様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 3 月 25 日現在

機関番号：13904
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：20560354
研究課題名（和文）
電波の相反性を用いた秘密鍵共有方式の研究
研究課題名（英文） A Study on Secret Key Sharing Based on Radio Reciprocity

研究代表者
大平 孝（OHIRA TAKASHI）
豊橋技術科学大学・大学院工学研究科・教授
研究者番号：30395066

研究成果の概要（和文）：個人情報など第３者に秘匿とすべき情報を無線で通信する際に有効となる秘密鍵を通信の相手方と共用する方法について理論的および実験的研究を行った。少ない電波のやり取りでできるだけ効率的に安全な鍵を共有するためには、盗聴者が近傍に存在すると想定し、盗聴者が推定する鍵と正規の相手が共有する鍵の相関を低減することがポイントである。本研究ではこの相関を低減できる新しいアンテナ構成と信号処理方式を発明し、実験によりこれを実証した。

研究成果の概要（英文）：This project worked on how to share a secret key between communication parties. To enhance the security, we assumed an eavesdropper located nearby and estimate correlation between the keys generated in the eavesdropper and in regular terminals. We proposed a new technique on smart antenna structure and signal processing procedure that can reduce such correlation. We also carried out an experiment where the concept was successfully proved.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
2008 年度	2,500,000	750,000	3,250,000
2009 年度	900,000	270,000	1,170,000
2010 年度	400,000	120,000	520,000
年度			
年度			
総 計	3,800,000	1,140,000	4,940,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信ネットワーク工学
キーワード：暗号、セキュリティ、電波、ゆらぎ、相反定理、秘密鍵

１．研究開始当初の背景

携帯メールやワイヤレス LAN の普及に伴い、だれもが電波を介してデータ情報交換や電子商取引をする機会が急増してきた。無線はどこでも使えて便利なので今後益々利用者シーンの広がりが期待できる。一方で、個人情報保護や企業コンプライアンスが安心安全社会のための必須ファクタとなってきている。電波は目に見えないため原理的に常に盗聴の危険にさらされている。電波はあらゆる空間へ伝搬するので盗聴されているかどうかを確認すること自体も至難である。一般に、デジタル情報のセキュリティを確保するには暗号化が有効である。実際、多くの市販パソコンには無線 LAN が内蔵されており、暗号化のソフトウェアがデフォルトでインストールされている。暗号通信を行うためには通信の相手方と「鍵」を共有する必要がある。現在用いら

れている鍵の方式には大きく分類して「秘密鍵方式」と「公開鍵方式」がある。秘密鍵は通信の相手方と暗号と復号に共通する鍵を保有し、それを第３者に一切開示しない方式である。すなわち「情報量的に」安全を保証する。これに対し、公開鍵は暗号鍵だけを公開し、そこから第３者は復号鍵を推定できないだろうという方式である。すなわち「計算量的」に安全を保障する。計算量的安全性とは具体的には例えば大きな整数の素因数分解は計算に時間がかかるため解けないだろうということをよりどころにしている。桁数を大きくしていけば安全性は増すが、コンピュータの性能向上により盗聴者側の計算能力も増すいわゆるイタチごっこである。つまり、公開鍵方式では、現在盗聴されたデータが何年か後に解読されるという危険性がある。一方、秘密鍵方式は情報量的に安全すなわち鍵情報そのものを開示しないので、第３者の計算能力が向上しても解読されない。秘密鍵方式では、鍵情報を第３者に漏洩することなくどうやって所望の相手方だけと共有するかが技術的課題ポイントである。最も単純な方法として、鍵情報を紙やカード媒体で相手方に手渡しするという方法があるが、原始的な方法であるためリアルタイム更新できず発展性に乏しい。最先端の光ファイバ通信分野で最近研究されている量子暗号も一種の秘密鍵であり情報量的安全性を目指す革新的試みであるが、フォトンを粒子として扱うハードウェアが必要であるため現状では非常に高価な装置となるという背景があった。

２．研究の目的

本方式を実現するための技術課題は、１）可変指向性アンテナの小型軽量化、２）秘匿性の高い電波ゆらぎの発生方法、３）ゆらぎから秘密鍵を生成するアルゴリズム、である。

１）可変指向性アンテナの小型化については既に研究が進んでおり、直径１波長の円筒アレーアンテナを無線 LAN の親機側に搭載する実験が報告されている。本研究では民生応用に鑑みアンテナの平面化を目指した。一般に平面アレーは立体構成に比べて素子配置形状が制限される。それゆえ電波の空間的ゆらぎの不規則性の自由度が低下し、生成できる最大有効鍵長が短くなってしまう。そこで、平面型可変指向性アンテナを端末側にも搭載することを考えた。これにより上下リンクともに送・受両方の指向性が可変となり、空間ゆらぎの自由度が格段に高くできる。このためにはアンテナの形状はノート PC に搭載できる程度の小型化が必要となる。本研究では、USB スティックメモリサイズの平面型可変指向性アンテナの開発を目的とした。

３．研究の方法

本研究では、情報量的に安全を保証する全く新しい第３の方法として「電波の空間的ゆらぎ」で鍵を生成するアプローチをとる。電波ゆらぎによる秘密鍵の基本アイデアは１９９０年代に提案された。電波にゆらぎを与えるハードウェア手段として、近年、簡易で低消費電力な可変指向性アンテナが開発されたことによりこの方式の現実性が増してきた。１）離れた場所同士で同一鍵を共有できる、２）鍵情報を電波に乗せない、３）高価なハードウェアを用いないという３点が本方式の特長である。これらの特長を活かせるようにアンテナの構成法ならびに無線信号処理方式を理論的に構築し、さらにそれを実験的に実証するという方法で研究を行った。

４．研究成果

初年度は原理的な実験を行った。可変指向性アンテナをスティックメモリサイズにまで小型化するための設計手法を確立するための具体的基本構造として、半波長ダイポールを３本平行に配置した。これに指向性可変機能を付加するため、中央素子に給電ポート、両側パラサイト２素子にバラクタを装荷した。バラクタに直流バイアス電圧を印加することにより指向性を制御する装置を試作した。指向性可変機能を高く維持したまま素子長と素子間隔を如何に小さくできるかの限界を極めるため、モーメント法により素子間電磁結合アドミタンス行列を数値的に求め、これに基づいて等価ウェイトベクトル法により放射指向性の可変パタンを算出した。振幅および位相指向性の空間相関を指標として、アンテナサイズの下限を１２分の１波長と決定した。この結果が正しいかどうか確認するためにプリント基板と銅線で製作したブレッドボードモデルで実験を行った。鍵生成するための十分なゆらぎが様々な環境において得られるかどうかを理論的ならびに実験的に調べた。上述の指向性計算結果を用いて、直接波およびマルチパス反射波によって生じる受信点でのゆらぎをレイトレース法により推定した。どのようなアンテナの構造パラメータおよびバラクタ電圧でどのようなゆらぎが得られるかをコンピュータシミュレーションで探った。これを種々の環境において繰り返し計算することによりゆらぎを統計的に評価した。ブレッドボードモデル２セットを離れた場所に設置し相互に送受を切り替えて実空間での鍵生

成実験を実施し、２地点間での電波ゆらぎ特性ならびに鍵一致率を実測することに成功した。これらにより得られた知見に基づきバラクタ電圧制御法を発明し特許として出願した。

次年度は鍵共有の性能向上を目指した実験を行った。一般に秘密鍵を生成し相手方と共有する際には正規局間の鍵一致率に加えて、第３者に対する耐盗聴性の確保が必須である。２つの正規端末と１つの盗聴端末が典型的なオフィスルームである８m×１０mの長方形空間にあるとして、シミュレーション実験を行った。部屋の中のランダムな位置に上記２つの正規端末を配置、第３の端末は盗聴に最も有利と考えられる位置（２つの正規端末を結ぶ直線上）に配置し、盗聴者は鍵生成のアルゴリズムを完全に知っているもの仮定した。このような条件で正規端末間で鍵生成を行っている状態において、盗聴端末を常に受信モードに設定して正規局で生成される鍵と盗聴局で生成される鍵の相互相関係数を評価した。正規局と盗聴局の場所を様々に変えてこの相互相関係数の評価を何度も繰り返していたところ、稀にある特異な現象があることを発見的に気づいた。最初はなんらかの計算誤差ではないかと疑ったが、同じ評価を場所を変えて実施してみたところ確率的に再現された。これは相互相関係数が平均的な値に比べて明らかに低い値となる場所があることを意味している。さらに繰り返して評価していくうちに、この現象は正規局間を直接到達する電波の強度が一旦壁に反射して到達する電波に比べて低い場合に発生するということがわかってきた。つまり、電波が相手端末に直接届かないような場合に盗聴耐性が向上することになる。そこで、このような環境をあえて設定しシミュレーション実験を再実施し統計的に相関係数を評価したたところ見事に優位さが現れた。これは反射を低減した方が良いという通常の無線通信の常識とは全く相反するものである。この発見にもとづき、正規局間でアンテナの偏波方向をあえて直交させる配置とする秘密鍵生成方式およびその装置を特許出願するに至った。

最終年度は本方式の総合実験段階に入った。ハードウェアとしては前年度までに試作したスティックタイプのアンテナ内蔵無線送受信回路およびこれを装荷したノートパソコンを複数台セットで用いた。実験環境として、大学の電波暗室での実験に加えてオフィスの実環境条件で所望の鍵長を有する鍵生成共有ができるかどうか試験を行った。実験場所が異なると、電波の伝播状態や反射物のレイアウト、さらには人体などの動きが様々である。上りリンクと下りリンクのわずかな時間差の間に環境が変化する可能性もある。その場合は電波伝播の相反性が成立しなくなる。さらには、実際の生活環境においては電子レンジや他の無線機器からの電波干渉が発生することも考えられる。鍵の生成に失敗した場合は、基本的にはリトライの繰り返しをすることになり、実際問題としては成功するまでの時間がかかってしまうことが懸念される。そこで本実験では、あらゆる環境下においてリアルタイムに鍵生成に成功するために、アナログ量である電波ゆらぎをデジタル信号に変換する際の信号量子化および得られたデジタル信号から「鍵」を生成するための信号処理アルゴリズムに工夫を施した。具体的には、電波ゆらぎの統計的性質を把握し、量子化における閾値付近のゆらぎを削除するというアイデアを実験で実証した。これにより盗聴耐性を高めるプライバシ増幅が確認できた。さらに、正規局と盗聴局の相関の大きな要因が直接波伝播であることを発見し、これを抑圧する複数の手法を実証実験した。得られた成果を国内公開研究会や招待講演を含む国際会議で発表した。学会論文誌に投稿し採択掲載された。これら業績一覧を大学ホームページにてインタネット上に公開した。

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１件）

[1] 長谷川拓，斎藤隆史，植松和正，成田譲二，上原秀幸，大平 孝，“エスパアンテナを用いた秘密鍵生成共有方式の雑音耐性と盗聴耐性を高める指向性選択，”電子情報通信学会論文誌 B，Vol.J94-B，No.2，pp.214-225，Feb. 2011，査読有.

〔学会発表〕（計 16 件）

[1]植松和正，斎藤隆史，上原秀幸，大平孝，“エスパアンテナを用いた無線秘密鍵生成システムの実証実験，” 電子情報通信学会技術報告，AP2010-186，pp. 77-82，2011-03.

[2] 森 翔太，菊池祐樹，高谷侑希，タンソパンナー，坂井尚貴，上原秀幸，大平孝，″2 素子エスパアンテナの指向性可変性能の素子長・素子間隔依存性″，AP2010-111，pp. 113-118，2010-11.

[3] Takafumi SAITO, Kazumasa UEMATSU, Taku HASEGAWA, Hideyuki UEHARA, and Takashi OHIRA, “A New Scheme for Anti-Tapping

Tolerance Enhancement inWireless Secret Key Generator Utilizing Horizontally-Polarized ESPAR Antennas," 2010 Asia-Pasific Radio Science Conference (AP-RASC'10), CBDEFK1-4, Toyama, Japan, Sep. 2010.

[4] Takashi OHIRA, "Maxwellian approach to secret key generation (invited as keynote)", Indonesia-Malaysia Microwave Antenna Conference, IMMAC2010, Plenary Session, Depok, June 2010.

[5] 森翔太, 菊池祐樹, タンソパンナー, 坂井尚貴, 上原秀幸, 大平 孝, "平行平板エスパアンテナの指向性可変特性", 電子情報通信学会技術報告, MW2010-26, pp.1-6, 2010-06.

[6] Naoki SAKAI, Hideyuki UEHARA, and Takashi OHIRA, "Variable Beamforming Characterization of a 3-Element Dipole ESPAR Antenna from a Complexity-of-Directivity Viewpoint," Asia-Pacific Microwave Conference 2009 (APMC2009), Suntec City, Singapore, Dec. 2009.

[7] 坂井尚貴, 三谷友彦, 上原秀幸, 大平孝, "3素子エスパアンテナの水平面内指向性の測定およびモーメント法解析", 電子情報通信学会技術報告, SPS2008-23, pp25-30, 2009-03.

[8] 長谷川拓, 成田譲二, 上原秀幸, 大平孝, "エスパアンテナを用いた秘密鍵共有システムにおいて秘匿条件付相互情報量 Imac を高めるための指向性セット選択法", 電子情報通信学会技術報告, SIP2008-124～163, pp161-166, 2009-01.

[9] 坂井尚貴, 上原秀幸, 大平 孝, "3 素子エスパアンテナの試作と性能評価実験", 電子情報通信学会技術報告, AP2008-66, pp165-170, 2008-07.

[10] 坂井尚貴, 上原秀幸, 大平 孝, "平面エスパアンテナが張ることができる複素指向性空間の次元数", 電子情報通信学会技術報告, AP2008-33, pp23-28, 2008-06.

[11] 長谷川拓, 成田譲二, 上原秀幸, 大平孝, "両端末に 3 素子エスパアンテナを用いた秘密鍵共有システムにおける秘匿条件付き相互情報量", 電子情報通信学会技術報告, RCS2008-3, pp13-18, 2008-05.

〔産業財産権〕
○出願状況（計２件）

[1]
名称：秘密鍵共有通信システム及び通信方法
発明者：大平 孝、成田譲二、長谷川拓
権利者：豊橋技術科学大学
種類：特許
番号：特願 2009-005563
出願年月日：平成２１年１月１４日
国内外の別：国内

[2]
名称：秘密鍵生成方法及びその装置
発明者：大平 孝、上原秀幸、斎藤隆史、植松和正、長谷川拓
権利者：豊橋技術科学大学
種類：特許
番号：特願 2010-042176
出願年月日：平成２２年２月２６日
国内外の別：国内

〔その他〕
ホームページ等
http://www.comm.ee.tut.ac.jp//we/

６．研究組織
(1)研究代表者
大平 孝（OHIRA TAKASHI）
豊橋技術科学大学・大学院工学研究科・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・大学院工学研究科・准教授
研究者番号：00293754