

豊橋技術科学大学長 殿




平成25年11月20日

審査委員長 上原 秀幸



論文審査及び最終試験の結果報告書

このことについて下記の結果を得ましたので報告いたします。

学位申請者	坂井 尚貴	学籍番号	第 063414 号
申請学位	博士 (工学)	専攻名	電子・情報工学専攻
論文題目	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の研究		
公開審査会の日	平成25年10月21日		
論文審査の期間	平成25年10月10日～平成25年11月20日	論文審査の結果	合格
最終試験の日	平成25年10月21日	最終試験の結果	合格
論文内容の要旨	無線通信における情報暗号化に用いる秘密鍵を第三者に解読されることなく無線回線で相手方と共有する手段として、可変指向性アンテナと電波伝播に対する空間の相反定理を利用する方式がある。本論文は、この方式の秘匿性を高めるための可変指向性アンテナ設計法を確立している。第1章では研究の背景と目的を述べている。第2章ではシステム性能指標となる秘匿性（秘匿条件付相互情報量）の定義と算出方法を述べている。第3章では秘匿性を高めるためにアンテナが持つべき性能を論じ、アンテナ設計のための指標を提案している。第4章ではアンテナ設計指標と秘匿性の関係を調べている。送受素波対応環境モデルおよび長方形部屋環境モデルにおいて電波伝播コンピュータシミュレーションを行い、アンテナ設計指標と秘匿性に高い相関があることを示している。第5章では可変指向性アンテナの例としてエスパアンテナ (Electronically Steerable Parasitic Array Radiator Antenna) の構造と動作原理を述べている。第6章では 2.4GHz 帯3素子エスパアンテナの設計と試作結果を述べている。第7章ではこのアンテナを小型化設計し、ノート型パソコンへ挿入できる USB スティックエスパアンテナを試作および性能測定している。第8章では結論を述べている。		
審査結果の要旨	企業コンプライアンスならびに個人情報保護の観点から、暗号の高性能化が益々重要となる。現在用いられている公開鍵方式は安全性を計算量的に担保しているため、正規局側と盗聴局側の計算機性能の攻防戦となる。本研究で扱う方式は電波のゆらぎという物理現象を用いて安全性を情報量的に担保しようとする新しいアプローチである。申請者は本方式の秘匿性を向上することができる可変指向性アンテナの設計法を確立した。アンテナ指向性の複雑度と多様性を定量的に把握するための指標を提案するとともに、情報の秘匿性とアンテナ性能の関係をコンピュータシミュレーションにより明確化した。申請者が提案する手法に基づいて設計・試作した結果、2.4GHz 帯で動作する可変指向性アンテナ（3素子エスパアンテナ）の開発に成功した。先行研究で報告されているアンテナに比べて同じ性能で1/8の小型化を達成した。これにより可変指向性アンテナをノートパソコンに直接プラグインできる USB スティックサイズに集積できた。これらの研究成果は査読付学術論文2編および査読付国際会議論文2件として採録された。以上により、本論文は博士（工学）の学位論文に相当するものと判定した。		
審査委員	上原 秀幸 	市川 周一 	大平 孝 
	印	印	印

(注) 論文審査の結果及び最終試験の結果は「合格」又は「不合格」の評語で記入すること。