様式Ｃ－１９

# 科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年５月１５日現在

機関番号：３４５０４
研究種目： 若手研究（B）
研究期間： 2009～2011
課題番号： 21760300
研究課題名（和文） 雑音通信路を利用した情報理論的に安全な暗号プロトコルの実現

研究課題名（英文） Unconditionally secure cryptographic protocols from noisy channels

研究代表者
井坂 元彦 （ ISAKA MOTOHIKO ）
関西学院大学・理工学部・准教授
研究者番号： 50351739

研究成果の概要（和文）：
多人数の間で安全に計算を行う上で，紛失通信と呼ばれる暗号プロトコルが有用となる．本研究課題では，不正者が無限の計算能力を有する場合でも安全である紛失通信を対象としている．特にアナログ値を出力する連続的な雑音通信路の存在を仮定することで紛失通信を実現することを目的とし，紛失通信を構成する 2 者が行うべき通信と計算に関して提案と評価を行った．さらにそこで用いられる符号化法に関しても検討した．

研究成果の概要（英文）：
A cryptographic protocol called oblivious transfer is a powerful tool in secure multiparty computation. In this research project, we studied unconditionally secure oblivious transfer whose secrecy is guaranteed even when a malicious player has unlimited computational power. We designed a procedure between two parties for realizing oblivious transfer by assuming the existence of continuous noisy channels. An efficient coding scheme to be used in this scenario is also proposed.

交付決定額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 2009 年度 | 1,300,000 | 390,000 | 1,690,000 |
| 2010 年度 | 1,200,000 | 360,000 | 1,560,000 |
| 2011 年度 | 900,000 | 270,000 | 1,170,000 |
| 年度 | | | |
| 年度 | | | |
| 総　計 | 3,400,000 | 1,020,000 | 4,420,000 |

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： 情報理論，安全性，暗号プリミティブ

## １．研究開始当初の背景

現在用いられている暗号方式は，攻撃者の計算能力に関する何らかの仮定を安全性の根拠としている．しかし，計算量に関する仮定に対して数学的証明は一般に与えられておらず，その安全性が長期的に保証されるとは限らない．そこで，攻撃者が無限の計算能力を有する場合でも安全であるような情報理論的な安全性に関する研究が盛んになっている．

ディジタル通信において通常，通信路上の雑音は通信品質を劣化させる要因として扱われるが，その一方で雑音を利用することで情報理論的な安全性を実現しえることが知られている．この話題は理論的に興味深い問

題であるばかりでなく，通常の通信環境を利用した簡易な装置の下でセキュリティを確保できることから，実用的な観点からも意義が大きい．

特に本研究開始当初には，紛失通信と呼ばれる暗号プロトコルの安全性を情報理論的な観点から達成する研究が見られるようになっていた．紛失通信とは，複数人の間で安全に関数を評価するマルチパーティ計算において重要となる 2 者間のプロトコルである．

## ２．研究の目的

ネットワーク上で第三者を介さずに信任投票や電子選挙を行う場合，各自の入力（投票内容）に関する情報がお互いに対して漏れないこと，さらに関数の評価（集計）が正しく行なわれることが必須の要件となる．このように不正者が含まれうる多人数の間で，安全に所望の関数を評価する一般的な枠組みは安全なマルチパーティ計算と呼ばれる．安全なマルチパーティ計算を実現する上で，2 者のプレイヤーの間で行われる紛失通信と呼ばれる暗号プロトコルが普遍的に有用であることが示されている．したがって効率的な紛失通信を構成することは理論的にも応用面でも極めて重要な課題となっている．

情報理論的に安全な紛失通信は，離散無記憶通信路を前提とすることで実現が可能であることが示されており，安全性を担保するための通信路に関する必要十分条件が明らかにされていた．しかし，移動通信などの通信環境で見られるアナログ的な出力を有する連続的通信路に対しては，暗号プロトコルの立場からの研究は必ずしも十分に行われていない．

以上を背景として，本研究では実用的な環境において暗号プロトコルを構築することを狙いとして，以下の課題に関して検討を行う：

- 連続的通信路において，情報理論的に安全な紛失通信を実現するための信号設計とその情報理論的効率の評価を行う
- プレイヤーが行うべき計算と通信の手順を明らかにし，そこで用いられる符号化方式の高度化を図る

これらの検討を通して，雑音通信路の暗号学的な意味での可能性を開拓することを本研究の目的とする．

## ３．研究の方法

紛失通信は送信者と受信者の 2 者により行われる暗号プロトコルであり，概ね以下の要件を満たす場合に安全であると言われる：

- 送信者は 2 個の系列を保有する
- 受信者はそのうちいずれか一方のみを選択し入手する．
- 受信者は他方の系列に関する情報をほとんど得られない
- 送信者はいずれの系列が受信者により選択されたか知ることができない

雑音通信路を利用して安全な紛失通信を実現する上で検討すべき課題とその方法を以下に示す．

### (1) 通信路入力アルファベットの設計

紛失通信を実現する過程では，まず送信者から受信者へ雑音通信路を通して信号の送信を行うことで，ランダムネスの共有が行われる．このとき，送信者が雑音通信路に送信する信号の設計を行うことが課題となる．設計基準としては，紛失通信の安全性が保証されること，および受信者が選択して得る系列の情報量が多いことが挙げられる．

本研究において主たる検討対象となる連続的通信路に対しては，ディジタル変調および符号理論の分野において符号化変調と呼ばれる多くの手法が検討されている．そこで得られている知見を暗号プロトコル構築の観点から検討することで，紛失通信の実現に適した通信路入力アルファベットを設計する．

なお，ディジタル通信において基本的な加法的白色ガウス雑音通信路に対してまず基礎的検討を行い，その後任意の無記憶連続通信路に対して拡張する．

### (2) 相関情報源に対する符号化

雑音通信路の使用により，送信者と受信者の間で等価的に相関情報源が共有される．しかし，送信者が有する系列が正しく受信者へ伝達されるためには，信頼性を確保するための適切な符号化を施す必要がある．本研究では，現実的な計算量で性能に優れた復号が可能な線形符号を用いることで，広範な情報源アルファベットに対して適用可能な符号化法の提案を行う．符号化の高度化を実現することは，紛失通信の情報理論的な効率の向上につながるものである．

## ４．研究成果

本研究における成果を以下に示す.

### (1) 加法的白色ガウス雑音通信路に基づく紛失通信の実現

2 者のプレイヤーの間に加法的白色ガウス雑音通信路が存在する仮定の下で紛失通信を実現するプロトコルに関して検討を行った．紛失通信において要求される安全性を満足するための通信路入力アルファベットに関する十分条件を与え，雑音通信路に対して送信されるべき信号の設計とプレイヤーが行うべき計算と通信の手順を提案した．特に通信路入力アルファベットが幾何学的一様性と呼ばれる性質を有すると，プレイヤーが行う操作が簡素化されることを示した．さらに，与えられたアルファベットに対して，最適な情報速度を達成する手法を明らかにした.

以上で提案した手順に基づく紛失通信の情報理論的な意味での効率に関する評価を行った．さらに，信号点集合の非対称性がもたらすプロトコルの効率への影響，通信路入力アルファベットの次元と伝達情報量の関係などに関する結果を与えており，紛失通信の実現にあたって送信されるべき信号に関して多面的に検討を行った.

これらの成果は，5. 発表論文に示すもののうち主に[雑誌論文]⑤および⑥，[学会発表]⑤にて公表している.

### (2) 一般の連続的通信路に基づく紛失通信の実現

研究成果(1)で検討した内容をより一般的な連続的通信路に拡張し，プレイヤーが行うべき処理と実現された紛失通信の情報理論的効率について検討した．特に陸上移動通信において，送信された信号はフェージングと呼ばれる現象の影響を受けるため，加法的白色ガウス雑音通信路に対する手順を直接的に適用することでは安全性が保証されない．このため，一般的な無記憶連続的通信路において用い得る通信路入力アルファベットを提案した.

これらの成果は 5. 発表論文に示すもののうち[学会発表]②，また関連した内容を[雑誌論文]②にて公表している.

### (3) 相関のある情報源に対する符号化

紛失通信を実現する手順において，雑音通信路の入出力を基にして送信者と受信者が共通系列を生成する必要がある．このために行われる両者の間の対話量を小さく抑えることが，紛失通信の情報理論的な効率を向上する上で求められる．この状況は，スレピアンとウォルフにより符号化定理が与えられた相関のある情報源に対する符号化の問題に帰着される.

本課題では，多値アルファベットを対象として，相関のある情報源に対する符号化の手法を扱う．特に二元線形符号を用いることで，任意の大きさの情報源アルファベットに対して効率的に符号化および復号が行える手法を提案した．さらに，低密度パリティ検査符号を用いることで理論的性能限界に迫る優れた性能が達成されることを示している．この符号化法により，先行研究における多元低密度パリティ検査符号を直接構成する手法と遜色のない性能が達成されることを確認した.

この成果は，5. 発表論文に示すもののうち，[雑誌論文]①にて公表している.

### (4) その他の関連する研究成果

加法的白色ガウス雑音通信路における通信路符号化を対象として，情報速度が通信路容量に迫る符号化と変調の方式に関して検討を行った．特に，情報速度が比較的小さい領域において理論限界に迫る性能を達成し得る手法を提案した．さらに，低密度パリティ検査符号を用いて符号化を行った場合の復号性能を計算機シミュレーションおよび EXIT チャートと呼ばれる手法を用いて評価を行った．この内容は 5. 発表論文に示すもののうち，[雑誌論文]③，[学会発表]④にて公表している.

また，歪みのある情報源符号化に関して，二元線形符号を用いた量子化の一手法を提案し，ブロック長が小さく抑えられる場合でも良好な圧縮性能を達成可能であることを示した．この成果は[雑誌論文]④にて公表している.

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　6 件）

① 岩田翔平、井坂元彦、相関のある多元情報源に対する二元線形符号による符号化、電子情報通信学会誌、査読有、vol. J95-B、2012、100-109

② Motohiko Isaka、Seiya Kawata、Signal sets for secret key agreement with public discussion based on Gaussian and fading channels、IEEE Trans. Inform. Security and Forensics、査読有、2011、523-531

③ 小川陽平、進藤篤史、井坂元彦、AWGN 通信路の通信路容量に迫る符号化変調に関する検討、電子情報通信学会論文誌、査読有、vol. J94-B、2011、74-84

④ Misako Kotani、Motohiko Isaka、Lossy coding of binary sources with short linear codes、IEICE Trans. Fundamentals、査読有、vol. E93-A、2010、2074-2076

⑤ Motohiko Isaka、Unconditionally secure oblivious transfer from algebraic signaling over the Gaussian channel、IEICE Trans. Fundamentals、査読有、vol. E93-A、2010、2017-2025

⑥ Motohiko Isaka、Oblivious transfer from the additive white Gaussian noise channel、IEICE Trans. Fundamentals、査読有、vol. E93-A、2010、516-525

〔学会発表〕（計　5 件）

① Shohei Iwata, Toshihiro Hattori, Motohiko Isaka、On coding for nonbinary source with side information at the decoder、International Symposium on Information Theory and its Applications (ISITA2010)、2010 年 10 月 18 日、Taichung,Taiwan

② Motohiko Isaka、On unconditionally secure oblivious transfer from continuous channels、IEEE International Symposium on Information Theory (ISIT2010)、2010 年 6 月 17 日、Austin, TX, USA

③ Motohiko Isaka, Seiya Kawata、On secret key agreement over the additive white Gaussian noise channel、IEEE International Conference on Personal Indoor Mobile Multimedia Communications (PIMRC2009)、2009 年 9 月 15 日、Tokyo、Japan

④ Yohei Ogawa, Katsuaki Honma, Wataru Morita, Motohiko Isaka、On the near-capacity signaling and coding scheme for the additive white Gaussian noise channel、International Symposium on Wireless Personal Multimedia Communications (WPMC2009)、2009 年 9 月 9 日、Sendai, Japan

⑤ Motohiko Isaka、Efficient oblivious transfer from algebraic signaling over the Gaussian channel、IEEE International Symposium on Information Theory (ISIT2009) 、2009 年 6 月 30 日、Seoul, Korea

６．研究組織
(1)研究代表者

井坂 元彦（ ISAKA MOTOHIKO ）
関西学院大学・理工学部・准教授
研究者番号： 50351739