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　３０　年　　６　月　１４　日現在

機関番号：　１３９０１
研究種目：　基盤研究(B)（一般）
研究期間：　2014～2017
課題番号：　２６２８９１１６

研究課題名（和文）コセット符号化の安全性を最も高める線形符号の解明

研究課題名（英文）Study of Linear Codes for Coset Coding with Highest Security

研究代表者
松本　隆太郎（Matsumoto, Ryutaroh）

名古屋大学・工学研究科・准教授

研究者番号：１０３３４５１７

交付決定額（研究期間全体）：（直接経費）　　8,300,000円

研究成果の概要（和文）：コセット符号化とは、情報理論的に安全なメッセージ秘匿化を行うときの代表的な方法であり、包含関係にある線形符号の対を用いて構成することが多い。線形符号を用いたコセット符号化が効果的である対象として、秘密分散法、セキュアネットワーク符号化が従来から知られているが、どのようなどのような線形符号を用いればそれぞれの対象について効果的であるか明らかではなかった。秘密分散法とセキュアネットワーク符号化では必要になる線形符号が異なるが、それぞれについて適した線形符号の性質を明らかにし、具体的な構成法を与えた。また、従来知られていなかった量子秘密分散法に適した線形符号の性質を明らかにした。

研究成果の概要（英文）：Coset coding is a representative method for securing messages in an information theoretic secure way, and it usually consists of a pair of linear codes. Coset coding with linear codes is useful for secret sharing and secure network coding. But it had been unknown which linear codes are suitable. In this project, we clarified which linear codes are suitable for secret sharing and secure network coding, respectively. Moreover, we also proposed explicit constructions of suitable linear codes. As another application, we also clarified the relationship between quantum secret sharing and suitable pairs of linear codes for it.

研究分野：　情報通信工学

キーワード：　秘密分散　セキュアネットワーク符号化　ネットワーク符号化　量子計算　量子情報　線形符号

１．研究開始当初の背景

本プロジェクトを開始する少し前に東北大震災があり、地理的に集中した場所にデータを蓄積すると１度の災害ですべて失われてしまうことに関心が高まり、データセンターを地理的に離れた場所に複数設置して一つの情報を保存する方法に関心が高まった。その際同一の複製を複数の場所に保管すれば情報が盗難されるリスクが高まる。そのような情報漏洩のリスクを無くすために秘密分散法が有効であり、秘密分散法により生成したシェアを異なる場所のデータセンターに格納することにより情報漏洩のリスクを下げながら災害等による情報消失のリスクも下げられる。そのような状況下で、研究代表者は KDDI 研究所の栗原ならびに東京工業大学の植松らと共に、線形符号の対からすべての線形秘密分散法を構成出来ることを明らかにし、そのときに線形符号が持つべき望ましい性質を明らかにした[1]。しかし、望ましい線形符号を具体的に与えるところまでは至っていなかった。また、線形符号を用いたコセット符号化自体は秘密分散法以外にもセキュアネットワーク符号化に使われ効果をあげているが、それらの応用と線形符号の間の関係は未解明であった。

２．研究の目的

（１）前述のような背景のもとで、秘密分散法に適した線形符号を具体的に構成することを目的とした。

（２）また、線形符号を用いたコセット符号化をセキュアネットワーク符号化に用いたときに、線形符号が持つべき性質を明らかにし、望ましい性質を持つ線形符号の具体的な構成法を与えることを目的とした。

３．研究の方法

前述（１）の目的を達成するために、従来の線形符号理論で用いられている Gilbert-Varshamov 限界の議論を流用して、最適な線形符号が持ちうる符号長と次元に関する限界を導出することを目指した。また、（２）の目的を達成するために文献[1]の方法をセキュアネットワーク符号化に適用するときにどこをどう変えればよいか検討した。さらに、線形符号の対を用いてコセット符号化などメッセージ秘匿化を行う際に、本プロジェクトの方法論を適用できる他の対象がないか検討した。

４．研究成果

（１－１）線形符号の対から秘密分散法を構成するとき、そのセキュリティに関する性能は符号の相対一般化ハミング重み(RGHW)から決まる[1]。まず、最適な線形符号が持つことが出来る符号長と次元を、従来の線形符号の Gilbert-Varshamov 限界を導出する議論を改変して明らかにした。符号長は秘密分散法のシェア数に、次元は秘密情報のビット数に正比例する。

（１－２）次に、線形符号としてリードソロモン符号を用いて秘密分散法を構成する方法が３８年前から知られているが、この方法はシェアの個数が多くなるにつれてシェア１つの大きさも大きくする必要があり、分散したい秘密情報が小さいときにシェアを格納するための記憶領域が無駄になるという問題点が知られていた。この問題を解決するために、固定された大きさの有限体の上で任意に長い符号長を持ち優れた性能を有する代数幾何符号を用いて秘密分散法を構成することによりこの問題を解決した。

（１－３）ランプ型秘密分散法とは、秘密情報の部分的な漏洩と引き換えにシェアの大きさを秘密情報の大きさ（ビット数）よりも小さくできる秘密分散法である。ランプ型秘密分散法で、秘密情報の一部がそのまま漏れることを防げる性質を強安全性と呼び、山本により定義された。従来から知られている、代数幾何符号を用いたマルチパーティ計算に適した秘密分散法が強安全性を持つことを証明し、従来から知られている手法の知られていない長所を明らかにした。

（２－１）線形符号を用いたコセット符号化をセキュアネットワーク符号化に用いるとき、どのような線形符号が適しているか明らかにする基準を KDDI 研究所の栗原と東京工業大学の植松とともに明らかにした。具体的には、研究代表者らが提案した相対一般化ハミング重みと、従来から知られている Gabidulin のランク重みを組み合わせた相対一般化ランク重み(RGRW)を提案し、これによってネットワーク内のμ本のリンクが盗聴され、コセット符号化を用いているときに、盗聴者に漏洩する最大の情報量が RGRW で正確に記述出来ることを明らかにするとともに、前述の強安全性を持つための線形符号の条件も明らかにし、強安全性をもち誤り訂正能力もあるセキュアネットワーク符号化法の具体的な構成を与えた。

（２－２）本プロジェクト遂行中に Guruswami らが、ネットワーク符号化法において従来の２倍程度の誤りを訂正できる方法を提案した。この方法は単一の線形符号を用いているからもう一つの線形符号と組み合わせてコセット符号化を構成しメッセージ秘匿性を付加できると考えたが、（２－１）で報告した理論は、Guruswami らの方法には直接適用できなかった。そこで Umberto Martinez-Penas と共同で、（２－１）の理論を拡張し、相対一般化行列重み (RGMW)を提案し、μ本のリンクが盗聴されたときに漏洩する情報量が RGMW で記述されることを明らかにし、RGRW が定義できない線形符号に対し

ても RGMW は常に定義でき、RGRW と RGMW の両方が定義できるときは両者の漏洩情報量の評価が一致することを示した。GMW に関する双対性定理を証明し、従来から知られている GHW と GRW に関する双対性定理が今回示した GRW の双対性定理の特別な場合として導出できることを示し、提案した概念が今までに研究された概念を統合し一般化するものであることを示した。さらに、Guruswami らが提案した従来法を大幅に上回る誤り訂正能力を持つネットワーク誤り訂正符号を改変して誤り訂正能力を維持しつつメッセージ秘匿性を追加する方法を提案した。

（３－１）これまでに述べた成果を他の文脈に応用できないか検討しているうちに、量子秘密分散法も線形符号の対から構成されるが、量子秘密分散法の安全性と、もとになった線形符号の関係については明らかになっていないことに気づき、これを明らかにした。一方量子情報処理においては媒体の情報量が大きくなるにつれて実現が難しくなるため、シェアの大きさを小さく保つことがますます重要になる。今まで知られている量子秘密分散法はシェアの個数が大きくなるにつれてシェア１個の大きさも大きくなるものしか知られていなかったので、本研究では代数幾何符号に基づいた量子秘密分散法の構成法を提案した。

（３－２）従来の秘密分散法については、シェアの大きさを不必要に大きくしないようにしながら任意のアクセス構造を実現する方法が岩本らによって提案されている。しかし、量子秘密分散法に関しては任意のアクセス構造を実現する方法について明らかではなかった。このため、（３－１）の方法と岩本らの方法を組み合わせて、小さいシェアで任意のアクセス構造を持つ量子秘密分散法を構成する方法を明らかにした。

（３－３）強安全性を定義するときに問題になった、秘密情報の一部分がそのままわかってしまう問題は量子秘密分散法にもあるかどうか未解明であった。研究代表者は Paul Zhang とともにそのようなことが従来の量子秘密分散法で起こりえる具体例を与え、そのようなことが起こらない強安全性を量子秘密分散法について定義し、強安全性を持つ量子秘密分散法を具体的に構成した。

（３－４）線形符号の対から量子秘密分散法を構成するときに、まず線形符号の対を量子誤り訂正符号に変換してから量子秘密分散法にする。線形符号の対から構成できない量子誤り訂正符号はよく知られているが、それを量子秘密分散法として使った場合に何らかのメリットがあるのか知られていなかった。そのような量子秘密分散法によって古典情報（ビット列）の秘密を分散すると、従来の古典力学で記述出来る秘密分散法ではどうやっても実現できないアクセス構造を実現できる実例をしめし、量子秘密分散法によって古典情報の秘密を分散する有用性をはじめて明らかにした。

（４－１）一般に、符号理論をベースとした秘密分散法では消失誤り訂正符号を用いてプロトコルが構成される。用いる符号を削除誤り訂正符号に変えられれば、より弱い仮定の下で秘密分散法を構成できる。そこで削除誤り訂正符号の調査を進めたところ、線形削除誤り訂正符号の符号化率は０．５未満に制限されることが Abdel らにより示されていることが判明した。そこで、非線形符号も研究の視野に入れ、削除誤り訂正符号の構成法を研究した。

＜引用文献＞

[1] J. Kurihara, T. Uyematsu, and R. Matsumoto, Secret Sharing Schemes Based on Linear Codes Can Be Precisely Characterized by the Relative Generalized Hamming Weight, IEICE Trans. Fundamentals, vol.E95-A, no. 11, pp. 2067-2075, 2012.

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 15 件）

1. R. Matsumoto, Coding Theoretic Construction of Quantum Ramp Secret Sharing, IEICE Trans. Fundamentals, E101-A, no.8, 2018 (掲載予定)

2. C. Galindo, F. Hernando, and R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields and Their Appl., 2018, DOI: 10.1016/j.ffa.2018.04.010

3. U. Martinetz-Penas and R. Matsumoto, Relative Generalized Matrix Weights of Matrix Codes for Universal Security on Wire-Tap Networks, IEEE Transactions on Information Theory, vol.64, no.4, pp. 2529 -2549, 2018.

4. R. Matsumoto. Quantum Stabilizer Codes Can Realize Access Structures Impossible by Classical Secret Sharing, IEICE Trans. Fundamentals, vol.E100-A, no.12, pp. 2738-2739, 2017.

5. Olav GEIL, Stefano MARTIN, Umberto MARTÍNEZ-PEÑAS, Ryutaroh MATSUMOTO, Diego RUANO, On asymptotically good ramp secret sharing schemes, IEICE

Trans. Fundamentals, vol.E100-A, no.12, pp.2699-2708, 2017.

6. R. Matsumoto, Quantum Optimal Multiple Assignment Scheme for Realizing General Access Structure of Secret Sharing, IEICE Trans. Fundamentals, vol.E100-A, no.2, pp. 726-728, 2017.

7. R. Matsumoto, Two Gilbert-Varshamov-type existential bounds for asymmetric quantum error-correcting codes, Quantum Information Processing, 2017, DOI: 10.1007/s11128-017-1748-y

8. R. Matsumoto, Unitary reconstruction of secret for stabilizer-based quantum secret sharing, Quantum Information Processing, 2017, DOI: 10.1007/s11128-017-1656-1

9. R. Matsumoto and M. Hayashi, Universal Secure Multiplex Network Coding With Dependent and Non-Uniform Messages, IEEE Transactions on Information Theory, vol.63, no.6, pp. 3773-3782, 2017.

10. M.Hagiwara, A short proof for the multi-deletion error-correction property of Helberg codes, IEICE Communications Express, 2016, DOI: 10.1587/comex.2015XBL0182

11. J. Kurihara, R. Matsumoto, and T. Uyematsu, Relative Generalized Rank Weight of Linear Codes and Its Applications to Network Coding, IEEE Transactions on Information Theory, vol.61, no.7, pp. 3912-3936, 2015.

12. R. Matsumoto, Strong Security of the Strongly Multiplicative Ramp Secret Sharing Based on Algebraic Curves, IEICE Trans. Fundamentals, vol.E98-A, no.7, pp. 1576-1578, 2015.

13. R. Matsumoto, Optimal multiple assignment scheme for strongly secure ramp secret sharing schemes with general access structures, IEICE Communications Express, 2015, DOI: 10.1587/comex.4.317

14. P. Zhang and R. Matsumoto, Quantum strongly secure ramp secret sharing, Quantum Information Processing, 2015. DOI: 10.1007/s11128-014-0863-2

15. Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, Yuan Luo, Relative Generalized Hamming Weights of One-Point Algebraic Geometric Codes, IEEE Transactions on Information Theory, vol.60, no.10, pp. 5938-5949, 2014.

〔学会発表〕（計　2件）

1. M. Hagiwara, On Ordered Syndromes for Multi Insertion/Deletion Error-Correcting Codes, Proc. of ISIT2016, July, pp.625-629, 2016. DOI: 10.1109/ISIT.2016.7541374, 2017.

2. M. Hagiwara, Perfect codes for single balanced adjacent deletions, Proc. of ISIT 2017: pp.1938-1942, 2017.

〔図書〕（計　1件）

萩原学（編者、著者）、松本隆太郎（著者）、他９名、進化する符号理論、日本評論社、2016/9.

６．研究組織

(1)研究代表者

松本　隆太郎（MATSUMOTO, Ryutaroh）
名古屋大学・工学研究科・准教授
研究者番号：10334517

(2)研究分担者

萩原　学（HAGIWARA, Manabu）
千葉大学・大学院理学研究科・准教授
研究者番号：80415728

(3)研究協力者

Olav Geil（GEIL, Olav）
Dirgo Ruano（RUANO, Diego）