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　　元 年　　６ 月 １５ 日現在

機関番号：３４３１０
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ０６０９１

研究課題名（和文）電波伝搬特性変動に基づく不規則・間欠的な区間設定を用いた秘密鍵共有に関する研究

研究課題名（英文）Study of secret key agreement using the irregular setting of the intermittent section based on the change of radio propagation characteristics

研究代表者

笹岡　秀一（SASAOKA, HIDEICHI）

同志社大学・理工学部・教授

研究者番号：７０３０９１９４

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：　無線通信におけるバーナム暗号の実現を目指して、電波を用いた秘密鍵共有において多量の秘密鍵を効率的に取得する方法を提案した。提案方式は、電波伝搬特性の変動に基づく間欠的な区間の不規則な設定とその区間内の乱数時系列の選択を使用している。計算機シミュレーションの結果、設定区間と秘密鍵の一致が可能なこと、提案方式が有用であることが分かった。また、多量の秘密鍵共有が可能な代替方式として、電波を用いた新しい秘密鍵共有と秘密通信を検討した。代替方式との優劣比較の結果、提案方式の優位性が明らかとなった。

研究成果の学術的意義や社会的意義
　研究課題（「電波伝搬特性の不規則・間欠的な区間設定を用いた秘密鍵共有方式に関する研究」）の研究を実施した結果、多量の秘密鍵の効率的に取得する方法を提案し、提案方式の特性評価を行った。この研究成果は、電波を用いた秘密鍵共有の課題を解決するものであり、無線通信におけるバーナム暗号の実現の可能性を示唆するものとなる。また、提案した手法は物理層セキュリティに広く応用可能な汎用的なものであり、研究成果は今後の学術分野の発展に寄与することが期待される。さらに、物理層セキュリティ技術をより実用的なものするのに役立ち、社会・産業への波及効果も将来期待される。

研究成果の概要（英文）：For the realization of the Vernam cipher in the wireless communication, I proposed a method to acquire a large quantity of secret key effectively in secret key agreement using radio. The proposed method uses the irregular setting of the intermittent section based on the change of radio propagation characteristics and choice of the random number series in the section. The result of the computer simulation shows agreement of the setting section and complete secret key agreement being possible and that a proposed method is useful. In addition, as the alternative method that the acquisition of a large quantity of secret key was possible, I examined new secret key agreement and secure communication using radio. The result of the superiority and inferiority comparison with the alternative method shows the superiority of the proposed method.

研究分野：暗号・セキュリティ

キーワード：物理層セキュリティ　秘密鍵共有　電波伝搬特性変動　レベル交差　擬似乱数

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

無線通信は開かれた空間を通して電波の送受を行うため、盗聴や不正アクセスなどに脆弱なことが問題である。この対策として、共通鍵暗号や公開鍵暗号など暗号技術を使用するのが一般的である。これら従来の計算量的な複雑性を安全性の根拠とする情報セキュリティ技術に対して、最近、情報量的な複雑性を安全性の根拠とする物理層セキュリティ技術に関心が集まっている。このうち、電波を用いた物理層セキュリティ技術として、電波を用いた秘密鍵共有と電波を用いた秘密通信が盛んに研究されている。

電波を用いた秘密鍵共有では、電波伝搬の可逆性に基づいて電波伝搬変動の標本値から鍵ビットを生成することが一般的であり、観測量と標本間隔の制約から多量の鍵生成を効率的に行うことが難しい。また、電波を用いた秘密通信により鍵配送が可能であるが、その守秘性が必ずしも十分と言えないものが多い。このため、多量の秘密鍵の共有または配送を簡易に実現する手法は提案されていない。また、無線通信において多量の秘密鍵を必要とするバーナム暗号の適用に関する研究も行われていない。しかし、多量の秘密鍵が用意できれば、バーナム暗号は暗号処理が簡単であり、処理演算が制限される小型無線端末に適している。

２．研究の目的

本研究は、無線通信におけるバーナム暗号の実現を目指して、多量の秘密鍵共有を簡易に実現する方法を検討することを目標としている。このため、電波伝搬特性の標本値から鍵ビットを生成する従来方式と異なる手法を検討した。その一手法として、高速で無線伝送される乱数系列に対して、電波伝搬特性の変動に基づいて不規則・間欠的に設定された区間内の乱数を送信側と受信側で選択することで乱数系列を盗聴者に秘密裏に共有する手法を提案する。この手法では、公開通信路による多量の乱数系列の取得と電波伝搬特性の変動に基づく不規則・間欠的な区間設定が独立に行われることで、秘密裏に多量の乱数系列の共有が可能となる。この技術的課題は、不規則・間欠的な区間設定を送信側と受信側で一致させる一方、盗聴者に区間設定を困難とする方法である。そこで、研究の主たる目的は、技術的課題を解決するとともに、提案方式の有効性を計算機シミュレーションで評価することである。

また、多量の秘密鍵共有を簡易に実現する他の手法との比較検討により、提案方式の有効性を確認することも目的としている。このため、他の手法として複数アンテナを用いた効率的な新しい秘密鍵共有の検討、MIMO システムにおける盗聴耐性に優れた秘密通信の検討、および複数アンテナを用いた新しい秘密通信の検討などを行った。

３．研究の方法

研究課題（「電波伝搬特性変動に基づく不規則・間欠的な区間設定を用いた秘密鍵共有に関する研究」）を達成するため下記の研究課題を順次実施する。はじめに、①不規則・間欠的な区間設定の効果を事前検討、②電波伝搬特性に基づく不規則・間欠的な区間設定の共有法の検討を実施する。区間設定の共有については、電波伝搬路の可逆性によりある程度可能となるが、完全に一致させるために公開通信路を介した正規局間の情報交換が必要となる。この情報交換により鍵共有の安全性が損なわれない工夫が重要となる。

次に、③不規則・間欠的な区間設定を用いた提案方式の有効性の計算機シミュレーションによる評価を実施する。これにより所期の性能が実現できたかを評価する。また、④多量の秘密鍵共有を簡易に実現する他の手法の検討を実施する。これについても、計算機シミュレーションで性能評価を実施する。さらに、⑤提案方式の課題抽出と改良方式の検討を行う。また、⑥電波伝搬特性を忠実に模擬した総合特性評価を実施する。

研究体制については、応募者が主体的に実施する他に、大学院生にシミュレーションの実施などを担当させる。

４．研究成果

電波伝搬特性変動に基づく区間設定と乱数系列の部分選択を用いた秘密鍵共有については二つの方式を提案した。その一つは、受信信号強度変動の極値を高精度に検出して区間設定を行う手法を用いており、もう一方は、複数搬送波間の位相差がある閾値を交差（レベル交差）する時刻に基づいて機関設定を行う手法を用いている。これらの提案方式に対して以下の(1)と(2)に示すような研究成果を得た。

また、提案方式の有効性を確認するための比較方式の検討については、複数アンテナを用いた効率的な秘密鍵共有法の検討、MIMO システムにおける盗聴耐性に優れた秘密通信の検討、および複数送信アンテナを用いた新しい秘密通信の検討を行った。その結果、以下の(3)、(4)、(5)に示すような研究成果を得た。

下記の(1)と(2)に示す提案方式の研究成果および(3)、(4)と(5)に示す比較方式の研究成果に基づいて、本研究課題が対象とした提案方式の有効性が明らかとなった。また、これらの研究成果は、新規性が高く有効性も高いものであり、今後、この分野の発展に寄与することが期待される。

(1) 受信信号強度変動の極値に基づく部分系列選択を用いた提案方式

はじめに、乱数系列の部分系列選択に受信信号強度変動の極値（極大値と極小値）から得た区間設定を用いる手法を提案した。提案方式では、選択した部分系列の集合に対して並べ替え

処理を行った後に鍵候補を作成し、一致確認処理後に秘密鍵を共有する。提案方式において鍵共有特性を左右する極大値・極小値の検出特性及び鍵一致特性を計算機シミュレーションで正規者と盗聴者に対して評価した。その結果、正規者間の極値の検出特性が十分に良好であり鍵不一致特性が十分小さいこと、盗聴者がほとんど極値を検出できず、鍵一致率が非常に小さいことが示された。このことから、提案方式は、盗聴者に秘密裏に正規者間で誤りなく秘密鍵を共有することが可能であることが分かった。

(2) 位相差のレベル交差に基づく区間設定を用いた提案方式

次に、受信信号強度変動の極値を用いる手法の課題を解決するため、複数搬送波間の位相差がある閾値を交差する時刻に基づく改良手法（レベル交差手法）を提案した。この提案方式では、レベル交差時刻から区間設定を行うので極値の検出が不要となる。この提案方式の特性を計算機シミュレーションで評価した結果、受信信号強度変動の極値に基づく提案方式とほぼ同等な特性が得られた。

(3)複数アンテナを用いた秘密鍵共有

多量の秘密鍵共有を簡易に実現できる他の手法として、伝搬特性の時間変化が少ない環境を前提とし、複数アンテナの重みを変化させて受信信号強度(RSSI)系列を得る秘密鍵共有方式の効率向上を検討した。この検討方式は、事前測定した電波伝搬特性を活用して複数アンテナ局では計算で受信信号強度を算出し、単一アンテナ局では RSSI を測定して秘密鍵共有を行う方式である。また、検討方式では、鍵不一致率の低減と生成する鍵ビットの増加の工夫を行っている。計算機シミュレーションの結果、鍵生成時間を従来の半分程度に短縮しながら、良好な秘密鍵容量が得られることが明らかとなった。しかし、鍵生成効率の画期的な向上には不十分な方式である。

また、別の検討方式として、複数アンテナ送受信システムにおいて事前に双方向の複数の伝搬係数を取得し、アンテナ重み情報の公開伝送を用いた秘密鍵配送方式を検討した。この検討方式は、鍵生成効率の画期的な増加の可能性を持っているが、実現に必要な演算処理と伝送情報量の増加に問題があることが分かった。

(4)MIMO における秘密通信

多量の秘密鍵共有を簡易に実現できる他の手法として、MIMO システムを用いた秘密通信を検討した。この手法は、独立成分分析による信号分離を用いた盗聴に脆弱であることが指摘されている。この独立成分分析を用いた攻撃を避けるには、MIMO で伝送される信号をガウス性に変更することが望ましい。

そこで、秘密信号と複素ガウス信号の乗積信号を用いた秘密鍵配送方式を検討し、計算機シミュレーションにより検討方式の特性を評価した。その結果、正規者間で秘密鍵配送が良好に行えること、盗聴者に対して鍵情報の秘密性を十分保持できることが分かった。しかし、盗聴耐性が不十分な場合が起こり得ること、盗聴耐性の向上と引き換えに伝送効率が大幅に低下する問題があることが分かった。この問題を解決するため、擬似ガウス信号の採用、秘密信号の分解と複数秘密信号の同時伝送を用いた方式を検討した。計算機シミュレーションの結果、特性の向上が図られることが分かったが、伝送効率の改善が十分とは言えない。

(5)複数送信アンテナを用いた秘密通信

多量の秘密鍵共有を簡易に実現できる他の手法として、複数送信アンテナを用いた秘密通信を検討した。検討した方式は、非変調信号を複数アンテナから重みを付けて送信し、特定の受信点で変調信号を生成（空間選択性のある変調信号を生成）する方式である。このため、チャネル係数、非変調信号、変調信号から送信アンテナ重みが算出される。ここでは、非変調信号として定振幅な位相変調波を用いている。

この検討方式の特性を計算機シミュレーションで評価した結果、正規者間で良好なビット誤り率特性が得られることが分かった。また、盗聴者に対して十分な秘密保持容量が得られることが明らかとなった。このため、検討方式を使用することで盗聴耐性に優れた秘密鍵配送が実現可能であることが確かめられた。しかし、送信重みの算出の演算量が、効率的な鍵生成の障害となることも分かった。

５．主な発表論文等

〔雑誌論文〕（計　7　件）

① 市川力、笹岡秀一、岩井誠人、“ MIMO システムにおける秘密信号と擬似複素ガウス信号の乗積信号を用いた秘密鍵配送方式 ”、電子情報通信学会論文誌 B、査読あり、Vol.J101-B、No.7、pp.546-557、2018.
DOI:10.14923/transcomj.2017WFP0004

② 中井宏樹、笹岡秀一、岩井誠人、“ 移動通信におけるフェージング変動に基づく秘密鍵共有方式の研究 ”、同志社大学ハリス理化学研究報告、査読あり、Vol.59、No.2、pp.113-124、2018.

③ 辻和輝、笹岡秀一、岩井誠人、“ 電波伝搬特性に基づく信号分解と空間ベクトル合成を用いた秘密情報伝送方式 ”、電子情報通信学会論文誌 B、査読あり、Vol.J100-B、No.9、pp.782-794、2017.
DOI:10.14923/transcomj.2017APP0015

④ 樋口拓己、笹岡秀一、岩井誠人、“伝搬係数の共有とアンテナ重み情報の公開伝送を用いた秘密情報共有方式”、電子情報通信学会論文誌 B、査読あり、Vol.J100-B、No.7、pp.449-457、2017.
DOI:10.14923/transcomj.2016WFP0010

⑤ 滝村拓馬、笹岡秀一、岩井誠人、“MIMO システムにおける秘密信号と複素ガウス信号の乗積信号を用いた秘密鍵配送方式”、電子情報通信学会論文誌 B、査読あり、Vol.J99-B、No.9、pp/772-781、2016.
DOI:19.14923/transcomj.2016A0015

⑥ 樋口拓己、笹岡秀一、岩井誠人、“電波伝搬特性の事前測定に基づく複数アンテナを用いた秘密鍵共有方式”、電子情報通信学会論文誌 B、査読あり、Vol.J99-B、No.9、pp.675-683、2016.
DOI:10.14923/transcomj.2016APP0016

⑦ 松本達也、笹岡秀一、岩井誠人、“公開通信路による乱数伝送と電波伝搬特性に基づく部分系列選択を用いた秘密鍵共有方式の検討”、電子情報通信学会論文誌 B、査読あり、Vol.J99-B、No.9、pp.665-674、2016.
DOI:10.14923/transcomj.2016APP0017

〔学会発表〕（計 6 件）

① 辻和輝、笹岡秀一、岩井誠人、“信号分解と空間ベクトル合成を用いた秘密情報伝送方式における盗聴耐性の評価”、電子情報通信学会無線通信システム研究会、Vol.RCS2017-229、pp.177-182、2018.

② 樋口拓己、笹岡秀一、岩井誠人、“伝搬係数の共有とアンテナ重み情報の公開伝送を用いた秘密情報共有の検討”、電子情報通信学会無線システム研究会、Vol.RCS2016-164、pp.65-70、2016.

③ 辻和輝、笹岡秀一、岩井誠人、“電波伝搬特性に基づく信号分解と空間ベクトル合成を用いた秘密情報伝送方式”、電子情報通信学会無線通信システム研究会、Vol.2016-163、pp.59-64、2016.

④ 市川力、笹岡秀一、岩井誠人、“MIMO システムにおける秘密信号と擬似複素ガウス信号の乗積信号を用いた秘密鍵配送方式”、電子情報通信学会無線通信システム研究会、Vol.RCS2016-162、pp.53-58、2016.

⑤ 樋口拓己、笹岡秀一、岩井誠人、“電波伝搬特性の事前測定に基づく複数アンテナを用いた秘密情報共有方式”、電子情報通信学会無線システム研究会、Vol.RCS2015-193、pp.19-24、2015.

⑥ 松本達也、笹岡秀一、岩井誠人、“公開通信路による乱数伝送と電波伝搬特性に基づく部分系列選択を用いた秘密鍵共有方式の検討”、電子情報通信学会無線通信システム研究会、Vol.RCS2015-192、pp.13-18、2015.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：
ローマ字氏名：
所属研究機関名：
部局名：
職名：
研究者番号（8 桁）：

(2)研究協力者
研究協力者氏名：
ローマ字氏名：

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。