継ステーションにおいて行うことで、伝送費用、伝送時間の縮小を計れる可能性を示唆したことにある。以来、数年の間に初等的ではあるが興味ある研究が多数成立して来ている。しかし、通信路の通信路容量を十分考慮に入れていないとか、伝送データの同期をどのように成立させるべきか，アクティブネットワーク技術の開発など実ネットワークの運用に向けて解決されねばならない問題が山積している。ここにおいて、マルチユーザ情報理論、高速復号アルゴリズムの研究で豊富な経験を積んで来た我々が、ブロードキャスト、多重アクセス-ネットワーク符号化のための基礎応用研究に取り組むことにした。

相関をもつ情報源から生み出されるデータのネットワークを介してのデータ共有方式の例に、アプリケーションプログラム更新、連続する動画像のフレーム更新などがある。これまでのファイルのコピーによるマルチキャストより優れた符号化マルチキャストのアイデアを導入し、ネットワークの各中継ノードでも符号化を導入することにより従来よりも効率的な情報伝送が実現できる可能性がある。

また、これまでネットワーク上で安全に情報を取り扱う様々なセキュリティプロトコルが研究されており、電子現金など実際の用いられているプロトコルも多い。しかし、さらにネットワーク環境に高性能、高信頼性を持たせたセキュリティの管理を行うには、新らしい発想の導入が必須で、それをふまえたネットワーク符号化のための情報セキュリティ技術を確立し、安全性解析を行いネットワークセキュリティシステムの設計を実現する必要がある。

このために具体的には、
１）ネットワーク符号化マルチキャスト、それを発展させた
２）ネットワーク符号化ブロードキャスト、
３）ネットワーク符号化多重アクセス・ブロードキャスト
のシステム構築を目指す。さらに、この中継ノードでの符号化と情報分割送信を組み合わせて、秘密分散の理論を実装した
４）ネットワーク符号化セキュリティーシステムを実現すること
を目標とする。

３．研究の方法

この研究は、近年導入されたネットワーク符号化という斬新なアイデアをさらに深化、展開して実用的で先進的なネットワーク環境の実現を目指しているところに際立った特色があり、高性能、高信頼性を持たせるネットワーク符号化だけを目標においているのではなく、情報セキュリティ的な視点も組み込んだ研究を行おうとしている点に独創的な発想がある。３年間の研究によって、ネットワークを通しての１対１、１対多（マルチキャスト、ブロードキャスト)、多対１（多重アクセス）の情報伝送の高性能、高信頼性を導くばかりでなく、多対多の通信も含めてネットワーク符号化の総合的研究をとおして、情報セキュリティまで組み込んだネットワーク符号化システムの構築を目指した。また、マルチユーザ情報理論の深化、発展も期待されて、情報通信の基本的枠組みに関する学術的意義もすこぶる大きい。

そこでネットワーク符号化における諸問題を，（1）理論的解析，（2）符号化方式・アルゴリズムの開発、および（3）関連分野への展開、の３つに分類し体系的に捕らえて取り組んだ。

（1）理論的解析：マルチキャスト・ネットワーク符号化の理論的な諸評価として、初年度はマルチキャストの研究に重点的をおき、１つの情報源からのデータをそれを要求する多利用者へマルチキャストする状況で，線形スカラー・ネットワーク符号化・線形ベクトル・ネットワーク符号化それぞれの適用できるネットワークの構造の特徴付けを行った。さらに、通信路容量制限が付加されている状況下のネットワーク符号化はどうあるべきかを検討した。 またマルチキャストからブロードキャストへの発展研究も計画した。

（2）符号化方式・アルゴリズムの開発：マルチキャストの状況にあるネットワークの終端ノードばかりでなく、各中間ノードにおいても、入力される複数の入力データを同時に復号し、それらをまた所望の目的にしたがって符号化しなければならない。そのための、高速の同時復号について研究した。

（3）関連分野への展開に関する研究：マルチキャスト・セキュリティネットワークの構成として，マルチキャストの状況にあるネットワークの各ノードに入力される複数の入力データを同時に符号化し、さらに、秘密分散の理論を適用した情報分割を組み合わせてセキュリティネットワークを構成した。

符号理論への通信路ネットワーク符号化研究からのフィードバックとして，ネットワーク符号化環境に適する通信路符号化方式、復号方式の研究から生み出される成果を、符号理論の新しい展開に結びつけることのできる可能性について検討している。

これら（1）理論的解析，（2）符号化方式・アルゴリズムの開発、および（3）関連分野への展開について、ネットワークの構造を

① ネットワーク符号の一般化
② マルチキャストからブロードキャストへ
③ 多重アクセス・ネットワーク符号化
④ 多重アクセス・ブロードキャスト・ネットワーク符号化
⑤ ネットワーク符号化の展開研究
⑥ 無線環境における多重アクセス・ネットワーク符号化
⑦ ネットワーク・セキュリティブロードキャスト

のように、多様なものを対象として取り組んだ。

４．研究成果

（1）１８年度（初年度）は、ネットワーク符号化問題におけるロバスト性とセキュア性の研究を中心として行った。マルチキャスト・ネットワーク通信において、ネットワーク中の複数のリンク上で観測するとき、観測データから情報を陽に復元可能とするロバスト性と，陽には復元できないセキュア性という相反する２種類の性質を同時に兼ね備える符号化の概念と条件を与え、その理論的性質を明示した。

また、ネットワーク符号の応用として、符号化を用いたファイル共有(P2P)システムについての計算機上のシミュレーション実験と理論的解析を行った。BitTorrent にネットワーク符号化を導入した Avalanche と呼ばれる手法を検証し、符号化を組織的に行う方法とランダムに行う方法を提案し、いずれも BitTorrent より優位であることを確認した。

さらに，ネットワーク符号化に関連するセキュアな暗号・セキュリティプロトコル、コンテンツ配信の電子透かしプロトコルの研究を行った。また、誤り・障害に対する信頼性の向上のため，代数的符号の高速高信頼の復号アルゴリズム、ＬＤＰＣ符号、ターボ符号などの構成、復号アルゴリズムの検討を行っている。

（2）１９年度（次年度）は、線型ネットワーク符号化(Linear Network Coding(LNC))に関する新しい構成法と多重アクセス・ブロードキャスト・ネットワークにおけるセキュリティに関する諸問題の研究を中心に行なった。前者に関しては、マルチキャスト LNC，ブロードキャスト LNC、ロバスト LNC の新しい構成法を提案した。最大 LNC という符号を用いたこの方法は、最大 LNC とマルチキャスト、ブロードキャスト、ロバストのそれぞれを目的とした符号化行列を組み合わせることで、最大 LNC からそれぞれの目的に合った LNC を構成することが可能で あるという特徴を持っている。

また、ソースノードのみに符号化行列を適用すればよいので、準備された最大 LNC により設定されたネットワーク内の中継ノードでの符号化関数を一切変更する必要がないという実用的に優れた特徴を持っている。後者の多重アクセス・ブロードキャスト・ネットワークにおけるセキュリティ 問題の解決のために、Multisignatures 方式、プライバシーを強化した電子現金方式、公開鍵暗号アルゴリズムの安全性解析、ネットワーク上で

のより安全なカギ交換方式等に関する研究を進めた。
　さらに、ネットワーク上での著作権保護に関する課題として、静止画、音声、動画等の実際のコンテンツに対する電子透かし方式の検討を行った。マルチキャスト・ネットワークの実現の観点から、ユーザ ID を埋め込む電子透かし方式である電子指紋について、より実用的な方式の検討を行っている。その中では結託耐性符号と埋め込み方式の一体化により実用的なビ ット数の電子指紋方式の実現などの提案を行った。

（3）２０年度（最終年度）は、ネットワーク符号化における諸問題について以下の通り研究を展開した。

①　ネットワーク符号化の展開研究：本年度の研究テーマの一つであるネットワーク符号化の発展研究として、ネットワーク誤り訂正符号の復号に関する基本概念と具体的な復号アルゴリズムおよび計算量の評価などの研究を行なった。従来提案 されている復号法は、exhaustive search(しらみつぶし法)(あるいは enumeration method(列挙法))に対応する方法しかなかった。我々は、従来の符号理論における検査行列の概念をネットワーク誤り訂正符号にも拡張し、シンドロームを用いた効率的な復号法 を提案した。特に、単一誤りに関しては、ネットワークのリンク総数に線形なオーダーで復号できる性能をもつことを示した。

②　無線環境における多重アクセス・ネットワーク符号化
有限状態通信路における理論的限界について新しい知見を得た。記録メデイアを具体的な対象とした有限状態マルコフ通信路の通信容量の解析をした。また無線環境における多重アクセス・ネットワーク符号化に適する誤り訂正符号の基礎的な符号化方法の検討として非２元ＬＤＰＣ符号の新たな解析方法、符号設計復号アルゴリズムの提案を行っている。

③　ネットワーク・セキュリティ
ネットワーク環境における暗号情報セキュリティプロトコルの諸問題の研究を遂行した。とくに、Task-Structured PIOA フレームワークにおける安全性解析、パスワードベースの鍵交換などを中心として研究を進めた。ネットワーク利用の諸問題への取り組みとして、様々なメデイアに適する電子透かし埋め込み方式、電子指紋の問題を扱った。秘密分散法 を利用した電子透かし方式の基礎的な検討を行ったが、これは現在検討されている ネットワーク符号化と親和性の高い方式となっている。

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　63 件）

① Brian Kurkoski, Justin Dauwels and Hans-Andrea Loeliger, ″Power-Constrained Communications Using LDLC Lattices,″ in Proc. of the Intl. Symposium on Information Theory, 5 pages, June (2009), 査読有
② Takashi Nishide, Kazuki Yoneyama, Kazuo Ohta, ″Attribute-Based Encryption with Partially Hidden Ciphertext Policies″ IEICE Trans, on Fundamentals, Vol.E92, A, No.1, pp.22-32, Jan, (2009), 査読有
③ Bagus Santoso and Kazuo Ohta, ″A New 'On the Fly' Identification Scheme: A Trade-off of Asymptoticity between ZK and Correctness,″ IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A, No.1, pp.122-136, (2009), 査読有
④ Lopez-Hernandez, Julio, Martinez-No.riega, Raul, Nakano-Miyatake, Mariko, Yamaguchi, Kazuhiko: ″DetectioNo.f BPCS-StegaNo.graphy Using SMWCF Steganalysis and SVM,″ Society on Information Theory and its App.lications, 2008 International Symposium on Information Theory and its Applications (ISITA2008), No.157,(2008), 査読有
⑤ Yu Sasaki, Lei Wang, Kazuo Ohta and No.boru Kunihiro, ″Extended Password Recovery Attacks against APOP, SIP, and Digest Authenticaiton,″ IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A, No.1, pp.96-104, (2009) 査読有
⑥ Brian M. Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ″No.ise Thresholds for Discrete LDPC Decoding Mappings,″ in Proc. of IEEE Global Communications Conf, (GLOBECOM 2008), pp.1-5, December (2008), 査読有
⑦ 米山一樹，國分雄一，太田和夫，″Task-Structured PIOA フレームワークを用いた適応的攻撃者に対する Diffie-Hellman 鍵交換の安全性解析″

電子情報通信学会論文誌 D 分冊 Vol.,J91-D, No.4, pp.859-872, Apr. (2008) 査読有

⑧ 阪田省二郎,代数的符号理論,IEICE Fundamentals Review,Vol.,1, No.3,44-57, (2008), 査読有

⑨ Hyunho Kang, Koutarou Yamaguchi, Brian Kurkoski, Kazuhiko Yamaguchi, and Kingo Kobayashi, "Full-Index-Embedding Patchwork Algorithm for Audio Watermarking", IEICE Trans, Inf, & Syst,, Vol.ume and Number: Vol., E91-D, No.11, pp. 2731-2734, Nov, (2008), 査読有

⑩ Youngran Park, Hyunho Kang, Kazuhiko Yamaguchi, Kingo Kobayashi, "Watermarking for Tamper Detection and Recovery," IEICE Electron, Express, Vol.,5, No.,17, pp.,689-696, (2008), 査読有

⑪ Bagus SANTOSO No.boru KUNIHIRO Naoki KANAYAMA Kazuo OHTA, "FactorizatioNo.f Square-Free Integers with High Bits KNo.wn," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E91-A, No.1, pp. 306-315, (2008), 査読有

⑫ Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi and Kingo Kobayashi, "Tracing illegal users of video: reconsideration of tree-specific and endbuyer-specific methods", Lecture notes in Computer Science, Springer-Verlag, Vol.4707, Part III, pp.1046-1055, (2007), 査読有

⑬ T. Nishide and K. Ohta, "Constant-Round Multiparty Computation for Interval Test, Equality Test, and Comparison," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol., E90-A, No.,5, pp., 960-968, (2007), 査読有

⑭ M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro and K. Ohta, "Visual Secret Sharing Schemes for Multiple Secret Images Allowing the Rotationof Shares," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E89-A, No.5, pp. 1382-1395 (2006) 査読有

〔学会発表〕(計 138 件)

① K. Kobayashi,Capacity Problem of Finite State Channels,Invited Lecture at Xidian University,March 9, 2009, Xian, China

② K. Kobayashi, An overview of Multi-User Information Theory, Invited Lecture at Xidian University, March 13, 2009, Xian, China

③ K. Kobayashi, Considerations on the capacity problem of finite state channels, 2009 Information Theory and Applications Workshop, Feb. 9, 2009, San Diego, USA

④ 小林欣吾,［特別講演］いくつかの有限状態通信路の通信路容量について,電子情報通信学会情報理論研究会,2008 年 10 月 7 日,鬼怒川温泉 あさやホテル (栃木県日光市)

⑤ 栗原正純,［ネットワークコーディングにおける誤り訂正符号の復号法についての一検討,情報理論とその応用学会 2008 情報理論とその応用シンポジウム, No.4.1.5, 2008 年 10 月 8 日,鬼怒川温泉 あさやホテル (栃木県日光市)

⑥ 阪田省二郎,［招待講演］代数的符号理論：夢と現実,電子情報通信学会情報理論研究会,IT2006-49, pp.25--32, 2006 年 11 月 28 日,花びしホテル (北海道函館市)

〔図書〕(計５件)

① (Eds.) M, Sala, T, Mora, L, Perret, S. Sakata, C. Traverso, "Groebner Bases," Coding, and Cryptography, Springer Verlag,1-425,(2009)

② 小林欣吾,情報理論講義,培風館 pp.1-186, (2008)

③ 太田和夫,計算理論の基礎 (原著第２版) １オートマトンと言語, ２計算可能性の理論, ３複雑さの理論, 共立出版,合計 507 頁, (2008)

④ 阪田省二郎, 数学書房, 日比孝之 (編) 「グレブナー基底の現在」第 6 章: 符号・配列・グレブナー基底, 25 頁 (全体 245 頁中), (2006)

⑤ 小林欣吾, 岩波数学辞典第４版 "情報理論",岩波書店, 43 頁, (2006)

〔産業財産権〕
○出願状況 (計２件)

① 名称：データ格納システム及び情報送信装置及びサーバ装置

発明者：伊藤隆(三菱電機㈱),北原恵介,坂井祐介,太田和夫
権利者：国立大学法人電気通信大学, 三菱電機株式会社
種類：特許権,特願 2009-008609
番号：特願 2009-008609
出願年月日：2009/01/19
国内外の別：国内

② 名称：本人確認システム
発明者：Bagus Santoso, 崎山一男, 太田和夫
権利者：国立大学法人電気通信大学
種類：特許権,特願 2009-008609
番号：特願 2008-289266
出願年月日：2008/11/11
国内外の別：国内

６．研究組織

(1)研究代表者

小林　欣吾 (Kobayashi Kingo)
電気通信大学・電気通信学部・教授
研究者番号：20029515

(2)研究分担者

阪田　省二郎 (Sakata Shojiro)
電気通信大学・名誉教授
研究者番号：20064157

太田　和夫 (Ohta Kazuo)
電気通信大学・電気通信学部・教授
研究者番号：60220258

山口　和彦 (Yamaguchi Kazuhiko)
電気通信大学・電気通信学部・准教授
研究者番号：60220258

Brian Kurkoski (Brian Kurkoski)
電気通信大学・電気通信学部・准教授
研究者番号：80444123

栗原　正純 (Masazumi Kurihara)
電気通信大学・電気通信学部・助教
研究者番号：90242346

(3)連携研究者