科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１６　日現在

機関番号：　１３９０４
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４５２

研究課題名（和文）無線秘密鍵共有方式のための可変指向性アンテナの研究

研究課題名（英文）Study of variable beam-forming antenna for wireless secret key agreement system

研究代表者
大平　孝（Ohira, Takashi）

豊橋技術科学大学・工学（系）研究科（研究院）・教授

研究者番号：３０３９５０６６

交付決定額（研究期間全体）：（直接経費）　　3,500,000円、（間接経費）　　1,050,000円

研究成果の概要（和文）：本研究は４つの成果が得られた．
（１）電波ゆらぎを用いた無線鍵生成・共有方式（電波ゆらぎ方式）の秘匿性を高めるアンテナ設計指針RDC（Reactance Domain Correlation)を提案，有効性を明らかにした．（２）RDCを用いてエスパアンテナの構造と秘匿性の関係を明らかにした．（３）USBスティックサイズの小型エスパアンテナの設計試作した．アンテナ，送受信回路，USBインターフェース，制御回路を１枚プリント基板上に実装，プラグアンドプレイできるシステムの構築に成功した．（４）構築したシステムは屋内環境において128ビットの鍵を45秒で生成できた．

研究成果の概要（英文）：This study outputs four significant results.
(1) We proposed Reactance Domain Correlation (RDC) in order to enhance secrecy of wireless secret key agreement systems, and showed effectivity of RDC. (2) We clarified the relation between ESPAR antenna structure and the system secrecy by employing RDC. (3) We designed and prototyped a USB stick size ESPAR antenna for the system, and integrated the antenna, transceiver, USB interface, and system control unit on a printed circuit board. We implemented all of them to work in plug and play on a laptop PC. (4) The system generates and shares the secret key of 128 bits in length within 45 seconds on indoor environment.

研究分野：　工学

科研費の分科・細目：　電気電子工学・通信・ネットワーク

キーワード：　可変指向性アンテナ　電波ゆらぎ　無線秘密鍵共有　エスパアンテナ　情報セキュリティ

１．研究開始当初の背景

スマートフォンやモバイル WiFi ルータなど，電波を用いた無線データ通信は様々なシーンで活躍している．一方でネットバンクやネットショッピングといった電子商取引サービスなどが活発になり，情報の保護が安心・安全なユビキタス社会の必須事項になってきている．一般に，セキュアな無線データ通信には暗号化技術が利用される．暗号化技術とは「鍵」を通信の相手方と共有し，それをデータの暗号・復号化に利用する技術である．現在，最も広く実用化されている暗号化技術は公開鍵方式である．公開鍵方式は暗号鍵を公開，復号鍵を非公開とする方式である．そして，第三者は暗号鍵から復号鍵を推定することは計算量的に困難であると考えられている．しかし，コンピュータの性能向上に伴い，現実時間での復号鍵推定が現実味を帯びてきており，コンピュータの性能に依らない新しい暗号化技術が望まれている．

この課題の解決策として，電波のゆらぎを用いた鍵生成・共有方式を，平成２０年度「基盤研究 C」で提案・実験してきた．この方式は，１）可変指向性アンテナを用いて双方向に電波のやり取りをするだけで相手方と同一鍵を共有できる，２）電波に鍵情報が一切含まれていない，３）高価なハードウェアを用いない，という特長がある．しかし，本方式の研究する過程で，周辺環境によって鍵の秘匿性が劣化する現象を発見した．

２．研究の目的

電波のゆらぎを用いた鍵生成・共有方式の秘匿性を飛躍的に向上させうる可変指向性アンテナを開発する．つまりは屋内・外といった，あらゆる環境において安心・安全な暗号鍵を生成することを目標とする．本方式は広範囲での無線システムの情報セキュリティ向上を，アンテナというハードウェアを小型携帯端末などのモノに挿入するプラグアンドプレイだけで，誰もが簡単に得ることができることを目指している．

３．研究の方法

秘匿性を高める可変指向性アンテナを設計・試作するに当たり，
(1)可変指向性アンテナの設計指針の提案，
(2)秘匿性を高めるアンテナ構造の探求，
(3)可変指向性アンテナの高速な測定手法の確立，
これら３つの技術課題を解決する．
(4)最後に鍵生成実験を教室，オフィス，ロビー等の屋内・屋外環境にて実施する．比較のため，アンテナ以外の実験環境は平成２０年度基盤研究 C で実施したものと同等とする．全環境において１２８ビットの鍵生成を２秒以内で成功する確率が９９％以上を最終達成目標とする．

４．研究成果

(1) 本方式の秘匿性を高めうる可変指向性アンテナの設計指針 RDC(Reactance Domain Correlation)を提案した．電波ゆらぎ方式の盗聴原理に着目，各素波のゆらぎが独立であれば盗聴されにくいことを発見した．電波ゆらぎと指向性の関係より，RDC を

$$E[r_{pd}]=\frac{1}{M^2}\sum_{i=1}^{M}\sum_{j=1}^{M}r_{pd}(a_i,a_j)$$

$$r_{pd}(a_i,a_j)=\frac{|C(a_i,a_j)|}{\sqrt{C(a_i,a_i)C(a_j,a_j)}}$$

$$C(a_i,a_j)=\frac{1}{N}\left[\sum_{h=1}^{N}\{D_h(a_i)D_h(a_j)^*\}-\frac{1}{N}\sum_{h=1}^{N}\{D_h(a_i)\}\sum_{h=1}^{N}\{D_h(a_j)^*\}\right]$$

と定義した．$D_h(\alpha)$はα方向の指向性を表す．コンピュータシミュレーションにより RDC と秘匿性の関係を確認した．図１の結果より RDC が低いほど盗聴量 E[ρe]が低減する．従って秘匿性向上に RDC が有効であることは明らかである．

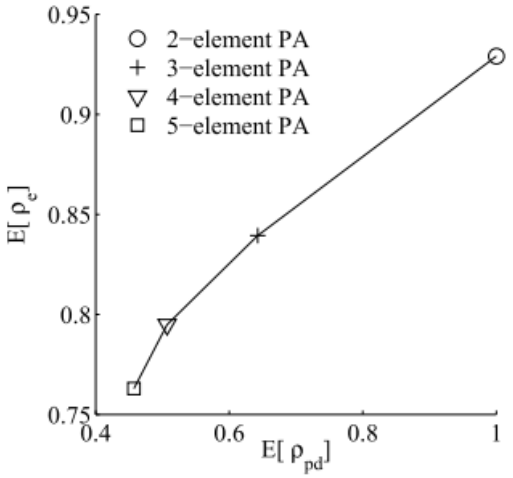


図１　RDC と秘匿性の関係

(2) 電波ゆらぎ方式のためのエスパアンテナを RDC などの設計指標を用いて設計した．はじめに可変リアクタンス回路の設計を行った．3 素子ダイポールエスパアンテナが形成可能な指向性パタンとリアクタンスおよび素子間隔依存性を調査し，その結果リアクタンスの最適可変範囲を見いだした．RDC を用い，3 素子ダイポールエスパアンテナの最適な素子間隔について調べた．結果，素子間隔λ/16 で RDC は最小となることが判明した．一般的に用いられた素子間隔λ/4 と比較しかなり狭い素子間隔が電波ゆらぎ方式に適しているといえる．

(3) エスパアンテナを高速に測定する手法として，空間分布イミタンス行列法を提案した．そして，提案測定手法について，エスパアンテナ簡易モデルを用いて原理検証を行った．

(4) エスパアンテナの可変性能と秘匿性の関係を明らかにした．エスパアンテナの指向性制御素子を増加させた時の鍵の秘匿性 をシミュレーションで評価した．指向性の制御

素子を増加させることで鍵の秘匿性向上を確認することができた．また，両正規局に可変指向性アンテナを搭載した場合(条件 A)と，正規局片側に可変指向性アンテナを搭載した場合(条件 B)で得られる鍵の秘匿性を比較した．結果，条件 A の可変指向性アンテナの指向性制御素子数の和と,条件 B の可変指向性アンテナの指向性制御素子数が等しいとき，得られる鍵の秘匿性はほぼ変わらないことを発見した．

５）USB スティック型エスパアンテナを，提案した可変指向性アンテナ設計指針 RDC(Reactance Domain Correlation)を用いて，設計試作した．アンテナの設計は，アンテナの素子間隔をパラメータとし，RDC が最も低くなる素子間隔を電磁界解析で探索した．試作においては，USB スティック形状プリント基板上に，エスパアンテナ，送受信回路，マイコン，USB インターフェース，可変リアクタンス回路を実装した．試作したアンテナを図２に示す．試作アンテナの指向性を測定し，指向性が可変することを確認した．

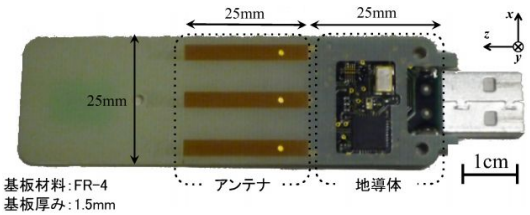


図２　試作したエスパアンテナ

６）電波ゆらぎ方式の秘匿性が向上しうる信号処理手法として，電波ゆらぎ固有値除去手法を提案した．シミュレーションにより，秘匿性が向上することを確認した．

７）電波ゆらぎ方式の新しい盗聴手法，能動的盗聴法を提案した．能動的盗聴端末周辺において，秘匿性が低下することをシミュレーションにより確認した（図３）．無線秘密鍵生成共有システムに新しい課題を見出した．

８）試作した USB スティック型エスパアンテナを用いて電波ゆらぎ方式鍵生成共有システムがプラグアンドプレイできるシステムの構築に成功した．構築したシステムは屋内環境において 128 ビットの鍵を 45 秒で生成できた．

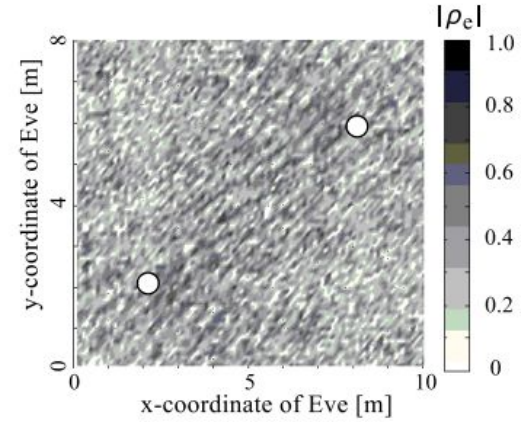
５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　２件）

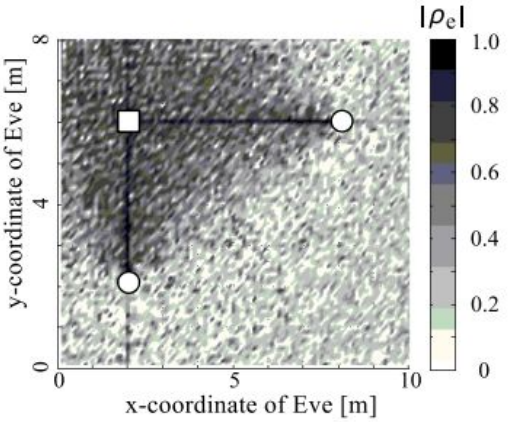
① 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平 孝，“無線秘密鍵生成共有方式の盗聴耐性を高める可変指向性アンテナ指向性多様性指標” 電子情報通信学会論文誌 B，査読有，Vol.J96-B，No.9，pp. 936-944，2013，http://search.ieice.org/bin/summary.php?id=j96-b_9_936&category=B&year=2013&lang=J&abst=.
② 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平 孝，“無線秘密鍵生成共有方式用 USB スティック型エスパアンテナ”電子情報通信学会論文誌 B，査読有，Vol.J96-B，No.9，pp. 1057-1066，2013，http://search.ieice.org/bin/summary.php?id=j96-b_9_1057&category=B&year=2013&lang=J&abst=.

〔学会発表〕（計　８件）

① Yosuke Omori, Naoki Sakai, and Takashi Ohira, “Active Tapping Scheme to Wireless Secret Key Generator Employing Duplex Amplifying Repeater,” Proc. 8th European Conference on Antennas and Propagation (EuCAP 2014), 6-11 April 2014, Hague, The Netherlands.
② Tadafumi Yoshida, Yosuke Omori, Naoki Sakai, Takashi Ohira, “Imac Enhancement Exploiting the Eigen- value of Radio Wave Fluctuation in Secret Key Agreement System,” 2013 Asia-Pacific Radio Science Conference (APRASC’13), 3-7 Sep. 2013, Taipei, Taiwan.



（a）従来の盗聴法（○：正規局）



（b）能動的盗聴法（□：能動的盗聴端末）

図３　電波ゆらぎ方式の秘匿性マップ（黒いエリアに盗聴局を配置すると鍵が傍受される．）

③ 坂井尚貴，小田康明，ウリントヤ，上原秀幸，大平 孝，“無線秘密鍵生成共有方式の秘匿性を高める可変指向性アンテナ指向性多様性指標の提案，”アンテナ・伝搬研究会，2013 年 1 月 15 日，宮崎．
④ 大森陽介，吉田斉史，坂井尚貴，上原秀幸，大平 孝，“無線秘密鍵共有方式において両端末ともにエスパアンテナを用いることによる盗聴耐性向上”，マイクロ波研究会，2012 年 10 月 18 日，栃木．
⑤ Tadafumi Yoshida, Takafumi Saito, Katsuhiro Fujiki, Kazumasa Uematsu, Hideyuki Uehara, and Takashi Ohira, “Impact of Direct-Path Wave on Imac in Secret Key Agreement System Using ESPAR Antennas”, URSI General Assembly,URSI-GA 2011, 13-20 Aug. 2011, Istanbul, Turkey.

〔図書〕（計　0件）

〔産業財産権〕
○出願状況（計１件）

名称：管理局，無線秘密鍵管理システム及びその方法
発明者：大平孝，坂井尚貴，藤木雄大，斎藤隆史，吉田斉史
権利者：同上
種類：特許
番号：特許出願 2011-203862
出願年月日：2011 年 9 月 16 日
国内外の別：国内

〔その他〕
① イノベーションジャパン 2011 に出展，東京国際フォーラム,2011 年 9 月 21 日-22 日．
② CEATEC 2011 に出展,幕張メッセ,2011 年 10 月 4 日-5 日．
③ Microwave Workshop and Exhibition 2011 に出展,パシフィコ横浜,2011 年 11 月 30 日-12 月 2 日

６．研究組織
(1)研究代表者
大平　孝　（OHIRA, Takashi）
豊橋技術科学大学・工学研究科・教授
研究者番号：30395066

(2)研究分担者
上原　秀幸（UEHARA, Hideyuki）
豊橋技術科学大学・工学研究科・教授
研究者番号： 00293754