様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２５　日現在

機関番号：　１２６１２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６４２０３４５

研究課題名（和文）情報理論的安全性をもつマルチキャスト通信の構築とその安全性解析

研究課題名（英文）Construction and Analysis of Information Theoretically Secure Multicast Communication

研究代表者

岩本　貢（Iwamoto, Mitsugu）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：５０３７７０１６

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：放送型暗号(BE)とセキュアネットワーク符号化(SNC)を融合する方法について検討し，(t,d)-組み合わせネットワーク（ソースノードがt個の中間ノードに接続され，　n人の受信者それぞれが，d個の中間ノードと接続されているネットワーク）に対しては非常に効率よく暗号化が実現できることを示した．具体的例として(≦100，≦3)-BEを考えると，これを従来の最適な放送型暗号で実現する場合，5GBのデータを送るために約834TBの暗号化鍵，809TBの復号鍵が必要であった．(5,3)組み合わせネットワークに対して符号化を行うと，暗号化鍵2.6TB，復号鍵75GBでBEが実現できる．

研究成果の概要（英文）：We discussed how to unify broadcast encryption (BE) and secure network coding (SNC), and clarified that it is possible when the network is (t,d)-combinatorial network where a source node is connected to t intermediate nodes, and each sink node is connected to t intermediate nodes.　Furthermore, the proposed scheme is highly practical compared to the original BE. For instance, 834TB and 809TB are necessary for encryption and decryption keys, respectively, to implement (≦100, ≦3)-BE by traditional method. On the other hand, in the case of (5,3)-combinatorial network, 2.6TB and 75GB are enough for encryption and decryption keys, respectively, by the proposed scheme. Key lengths of proposed scheme are not short, but are more practical compared to the traditional BE.

研究分野：　暗号理論

キーワード：　放送型暗号　セキュアネットワーク符号化　秘密分散法　情報理論的安全性

１．研究開始当初の背景

暗号技術は現代のネットワーク社会における重要な基盤技術である．安定期を迎えたインターネット社会においては，長期的な視点に基づくセキュリティ技術の運用が求められるようになっている．例えば，個人情報のような半永久的に秘匿したいデータの暗号通信や，大規模な基盤インフラといった長期間更新せずに運用したい情報システムに対する安全性の重要度が今後より高まると予想される．

しかし，現在の暗号技術の多くは計算量的安全性と呼ばれる安全性概念に基づいて設計されており，計算機の性能向上や暗号解読アルゴリズムの高速化，量子計算機の実現などによって危殆化するおそれがある．一方で，攻撃者の攻撃能力を一切制限せずに長期間安全性を保証できる技術として，情報理論的に安全な暗号技術（情報理論的暗号）がある．本研究では，ネットワーク通信に対応した情報理論的暗号方式の構築と理論解析を課題とした．ネットワーク上で利用する情報理論的に安全な暗号通信の研究は，暗号理論・情報理論の両分野で積極的に行われている．有名なものとして，暗号理論の分野では放送型暗号方式(Broadcast Encryption, BE)が，情報理論の分野ではセキュアネットワーク符号化(Secure Network Coding, SNC)が知られている．共に，マルチキャスト通信（単一の情報を複数のユーザに配信する）を行う点では共通している．一方で，BE では各ユーザが秘密鍵を所持し，サーバの送信する同報メッセージ（暗号文）によって，一部のユーザグループが送信メッセージ（平文）を得られる一方で，グループに属さない人には平文に関する情報が得られないようになっている．SNC は，ネットワーク符号化(NC)にセキュリティの機能を付加したもので，ネットワークのルータ（ノード）で演算を行うことを許し，効率と安全性を両立して複数のユーザにマルチキャスト送信を実現するものである．

共通点の多い BE と SNC であるが，大きな相違点もある．まず，BE は（ネットワーク網をモデル化せず）放送型の通信を用いて，平文を送信したいユーザ集合を暗号化器によって制御する．SNC はネットワーク網をグラフでモデル化し，各ノードに演算機構をもたせることで，ユーザ全員に効率よく情報を送信することに注力している．BE での暗号化器をノードとみれば，ネットワーク網の利用方法の観点からは SNC の方が一般的である．また，BE では通常，通信の前に送信者とユーザが鍵を共有する必要があるが，SNC は各ノードで計算（符号化）が可能であることを利用し，各ユーザが送信者と事前に鍵共有をすることなく暗号化通信が出来るという意味で，SNC は BE より優れている．しかし，例えば，放送コンテンツなどのオンデマンド配信を考えれば，受信者グループが制御できるという意味で，BE の方が高機能である．

２．研究の目的

本研究の目的は，BE と SNC を統合することを目指した．より具体的には，

(A) BE と SNC の長所を継承したネットワーク向けのマルチキャスト通信を提案し，
(B) 情報理論と暗号理論，双方の最新の理論を駆使してその性能を評価する

ことが研究の目的である．

大まかにいうと，BE は使い捨て暗号に鍵配事前送方式(KPS)を組み合わせた方式であり KPS は多項式ベースの暗号であると見なせること，および，SNC は秘密情報を符号化して分散送信すると見なせることに注意すると，両者は秘密分散法と呼ばれる暗号技術と関連が強い．そこで，秘密分散法の技術を活用して，両者のモデルと構成法を融合することは（全く考えられていないにも関わらず）技術的に比較的自然なものであると予想した．

３．研究の方法

研究を進める上で，BE と SNC の融合は，理論としての親和性の高さは予想できたものの，前者は対称多項式やデザイン理論，後者はネットワークの理論やシャノン理論，符号理論などに立脚しており，単純に融合できないことが徐々に明らかになってきた．

そこで，ネットワーク符号化の特徴であるノード上での演算を行わない，秘密分散型ネットワーク（組合わせネットワーク）の場合に特化し，具体例を構築していくことで，ネットワークを介して BE を実現することを目指した．(t,d)-組み合わせネットワークとは，ソースノードから t 個の中間ノードにノイズのない通信路で接続され，n 人の受信者それぞれが，それぞれ d 個の中間ノードと接続されているようなネットワークであり，ノード上での演算が行われない反面，符号化の方法が単純になる．

このようなネットワーク上では，（セキュアとは限らない）ネットワーク符号化で符号化したメッセージに対して BE の技術を適用することで，BE の鍵長や暗号文長が長くなる問題点を大幅に改善できることが分かった．

４．研究成果

「研究の方法」で述べた，組合せネットワークを用いて放送型暗号が実現できるかを議論し，この方針に基づくと BE と SNC の利点をうまく組み合わせることが出来ることを明らかにした．その結果，既存の放送型暗号の鍵長を大きく削減する放送型暗号が構成できることを示した．

具体的に例えば，100 人以下の任意のグループに対して鍵が配送でき，3 人以下の結託に対して安全な放送型暗号((≦100，≦3)-one time secure 放送型暗号)を考える．これを従来の最適な放送型暗号で実現する場合，5GB のデータを送るために約 834TB の暗号化鍵，809TB の復号鍵が必要であったが，(5,3)型組み合わせネットワーク（ソースが 5 個の中間ノードにノイズのない通信路で接続され，各ユーザがそれぞれ 3 つの中間ノードと接続されているネットワーク）に対して符号化を行うと，暗号化鍵 2.6TB，復号鍵 75GB で放送型暗号が実現できることを示した．このように，単一の放送型通信路を用いるより，ネットワークの特性を活かすことで情報理論的安全性を達成しつつ，比較的現実的な鍵サイズで放送型暗号が実現できることが明らかに出来た．この意味で，当初の研究計画は概ね達成できたといえる．特に，従来（最適な構成法であっても）非現実的だと思われていた放送型暗号が組み合わせネットワークを用いることで現実的なレベルで構成できることを明らかにしたことは，理論面だけでなく，実用的な側面からも大きな意味があると考えている．

また，ネットワーク符号化の技術を直接的に用いることで，(3,2)-組み合わせネットワーク上で BE を実現する例も構築したが，一般化には成功しておらず，今後の課題となっている．組み合わせネットワーク以外の一般的なネットワークに対する一般化や提案手法の最適性証明など，今後の課題も存在するため，今後も研究を進める予定である．

最後に，本研究に関連して，秘密分散法やマルチパーティ計算に関する成果も幾つか得られた．

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１件）

1. T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K. Ohta, “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,” CANS2016, LNCS 10052, pp. 350–364, 2016. 査読有

〔学会発表〕（計 19 件）

1. 岩本貢, 渡邉 洋平 “秘密分散型放送暗号,” 暗号と情報セキュリティシンポジウム (SCIS2017), 4F2-2, ロワジールホテル那覇（沖縄県那覇市）, 2017 年 1 月 27 日.
2. 岩本貢, “マルチパーティ計算に関する安全性概念の定式化について,” 暗号と情報セキュリティシンポジウム (SCIS2017), 2D4-3, ロワジールホテル那覇（沖縄県那覇市）, 2017 年 1 月 25 日.
3. A. Espejel-Trujillo, M. Iwamoto, “Steganalysis of Bit Replacement Steganography for a Proactive Secret Image Sharing,” 暗号と情報セキュリティシンポジウム (SCIS2017), 1A1-6, ロワジールホテル那覇（沖縄県那覇市）2017 年 1 月 24 日
4. T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K. Ohta, “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,” CANS2016, LNCS 10052, pp. 350-364, Milan (Italy), 15th November, 2016.
5. Y. Kamoshida, M. Iwamoto, and K. Ohta, “Application of Joux-Lucks Search Algorithm for Multi -Collisions to MicroMint,” IWSEC2016 (poster session), お茶の水ソラシティ（東京都千代田区）2016 年 9 月 12 日.
6. A. E. Trujillo and M. Iwamoto “Proactive Secret Image Sharing with Quality and Payload Trade-off in Stego-images,” 暗号と情報セキュリティシンポジウム (SCIS2016), 3A1-2, ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）, 2016 年 1 月 21 日.
7. 鴨志田優一, 岩本貢, 太田和夫, “Joux-Lucks のマルチコリジョン探索アルゴリズムの MicroMint へ の応用,” 暗号と情報セキュリティシンポジウム (SCIS2016), 3D1-3, ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）, 2016 年 1 月 21 日.
8. 三澤 裕人, 徳重 佑樹, 岩本貢, 太田 和夫, “人間向け暗号/認証プロトコルの統一的安全性評価,” 暗 号と情報セキュリティシンポジウム (SCIS2016), 3E3-5, ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）, 2016 年 1 月 21 日.
9. 中井雄士, 三澤裕人, 徳重佑樹, 岩本貢, 太田和夫, “カード操作の分類とカードベース暗号プロトコ ル,” 暗号と情報セキュリティシンポジウム (SCIS2016), 4A2-2, ANA クラウンプラザホテル熊本ニュースカイ（熊本県熊本市）, 2016 年 1 月 21 日.
10. 三澤 裕人, 徳重 佑樹, 岩本貢, 太田 和夫, “ブロックサインの安全性に対するコードブックの影響,” コンピューターセキュリティシンポジウム, 3C2-2, pp. 1011-1018, 長崎ブリックホール（長崎県長崎市）23rd, Oct., 2015.
11. Y. Misawa, Y. Tokushige, M. Iwamoto and K. Ohta, “Comparison of Security on Coded Signs with Public/Private

Code Book，” International Workshop on Information Security (IWSEC2015), (poster session), 東大寺文化センター（奈良県奈良市）26th August, 2015.

12. T. Nakai, Y. Tokushige, M. Iwamoto and K. Ohta, “Toward Reducing Shuffling in Card-based Cryptographic Protocol for Millionaire Problem,” International Workshop on Information Security (IWSEC2015), (poster session), 東大寺文化センター（奈良県奈良市）26th August, 2015.
13. M. Iwamoto and J. Shikata, “Construction of symmetric-key encryption with guessing secrecy,” IEEE International Symposium on Information Theory (ISIT2015), Hong Kong Convention and Exhibition Centre, Hong Kong (China), 15th, June, pp.725-729, 2015.
14. P. Lumyong, M. Iwamoto, and K. Ohta, “Cheating on a Visual Secret Sharing Scheme under a Realistic Scenario,” International Symposium on Information Theory and Its Applications (ISITA2014), pp. 546-550, Melbourne Convention Center, Melbourne (Australia), Oct. 29th, 2014.
15. M. Iwamoto and J. Shikata, “Secret Sharing Schemes Based on Min-entropies,” IEEE International Symposium on Information Theory (ISIT2014), pp.401-405, Hawaii Convention Center, Hwaii (USA), 1st, July, 2014.
16. K. Ohara, Y. Sakai, F. Yoshida, M. Iwamoto, and K. Ohta, “Privacy -Preserving Smart Metering with Verifiability for Both Billing and Energy Management,” The 2nd ACM ASIA Public-Key Cryptography Workshop (ASIAPKC2014)，pp. 23-32, 京都ガーデンパレス（京都府上京区）2014 年 6 月 3 日.
17. 岩本貢，四方順司，“推測成功確率に基づいた安全性基準をみたす秘密分散法，” 暗号と情報セキュリ ティシンポジウム（SCIS2015），2D1-4，リーガロイヤル小倉（福岡県北九州市），2015 年 1 月 21 日.
18. 岩本貢，四方 順司，“推測確率に基づいた安全性基準をみたす暗号化方式の構成法，” 暗号と情報セキュ リティシンポジウム（SCIS2015），2D1-5，リーガロイヤル小倉（福岡県北九州市），2015 年 1 月 21 日.
19. 岩本貢，“秘密分散法と視覚復号型秘密分散法 – 共通点と相違点，”電子情報通信学会マルチメディア情報ハイディング・エンリッチメント研究会(招待講演)，EMM2014-7，pp.35-40，東京理科大学葛飾キャンパス（東京都葛飾区），2014 年 5 月 16 日.

〔その他〕
ホームページ等
http://ohta-lab.jp/
http://ohta-lab.jp/member/mitsugu/
http://ohta-lab.jp/users/mitsugu/
http://ohta-lab.jp/member/ohta/

６．研究組織
(1)研究代表者

岩本　貢（Mitsugu Iwamoto）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：５０３７７０１６

(2)研究分担者

太田 和夫（Mazuo Ohta）
電気通信大学・大学院情報理工学研究科・教授
研究者番号：８０３３３４９１