様式 C-19

科学研究費補助金研究成果報告書

平成２３年　５月　３１日現在

機関番号：１６１０１
研究種目：研究活動スタート支援
研究期間：2009～2010
課題番号：21860064
研究課題名（和文）　情報理論的暗号における効率および安全性の解析
研究課題名（英文）　Study on the efficiency and security of information theoretic cryptography
研究代表者
渡辺　峻（WATANABE　SHUN）
徳島大学・大学院ソシオテクノサイエンス研究部・助教
研究者番号：70546910

研究成果の概要（和文）：
本研究では，情報理論的暗号の効率および安全性の解析に取り組み，主に以下の三つの成果を得た．第一に，量子鍵配送プロトコルにおいて最適な偏光軸の補正法の解明に取り組み，ユニタル通信路と呼ばれるクラスに対しては最適な補正方法を解明した．第二に，従来広く使われていた秘密鍵生成の方法が脆弱性であることを解明した．第三に，ガウス型情報源からの秘密鍵共有において，公開通信のレートと秘密鍵の生成レートのトレードオフ関係の解明した．

研究成果の概要（英文）：
In this study, we investigated the efficiency and the security of information theoretic cryptography, and main results are summarized as follows. First, in the quantum key distribution protocols, we clarified the optimal polarization axis compensation method for the unital channel class. Second, we clarified that the key generation method widely used in literatures is not secure in the sense of the so-called strong security criterion. Third, in the secret key agreement from correlated Gaussian sources, we clarified the trade-off between the public communication rate and the key generation rate.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,010,000	303,000	1,313,000
2010 年度	780,000	234,000	1,014,000
年度			
年度			
年度			
総　計	1,790,000	537,000	2,327,000

研究分野：情報通信
科研費の分科・細目：共通基礎研究
キーワード：情報理論的暗号、情報理論、量子暗号

１．研究開始当初の背景

近年，量子効果を積極的に情報通信に利用した量子情報が注目を集めている．その中でも最も実用化に近いのが量子鍵配送である．量子鍵配送は現在主流である公開鍵暗号とは根本的に異なり，攻撃者が十分な計算資源（計算時間）を費やしたとしても破ることができないという安全性（情報理論的な安全性）を要求する情報理論的暗号のひとつである（図１参照）．

２．研究の目的

本研究の目的は，申請期間の２年間におい

て，情報理論的暗号の理論解析を行うことで，その内容は大きく分けると以下の２つの課題からなっていた．

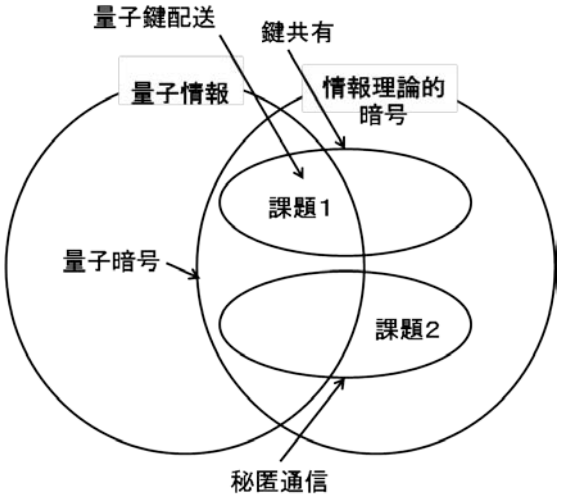


図1：本研究で扱う研究分野の関係

(課題 1) 量子鍵配送における送受信機の偏光軸の最適な補正方法の解明---量子鍵配送プロトコルは大きく分けると三つのステップ，ビット列の伝送，通信路の推定，後処理から成っている．しかし，プロトコルを実装する際には，ビット列の伝送のステップにおいて高い信頼度でビット列を伝送し秘密鍵の生成レートを向上させるために，送受信器の偏光軸の補正を行う．しかしながら，どのような偏光軸の補正方法について従来は十分な研究がされてなく，最適な補正方法が不明であった．本研究の目的は，鍵の生成レートを最大にするという意味で最適な軸補正法を明らかにすることであった．
(課題 2) 秘匿通信のための現在広く使われている符号設計法の脆弱性の解明---情報理論的な秘密鍵共有や秘匿通信において，鍵の長さや送信したビット数に対して，盗聴者に漏洩する情報の割合が小さいことを要求する弱い安全性と，盗聴者に漏洩する情報の量そのものが小さいことを要求する強い安全性がある．そして，従来情報理論的暗号において広く使われていた鍵共有や秘匿通信の方法は，弱い安全性を満足することはよく知られていたが，強い安全性を満足するか不明であった．本研究では，従来広く使われていた鍵共有や秘匿通信の方法は，強い安全性を満足せず，脆弱であることを明らかにすることであった．

３．研究の方法

平成 21 年度は課題 1 に取り組み，平成 22 年度は課題 2 に取り組む予定であった．課題 2 については，本研究の申請時に部分的に解決済みであった，秘密鍵共有における問題から取り組む予定であった．秘密鍵共有において従来広く使われていた鍵の生成方法が脆弱であることを明らかにし，その後，秘匿通信において従来広く使われていた伝送方法が脆弱であることを明らかにする予定であった．課題 1 については，本研究の新政治に部分的に解決済みであった，ユニタル通信路に対する問題から取り組む予定であった．その後，ユニタル通信路を含む一般の通信路クラスに対して，最適な軸補正方法を明らかにする予定であった．

４．研究成果

課題 1 については，ある対称性を持つユニタル通信路と呼ばれる通信路クラスに対しては，最適な軸補正法を明らかにすることに成功した．しかしながら，本研究で提案した補正方法が，一般の通信路クラスに対しても最適であるかは現段階では明らかにはなっていない．しかしながら，従来は軸補正法について全く指針がなかった状況を考えると，本研究の成果によって大きく前進したと考えられる．

課題 2 については，秘密鍵共有において従来広く使われていた鍵共有の方法が脆弱であることについて，研究申請時より強い結果を得ることに成功した．すなわち，盗聴者に漏洩する情報の量が，共有する秘密鍵の長さを N としたとき，$\sqrt{N}$ のオーダーで増加することを明らかにした．本研究成果は，鍵生成の手続きである秘密増幅と呼ばれる手続きが，復号器で補助情報を利用した Slepian-Wolf 符号化と呼ばれるデータ圧縮の手法と双対であることを利用して得られた（図 2 参照）．本研究の成果によって，乱数生成問題と情報源符号化の問題の関連がより明らかになった．また，本研究の成果によって，今後は強い安全性基準を採用した秘密鍵共有の研究が促進されるものと思われる．

課題 1 と課題 2 を当初予定していたところまで解決することは非常に困難であると判断し，研究機関の途中から，新たに，ガウス情報源からの秘密鍵共有における公開通信のレートと秘密鍵レートのトレードオフを解明するという課題に取り組み始めた．この課題は，近年非常に注目されているガウス変調を利用した連続信号の量子暗号と関連が深く，非常に重要な問題である．ガウス情報

源のような連続信号からの秘密鍵共有では，離散情報源からの秘密鍵共有とは異なり，情報源を離散信号に量子化するステップを加える必要があり，情報源をどのように量子化するかということが非常に重要になる（図3，4 参照）．また，工学的に意味のある問題設定にするには，秘密鍵共有プロトコルで使用する公開通信路のレートに制限を入れ，秘密鍵の生成レートとのトレードオフを議論する必要がある．本研究では，情報源がスカラーガウス情報源とベクトルガウス情報源の場合に，公開通信のレートと鍵の生成レートのトレードオフ関係を解明することに成功した．本研究では，送受信者，盗聴者の信号が全て古典的な信号である場合を考えていたが，今後は本研究の成果を量子鍵配送の枠組みに拡張することが望まれる．

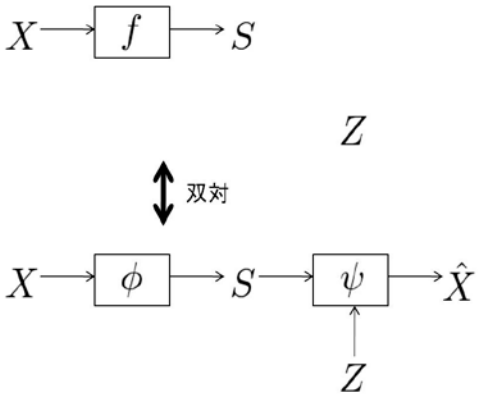
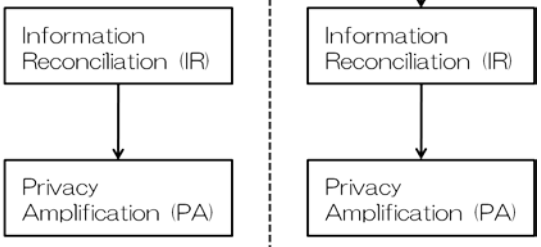


図2：秘密増幅（上）とSlepian-Wolfシステム（下）の対応関係．秘密増幅では種となるビット列Xから関数fによって秘密鍵Sを取り出す．秘密鍵Sは盗聴者の情報Zとは統計的に独立でることが望まれる．一方，Slepian-Wolfシステムでは，情報Xを符号化器φで圧縮して送り，復号器ψでは情報Zを参照しながらXを推定する．



(図3)離散信号を用いた鍵共有の流れ

(図4)連続信号を用いた鍵共有の流れ

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３件）

① Shun Watanabe, and Yasutada Oohama, “Secret Key Agreement from Vector Gaussian Sources by Rate Limited Public Communication,” IEEE Transactions on Information Forensics & Security, (accepted for publication), 2011, （査読あり）

② Shun Watanabe, and Yasutada Oohama, “Secret Key Agreement from Correlated Gaussian Sources by Rate Limited Public Communication,” IEICE Transactions Fundamentals, vol. 93-A, no. 11, pp. 1976-1983, November 2010, （査読あり）

③ Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu, “Strongly Secure Privacy Amplification Cannot Be Obtained by Slepian-Wolf Code,” IEICE Transactions Fundamentals, vol. 93-A, no. 9, pp. 16550-1659, September 2010, （査読あり）

〔学会発表〕（計５件）

① Shun Watanabe, and Yasutada Oohama, “Secret Key Agreement from Vector Gaussian Sources by Rate Limited Public Communication,” 2010 IEEE International Symposium on Information Theory, Austin, U.S.A., June 13-18, 2010

② Shun Watanabe, and Yasutada Oohama, “Secret Key Agreement from Vector Gaussian Sources by Rate Limited Public Communication,” 電子情報通信学会情報理論研究会，徳島大学常三島キャンパス，2010 年 5 月 21 日

③ Shun Watanabe, and Yasutada Oohama, “Secret Key Agreement from Correlated Gaussian Sources by Rate Limited Public Communication,” 第 32 回情報理論とその応用学会，山口県湯田温泉ホテルかめ福，2009 年 12 月 1 日-12 月 4 日

④ Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu, “Optimal Axis

Compensation in Quantum Key Distribution Protocols over Unital Channels," IEEE International Symposium on Information Theory, Seoul, Korea, June 28-July 3, 2009

⑤Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu, "Strongly Secure Privacy Amplification Cannot Be Obtained by Slepian-Wolf Code," 2009 IEEE International Symposium on Information Theory, Seoul, Korea, June 28-July 3, 2009

６．研究組織

(1)研究代表者

渡辺　峻（WATANABE　SHUN）

徳島大学・大学院ソシオテクノサイエンス研究部・助教

研究者番号：70546910

(2)研究分担者

なし

研究者番号：

(3)連携研究者

なし

研究者番号：