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 ２７ 日現在

機関番号：３３３０２
研究種目：若手研究(B)
研究期間：2017～2021
課題番号：１７Ｋ１４６８０

研究課題名（和文）歩きながらワイヤレス充電を盗電から守る磁界ゆらぎ秘密鍵生成共有の研究

研究課題名（英文）Wireless secret key agreement system on magnetic fluctuation for wireless charging system.

研究代表者
坂井　尚貴（Sakai, Naoki）

金沢工業大学・電気・光・エネルギー応用研究センター・研究員

研究者番号：１０７３６１７７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究は磁界結合型ワイヤレス給電(WPT)システムに搭載する、磁界ゆらぎを用いた無線秘密鍵生成共有システム(磁界秘密鍵方式)を提案し、その安全性を示す。内容①磁界秘密鍵方式で生成する秘密鍵の秘匿性を示す。内容②秘密鍵の盗聴耐性を明らかにする。成果①４x４の送電コイルを床面に敷き詰めたWPTシステムにおいて、送電装置と送電コイルの接続を無作為に切替えて磁界ゆらぎを生成する。ゆらぎから生成した受電電力履歴は高い秘匿性が得られた。成果②前述のシステムに盗聴局を配置し、受電電力履歴から生成する秘密鍵の盗聴耐性を評価した。送電装置と送電コイルの接続数の工夫により高い盗聴耐性が得られた。

研究成果の学術的意義や社会的意義
本研究の成果は磁界ゆらぎという物理現象を情報の暗号化に活用できる可能性が高いことを、世界で初めて示したことが学術的に意義深いといえる。また、計算機や数学の進歩によらない新しい暗号化技術の可能性を示すという点において、情報化社会にとっても重要な知見である。

研究成果の概要（英文）：This work proposes the wireless secret key agreement (WSA) system for a wireless charging system based on magnetic coupling and evaluates the secrecy of the proposed approach.
Evaluation 1: we evaluate the secrecy of the received power fluctuation generated by the WSA system. Evaluation 2: we evaluate wiretapping tolerance of the secret key.
Result 1: the WSA system generated the received power fluctuation that occurred by changing randomly for the connection between the RF source and a transmitting coil in 4x4 transmitting coils. The received power fluctuation is high secrecy. Result 2: the WSA system is added an illegal receiver. We generated the secret key from the received power fluctuation of a legal receiver and evaluated the wiretapping tolerance of the secret key. High wiretapping tolerance was obtained by adjusting the number of connections between the power source and the transmitting coils.

研究分野：マイクロ波

キーワード：近傍電磁界　無線秘密鍵共有システム　磁界結合方式　ワイヤレス電力伝送　フレネル界

１．研究開始当初の背景

ワイヤレス給電技術を利用した「置くだけ充電」が既に製品化されている。この置くだけ充電の特長は有線充電と比べて差異が小さい。次なるターゲットとして「歩きながら充電」の研究開発が進められている[1]。歩きながら充電は室内だけでなく、公共スペースでの利用も想定される。ゆえに盗電対策が必要である。本研究は歩きながら充電を実現する、ワイヤレス給電システム(WPT システム)を対象とし、その ID 認証技術の基礎検討の一つである。対象のシステムは一面に送電コイルを敷き詰めて移動する受電端末へ磁界で高周波(RF)電力を送電する（図１）。現状の WPT システムで用いる ID 認証技術は通信で用いられる公開鍵暗号方式が適用されている[2]。

■国内外における研究動向及び位置づけ

ID 認証は公開鍵暗号方式[3]による暗号化通信が一般に用いられる。この方式について、送信端末は受信端末が公開する公開鍵で情報を暗号化・送信する。受信端末は秘密鍵で情報を複合化する。第三者は公開鍵から秘密鍵を効率的に推定できないため、送信端末は安全に情報を送れる。しかし，計算機や数学の進歩により、現実時間で秘密鍵が推定される恐れがある。故に計算機や数学の進歩に依らない新しい暗号化技術が望まれている。

本研究は磁界のゆらぎという物理現象を駆使した秘密鍵生成共有技術（磁界秘密鍵方式）を提案する。提案方式について図 1 を用いて説明する。提案方式は受電端末 Alice と送電器 Bob が互いに電力の送受を繰り返す。そして、互いに得た受電電力の履歴を秘密鍵とし、暗号・復号に用いる。受信電力履歴が秘密鍵になる理由は、以下の３つの物理現象で説明できる。

① Alice 周辺の環境変化により送受コイル間の結合が時間変動すること、送電コイル（図中実線コイル)の無作為な切替わりにより送受コイル間の結合が時間変動することで受電電力が無作為に時間変動する（磁界結合の時間変化)。
② 送受コイルは 2 ポート線形回路網とみなせるため、Alice と Bob は同じ受電電力履歴を得る（磁界結合の相反性)。
③ 盗電端末 Eve は Alice と配置場所が異なるため、Bob とのコイル間結合が Alice と異なる。結果 Alice と Eve は異なる受電電力履歴をもつ（磁界結合の場所依存性)。

■着想に至った経緯

応募者はワイヤレス給電に用いる磁界と無線秘密鍵生成共有システムに用いる電波は、同じ電磁界であることに着目した。これまでの研究成果を駆使することで、WPT システムのための磁界ゆらぎによる秘密鍵生成共有が可能であると確信し、本研究の着想に至った。

[1]“磁気共鳴型ワイヤレス電力伝送コイルの面方向へのアレー化に関する一検討,”WPT2010-17,January 2011.
[2]“ワイヤレス電力伝送システム用制御通信技術，”東芝レビュー，vol.68，no.7，2013.
[3]“暗号技術入門-秘密の国のアリス-,”ｿﾌﾄﾊﾞﾝｸ ｸﾘｴｲﾃｨﾌﾞ(株),2013 年 3 月,ISBN978-4-7973-5099-9.

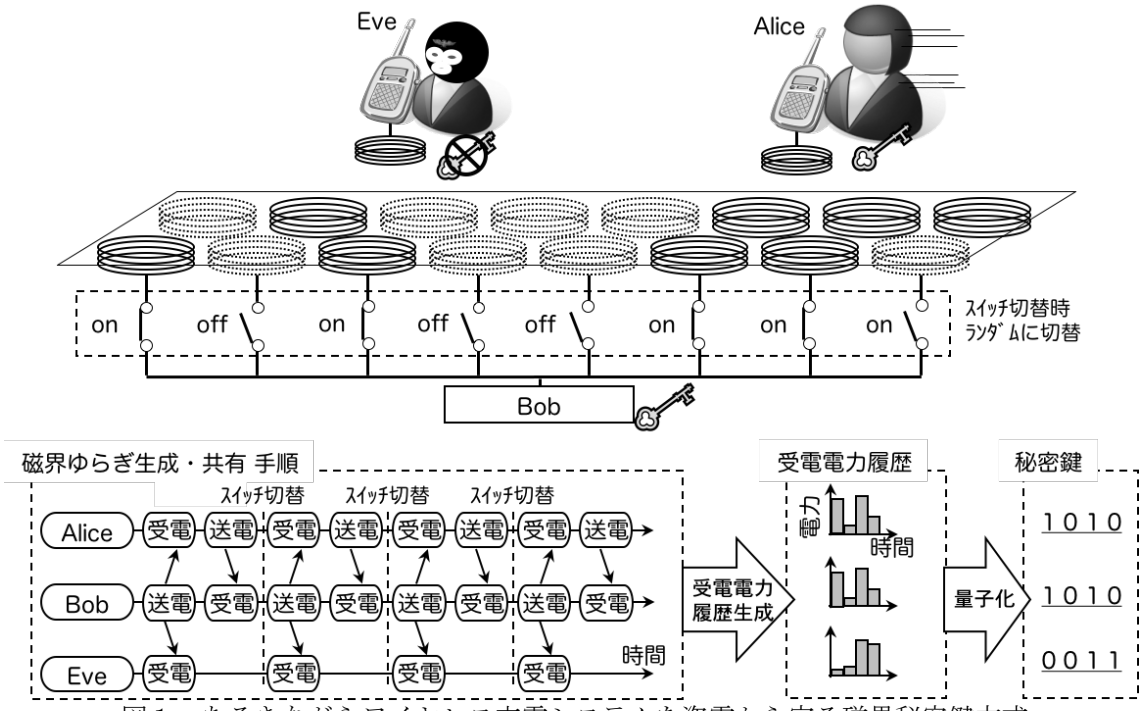

図１　あるきながらワイヤレス充電システムを盗電から守る磁界秘密鍵方式

２．研究の目的
本研究期間内で磁界のゆらぎにより生成共有される秘密鍵の安全性を示す。具体的には、
目的１）磁界秘密鍵方式により生成される秘密鍵の秘匿性を担保する Alice の移動範囲および送電コイル切替パタンを明確にする。
目的２）磁界秘密鍵方式により生成される秘密鍵の盗聴耐性を担保する Alice の移動範囲、送電コイル切替パタン、および Eve の配置を明確にする。
目的３）磁界秘密鍵方式を搭載した WPT システムを試作する。そして、磁界秘密鍵方式により生成される秘密鍵の秘匿性および盗聴耐性が担保されていることを実験で実証する。

３．研究の方法
【目的①】 磁界秘密鍵方式により生成される受電電力履歴の秘匿性を検証する。秘匿性とは受電電力履歴が雑音と区別がつかないことを示しており、Alice がもつ受電電力履歴の自己相関係数で評価する。受電電力履歴は磁界結合の時間変化による磁界のゆらぎを表す。
【実施内容①】 Alice の移動による時間的ゆらぎにより得られる受電電力履歴を評価する。Alice は任意高さの水平面内を移動する。送電コイル ON/OFF の組合せ（以後：送電パタン）を変えていき、最も秘匿性が高くなる送電パタンを探求する。同時に秘匿性が低くなる Alice の高さ、移動ルート、送電パタンを明確にする。送電パタンの切替えによる空間的ゆらぎにより得られる受電電力履歴を評価する。Alice の配置は固定し、送電パタンを切替える。最も秘匿性が高くなる送電コイルの切替パタンを探求する。同時に秘匿性が低くなる Alice の配置を明確にする。上記得られた成果を組合せ、磁界結合の時間変化により得られる受電電力履歴を評価する。磁界秘密鍵方式により生成される秘密鍵の秘匿性を担保する、Alice の移動範囲および送電コイルの切替パタンを明確にする。

【目標②】 提案する磁界鍵生成方式により生成される受電電力履歴の盗聴耐性を検証する。盗聴耐性とは非正規端末の受電電力履歴傍受に対する正規端末の受電電力履歴の耐性を示しており、Alice と Eve の受電電力履歴の相互相関係数で評価する。
【実施内容②】 送電コイル網に Eve を配置し、Alice が生成する受電電力履歴の盗聴耐性を評価する。Eve は Bob からの送電電力を傍受する。Alice が生成する受電電力履歴の盗聴耐性を担保する、Alice の移動範囲、Eve の配置および送電コイルの切替パタンを明確にする。

【目標③】 磁界秘密鍵方式の秘匿性および盗聴耐性が担保されることを実験で実証する。加えて、生成される秘密鍵の秘匿条件付き相互情報量(以後：Imac)を実証実験で評価する。
【実施内容③】 実証実験に用いる WPT システムを、協力者の発表論文[4]のシステムをベースに設計・試作する。試作したシステムを用いて Alice が得た受電電力履歴の秘匿性、盗聴耐性および Imac を評価する。Alice は解析で得た移動範囲を自由に動く。Eve は任意に配置する。送電コイル切替パタンは解析で得られた成果を用いる。
[4]“励振ループを用いた複数受電器への電力分配手法の実機検証,” WPT 第二種研究会, 5 件目, Nov. 2013.

４．研究成果
【成果①】
磁界秘密鍵方式を搭載する WPT システムの解析モデルを図２に示す。送電コイルは床面に 4x4 で配置されており、各送電コイルは送電装置に接続される。受電コイルはいずれかの送電コイルの直上に配置される。次に受電電力履歴の生成プロセスについて説明する。各送電コイルの入力端子は無作為で「送電装置に接続」「開放」「短絡」3 つの状態になる。そして、送電装置から電力を送電する。このとき、各送電コイルへ送電される高周波電力の位相差はランダムである。電力を送電するたびに、送電コイルの入力端子の状態および高周波電力の位相を無作為に変動させることで、受電電力履歴は秘匿性をもつ。本解析では、256 の受電電力履歴を作成する。Alice の位置による受電電力履歴の自己相関係数を図３左図に示す。図３より、Alice の位置によらず、受電電力履歴の自己相関係数 $\rho(k\neq 0)$ は 0.1 を下回っている。つまり、Alice のもつ受電電力履歴は白色ガウス雑音とほぼ同じと言え、非常に高い秘匿性を有する。

【成果②】
実施内容①でもちいた図２のシステムに盗聴局(Eve)を配置し、Alice と Eve が受電電力履歴から生成する 256bit の鍵から盗聴耐性を算出する。盗聴耐性とは、Eve が持つ Alice の鍵の情報量のことである。また、Bob が Alice へ電力を送電する際にその電力を Eve は任意の位置で傍受し受電電力履歴を生成する。Alice が送電コイル#6 の直上にいるときの、鍵の盗聴耐性を図３に示す。横軸は Eve の配置を示している。縦軸は盗聴耐性を示しており、1 に近いほど Alice の鍵が盗まれていないことを示している。今回の解析では送電装置に無作為に接続する送電コイルの数を１、２，４と３ケースで評価している。図３より、Alice と同じ位置以外では、Eve の盗聴耐性は 0.4 以上が得られている。また送電装置に接続する送電コイルの数が多いほど、Eve の配置によらず安定した盗聴耐性が得られていることがわかる。従い、送電装置に無作為に接続

する送電コイルの数は、送電コイルの全体の数に対して、適切な数を割り当てることが重要と考えられる。

今回の基礎検討による２つの成果より、磁界秘密鍵方式により生成される秘密鍵は秘匿性、盗聴耐性ともに十分な値が得られており、本提案方式の有用性を示すことができた。しかし、今回の研究期間で実施内容③まで達成できなかった。したがって、得られた成果①、②を踏まえ、引き続き研究を継続し、実施内容③に取り組む。

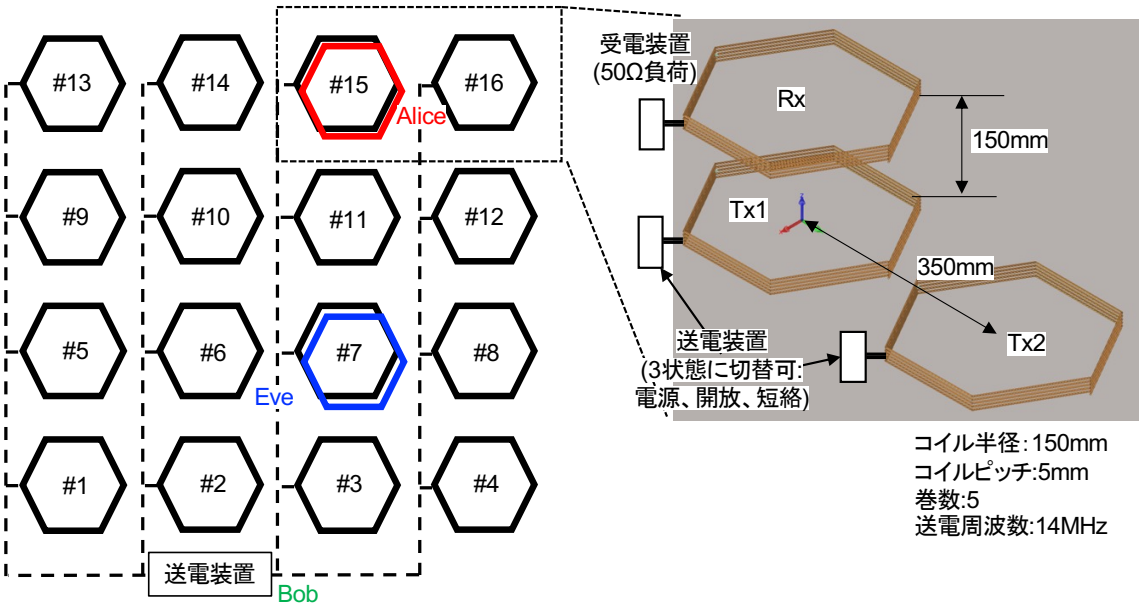

図２　磁界秘密鍵方式を搭載する無線電力伝送システムの解析モデル

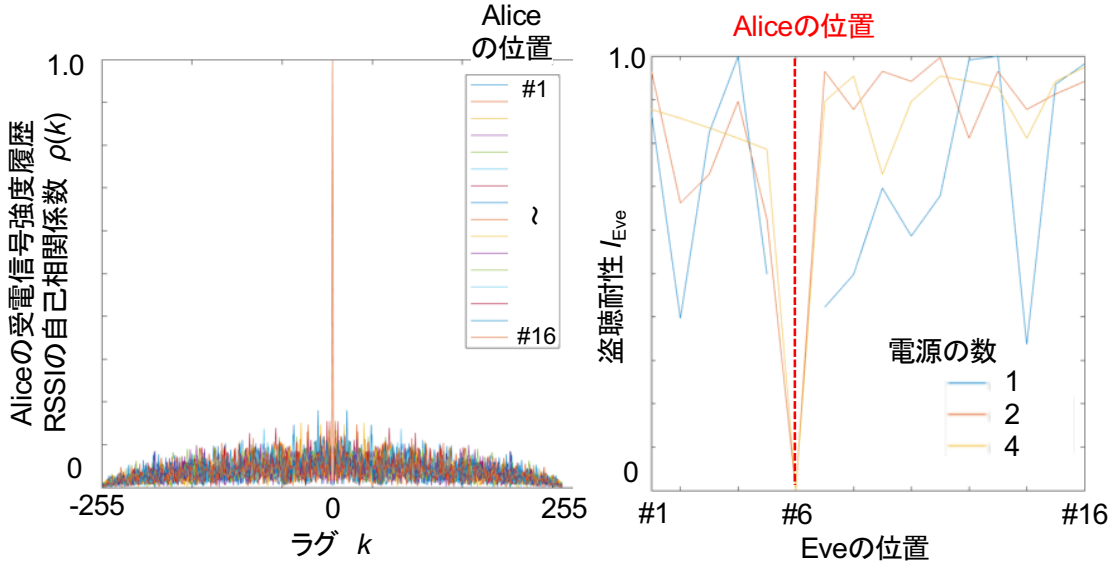

図３　磁界秘密鍵方式による秘密鍵の秘匿性と盗聴耐性の評価

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計0件

〔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

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