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

令和　４ 年　 ６ 月 ２９ 日現在

機関番号：８２７２７
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ０４４０２

研究課題名（和文）多元接続を導入した物理層のセキュリティと秘密分散で情報保護がなされた無線通信方式

研究課題名（英文）Wireless communication systems protected by secret sharing and physical layer security incorporated with multiple access

研究代表者

宮崎　真一郎（MIYAZAKI, Shinichiro）

独立行政法人高齢・障害・求職者雇用支援機構職業能力開発総合大学校（能力開発院、基盤整備センター）・能力開発院・准教授

研究者番号：４０６４８９３７

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：秘密分散法の一つである（k, n）しきい値法は，秘密情報をn個のシェアと呼ばれる情報に分散し，シェアをk個以上集めると元の情報を復元できる方式である．これは，k-1個のシェアを集めても一部の情報も復元できないため，情報漏えいに強い方式といえる．物理層のセキュリティにおいては，正規端末の受信品質を可能な限り向上させることにより，正規端末と非正規端末の受信品質の差を大きくすることが重要となる．本研究では，正規端末と非正規端末の秘密情報再生確率に差を設ける秘密分散の手法と，多元接続通信において正規端末の受信品質を向上させる手法を提案しその特性を明らかにした．

研究成果の学術的意義や社会的意義
無線通信は，その利便性から様々な通信システムにおいて需要が拡大している．それにともない，盗聴による情報漏えいなどのリスクに対して情報保護への要求も拡大している．一般的には暗号化や認証といった手段で情報を保護しているが，計算機の計算能力が飛躍的に向上すれば情報漏えいの危険性もある．そのため，無線通信における情報保護をより強化するために，秘密分散や物理層のセキュリティなどの伝送系の信号処理といった新たな手法を加え，情報保護手法の要求条件等を明らかにしたことは社会的意義が大きい．

研究成果の概要（英文）：The threshold secret sharing scheme distributes secret information into n shares, and the original information can be recovered when k or more shares are collected. This scheme is resistant to information leakage because no information can be recovered even if k-1 shares are collected. In physical layer security, it is important to increase the difference in reception quality between authorized and unauthorized terminals by improving that of authorized terminals as much as possible.
In this study, we proposed a method of secret sharing that provides a difference in the probability of reproducing secret information between authorized and unauthorized terminals, and a method of improving the reception quality of authorized terminals in multiple access. The characteristics of the proposed methods are demonstrated by computer simulations.

研究分野：通信工学

キーワード：秘密分散　多元接続　信号処理

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

無線通信は，スマートフォンやノートパソコンを用いて，個人情報などの秘密情報を含む様々なデータを手軽に誰でもが送受信することを可能にする．近年では，人だけでなく，家電やセンサなど「モノ」をインターネットに接続する IoT（Internet of Things）が注目されており，その端末数は爆発的に増加を続けている．そのため，無線通信の需要は，様々なシステムにおいて，ますます拡大しているといえる．一方，無線通信は利便性だけでなく，正規の通信相手ではない者に，故意または偶然にその通信を傍受されるという危険性がある．そのため，安全性に対する期待は高く，情報漏えいに対して暗号化など様々な対策が検討され実装されている．

暗号化では，暗号のために用いる鍵の管理が重要となる．家の玄関の鍵と同じように，鍵を消失してしまうと正規の者であっても家の玄関を開けること（復号）はできない．鍵の消失を防止するために，合鍵など鍵の複製を増やすと，それだけ盗難（盗聴）の危険性は増加してしまう．たとえ暗号化された通信であっても，鍵の情報が漏えいすれば盗聴を防ぐことはできない．鍵の消失と漏えいの対策技術として，秘密分散が注目されている．秘密分散の一つの方式として（k, n）しきい値法がある．それは，秘密情報を n 個のシェアと呼ばれる情報に分散し，その中から k 個（$k \leq n$）以上のシェアを集めると秘密情報を復元できる方式である．図 1 に（4, 7）しきい値法の例を示す．このとき，非正規端末が$k-1$個までのシェアを集めても，秘密情報に関する情報はまったく得ることができないため，漏えいに強い方式といえる．また，正規端末が$n-k$個のシェアを消失した場合でも，秘密情報を復元できるため，消失に強い方式といえる．

また，近年，正規端末の受信品質を高め，非正規端末の受信品質を下げ，両者に著しく差を設けることで情報漏えいを防止する，物理層のセキュリティ技術が注目されている．正規端末に複数アンテナを用いて電波の放射方向を制御したり，送信電力を制御したりすることで，非正規端末との受信品質に差を設ける．

２．研究の目的

秘密分散において，正規端末と非正規端末の秘密情報再生確率に差を設ける通信方式を開発する．また，正規端末の受信品質を可能な限り向上させることにより，正規端末と非正規端末の受信品質の差を大きくする方式を開発する．これは，正規端末の受信品質が向上すると，基地局から送信する信号の大きさを小さくすることができ，その結果，非正規端末の受信品質をいっそう劣悪にすることができる．これらの通信方式の性能を評価し有効性の確認を研究の目的とする．

３．研究の方法

秘密分散や物理層のセキュリティに関する技術について調査を行う．この調査をもとに，組織リードソロモン符号に基づく秘密分散を適用する方式を提案する．また，正規端末の受信品質を向上させる方式についても検討する．これらの方式について，情報保護の特性の解析，および，計算機シミュレーションにより，正規端末と非正規端末の秘密情報再生確率や秘密情報のビット数に応じた秘密情報再生確率，誤り率特性等について評価する．

４．研究成果

（k, n）しきい値法の秘密分散は，組織リードソロモン符号，または，非組織リードソロモン符号で実現できることが知られている．組織リードソロモン符号は，n個のシェアのうち，$k-1$個のシェアを保護対象の秘密情報に依存しないように設定できる．そこで，組織リードソロモン符号を用いた秘密分散方式で，正規端末と非正規端末の間で秘密情報の復元条件に格差を設ける方式を提案する．$k-1$個までのシェアを正規端末の固定された識別情報として基地局と正規端末の間で事前に共有する．これらは，送信する必要がないため，安全な通信路でシェアが配信されたこととなる．保護対象の秘密情報に依存する$n-k+1$個のシェアは，通常の通信路で送信されることになる．この提案方式により，正規端末は，送信したシェアのうち少なくとも 1 個を取得すると秘密情報を得ることができるが，非正規端末はk個以上を取得しなければ秘密情報を得ることができない．そのため，正規端末と非正規端末の情報再生確率に差を設けることができる．また，$2 \leq k \leq n \leq 2k-2$の条件を満たす場合，$n-k+1 \leq k-1$となり送信されるシェアは$k$個未満となるため，非正規端末はすべてのシェアを取得しても秘密情報を得ることができない．$n > 2k-2$ の場合，非正規端末が秘密情報を再生する確率 P_0 は，$P_0 = \sum_{i=k}^{n-k+1} {}_{n-k+1}\mathrm{C}_i (1-p)^i p^{n-k+1-i}$となる．ただし$p$は受信シェアの消失確率である．正規端末が秘密情報を再生する確率P_1は，$P_1 = \sum_{i=1}^{n-k+1} {}_{n-k+1}\mathrm{C}_i (1-p)^i p^{n-k+1-i}$となる．図 2 に，$k = 5$，$n \geq 5$，共有するシェア数を$k-1=4$，送信されるシェア数を$n-k+1$とする提案方式の，$p = 0.5$としたときの正規端末と非正規端末の秘密情報再生確率を示す．$n \leq 2k-2$のとき，送信されるシェアはk個未満のため，非正規端末はすべてのシェアを取得しても秘密情報を得ることができないことを明らかにした．次に，2 位相シフトキーイング伝送において加法性白色ガウス雑音通信路を想定した解析を行った．図 3 に，シェアが収容されているパケットヘッダのビット数を 32bit，64bit，128bit，256bit としたときの，正規端末の秘密情報再生確率を示す．これより，正規端末が秘密情報を再生する所望確率を，ビット数および信号対雑音比の関係を明らかにした．

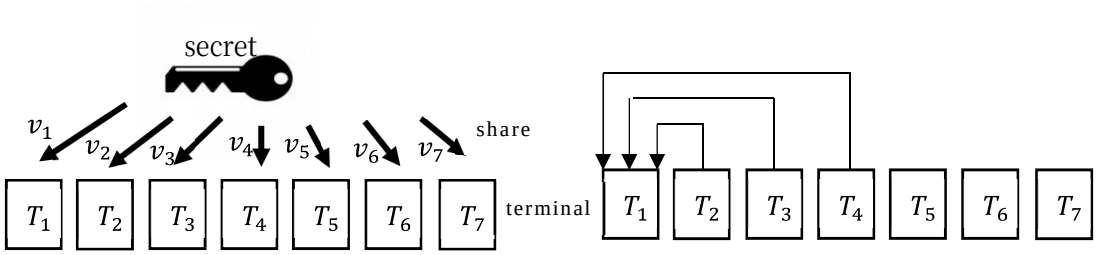

図 1　(4,7)しきい値法でシェアvの配信と秘密情報の復元

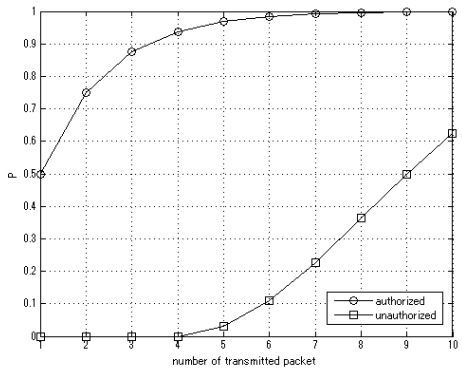

図 2 正規端末と非正規端末の秘密情報再生確率

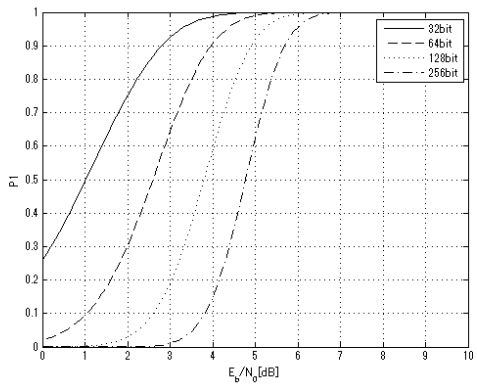

図 3 信号対雑音比と秘密情報再生確率

また，高速大容量通信の第 5 世代（5G）無線通信の補完的な技術として，可視光通信が注目されている．光源となる発光ダイオード（LED）の変調帯域幅がメガヘルツと狭いことから，パワードメイン非直交多元接続（NOMA）が注目されている．我々は，光符号分割多元接続（O-CDMA）通信において，各ユーザの異なる送信信号に対して同じ符号語で拡散し，それらを異なる強度レベルに変更した上で多重化することで通信量を増加させる方式を提案した．図 4 に送受信機の構成を示す．この方式では，受信機において，最も強度の大きな信号から復号し，その再生信号を生成する．受信信号から再生信号を減算することで残りの信号の中で最も強度の大きな信号の復号が可能となる．そのため，最も強度の大きな信号の強度を正確に推定し，信号分離することが重要となる．

まず，推定誤差が与える影響について検討した．その結果，推定誤差が±α%の場合，信号点間距離が 2α%短くなることを示した．これにより，信号点間距離が短くなるほど雑音耐性が下がり受信品質が低下するため，推定誤差が受信品質に影響を与えることを確認した．次に，強度推定方式として，移動平均法を用いる方式と最小二乗平均法を用いる方式を提案し，評価した．図 5 に 1000 サンプルの移動平均法を用いた強度推定特性を示す．移動平均法は，収束に時間がかかることと，雑音がない環境でも収束後の標準偏差に影響を与えることを示した．最小二乗平均法は，推定の標準偏差が小さくなるように改良を加えた．そのときの，強度推定特性を図 6 に示す．最小二乗平均法は，収束が速く，収束後の標準偏差も小さくできることを示した．最小二乗平均法は，収束が速いため，通信路ゲインが変動する環境でも使用できる．強度推定により，正規端末の受信品質を向上できるため，基地局からの送信信号の大きさを小さくしたり，制御したりすることで非正規端末の受信品質をいっそう劣化させることができることを示した．

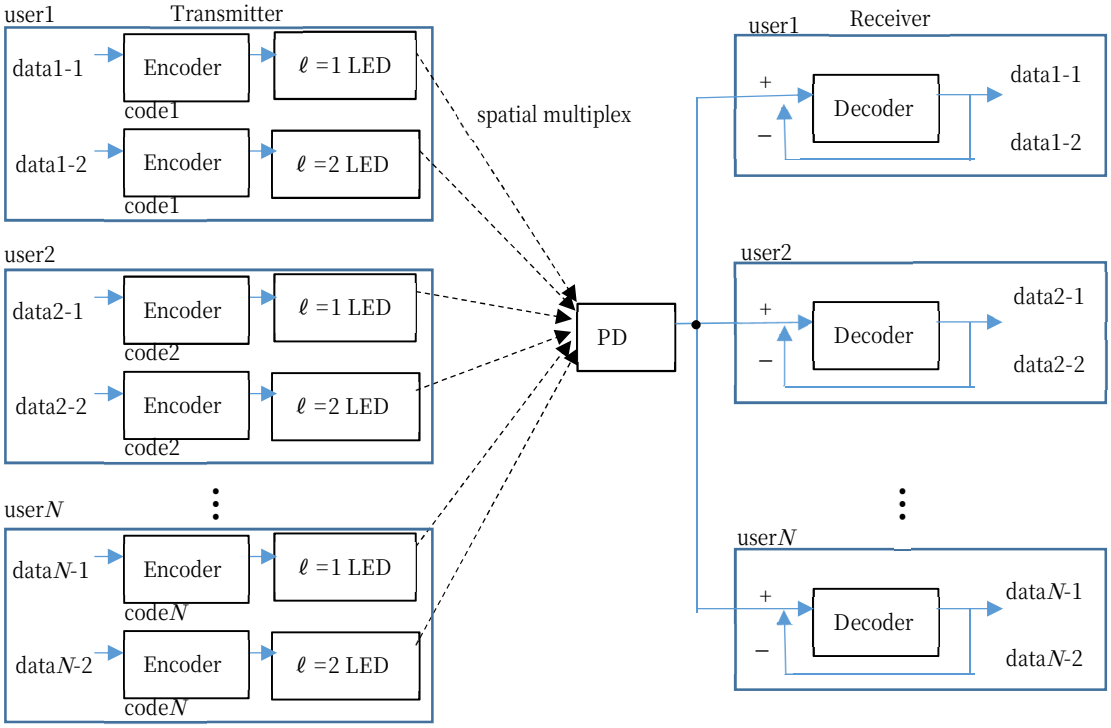

図 4　送受信機の構成（レベル数 $L=2$）

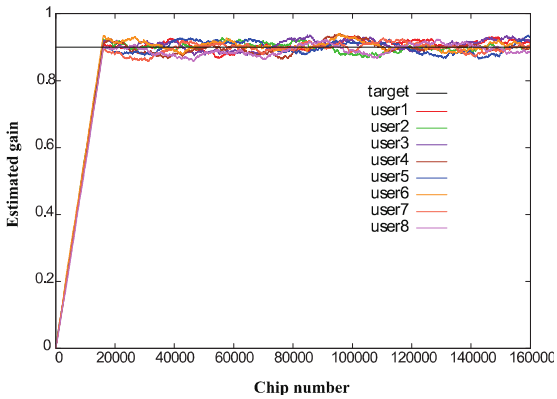

図 5　移動平均法を用いた強度推定特性

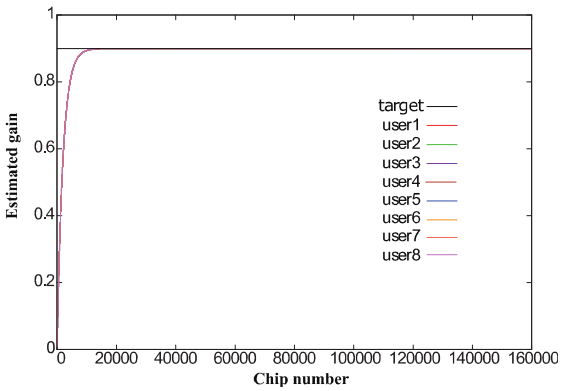

図 6　最小二乗平均法を用いた強度推定特性

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 ONO Kyohei、YAMASAKI Shoichiro、MIYAZAKI Shinichiro、MATSUSHIMA Tomoko K.	４．巻 Vol. E104-A, No.9
２．論文標題 Optical CDMA Scheme Using Generalized Modified Prime Sequence Codes and Extended Bi-Orthogonal Codes	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1329～1338
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1148	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 上方文理，小野恭平，宮崎真一郎，山嵜彰一郎，松嶋智子，大村光徳	４．巻 Vol.J104-A,No.08
２．論文標題 レベル分割多重を用いた光符号分割多元接続方式	５．発行年 2021年
３．雑誌名 電子情報通信学会論文誌 A	６．最初と最後の頁 178-190
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transfunj.2020JAP1034	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 上方文理，松嶋智子，山嵜彰一郎，宮崎真一郎，大村光徳	４．巻 vol.J103-A, No.7
２．論文標題 多重ユーザ干渉と背景光を同時に除去する同期光CDMAシステムに関する研究	５．発行年 2020年
３．雑誌名 電子情報通信学会論文誌A	６．最初と最後の頁 126-141
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計16件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 上方文理，宮崎真一郎，大村光徳，大野成義，山嵜彰一郎，松嶋智子
２．発表標題 LDMを用いた同期光CDMA 方式の受信光強度推定に関する検討
３．学会等名 第44回情報理論とその応用シンポジウム（SITA2021）
４．発表年 2021年

１．発表者名
上方文理，宮崎真一郎，大村光徳，大野成義，山嵜彰一郎，松嶋智子

２．発表標題
レベル分割多重を用いた同期光CDMA 方式の受信光強度推定に関する検討

３．学会等名
電子情報通信学会 技術研究報告，IT2021-51

４．発表年
2021年

１．発表者名
上方文理，迫田光主，大村光徳，宮崎真一郎

２．発表標題
LDM を用いた同期光 CDMA 方式における強度推定の検討

３．学会等名
第29回職業能力開発研究発表講演会講演論文集，27-F-6

４．発表年
2021年

１．発表者名
松浦大那，宮﨑 真一郎，大村光徳

２．発表標題
しきい値復号システムの開発

３．学会等名
第29回職業能力開発研究発表講演会講演論文集，27-F-7

４．発表年
2021年

１．発表者名
田中倫太郎，大村光徳，宮崎真一郎

２．発表標題
無線伝送のビット誤り率特性の活用

３．学会等名
第29回職業能力開発研究発表講演会講演論文集，27-F-5

４．発表年
2021年

１．発表者名
髙田康平，宮崎真一郎，山嵜彰一郎，松嶋智子

２．発表標題
無線伝送の周波数領域等化における残留歪みの軽減方式の検討

３．学会等名
電子情報通信学会 技術研究報告，RCS2020-178

４．発表年
2020年

１．発表者名
上方文理，小野恭平，宮崎真一郎，山嵜彰一郎，松嶋智子，大村光徳

２．発表標題
レベル分割多重を用いた光CDMA伝送方式の特性評価

３．学会等名
電子情報通信学会 技術研究報告，IT2020-58

４．発表年
2020年

１．発表者名
上方文理，小野恭平，松嶋智子，山嵜彰一郎，宮崎真一郎，大村光徳

２．発表標題
背景光とシンチレーションを考慮した光 CDMA 空間伝送の評価

３．学会等名
第28回職業能力開発研究発表講演会講演論文集，28-H-2

４．発表年
2020年

１．発表者名
小野恭平，山嵜彰一郎，松嶋智子，宮崎真一郎，大村光徳

２．発表標題
秘密分散で情報保護を施した無線通信方式の検討

３．学会等名
第27回職業能力開発研究発表講演会講演論文集，30-H-11

４．発表年
2019年

１．発表者名
山嵜彰一郎，松嶋智子，宮崎真一郎，大村光徳

２．発表標題
ElGamal暗号系と組み合わせた組織Reed-Solomon符号を用いる秘密分散方式

３．学会等名
電子情報通信学会ソサイエティ大会，基礎境界/NOLTA講演論文集，A-2-2

４．発表年
2019年

１．発表者名
松嶋智子，山嵜彰一郎，上方文理，大村篤生，遠藤克帆，宮崎真一郎，大村光徳

２．発表標題
背景光と多重ユーザ干渉を同時に除去する同期光CDMA方式に関する研究

３．学会等名
電子情報通信学会 技術研究報告，WBS2019-20

４．発表年
2019年

１．発表者名
松嶋智子，山嵜彰一郎，宮崎真一郎，大村光徳

２．発表標題
レベル分割多重を用いた光CDMA多重伝送に関する研究

３．学会等名
電子情報通信学会ソサイエティ大会，基礎境界/NOLTA講演論文集，A-2-3

４．発表年
2019年

１．発表者名
山嵜彰一郎，松嶋智子，小野恭平，遠藤克帆，大村篤生，宮崎真一郎，大村光徳

２．発表標題
レベル分割多重を用いた光CDMA多重伝送方式

３．学会等名
第42回情報理論とその応用シンポジウム(SITA2019)，3.4.4

４．発表年
2019年

１．発表者名
遠藤克帆、山嵜彰一郎、松嶋智子、宮崎真一郎、大村光徳

２．発表標題
レベル分割多重を用いた光CDMA伝送の基本構成と特性

３．学会等名
第27回職業能力開発研究発表講演会講演論文集，30-H-9

４．発表年
2019年

１．発表者名
大村篤生、山嵜彰一郎、松嶋智子、宮崎真一郎、大村光徳

２．発表標題
多段階のレベル分割を用いた光CDMA方式における多重化分離処理

３．学会等名
第27回職業能力開発研究発表講演会講演論文集，30-H-10

４．発表年
2019年

１．発表者名
上方文理，松嶋智子，山嵜彰一郎，宮崎真一郎，大村光徳

２．発表標題
背景光を除去する同期光CDMA方式の評価

３．学会等名
第27回職業能力開発研究発表講演会講演論文集，30-H-8

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	松嶋　智子 (MATSUSHIMA tomoko) (30648902)	独立行政法人高齢・障害・求職者雇用支援機構職業能力開発総合大学校（能力開発院、基盤整備センター）・能力開発院・教授 (82727)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	大村　光徳 (OMURA kotoku) (40725719)	独立行政法人高齢・障害・求職者雇用支援機構職業能力開発総合大学校（能力開発院、基盤整備センター）・能力開発院・准教授 (82727)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関