氏名	静谷(しずや)啓樹(ひろき)
授与学位	工学博士
学位授与年月日	昭和62年3月25日
学位授与の根拠法規	学位規則第5条第1項
研究科，専攻の名称	東北大学大学院工学研究科 （博士課程）電気及通信工学専攻
学位論文題目	**擬似ランダム系列の通信分野への応用に関する研究**
指導教官	東北大学教授 高木 相
論文審査委員	東北大学教授 高木 相　東北大学教授 重井 芳治 東北大学教授 斎藤 伸自　東北大学助教授 越後 宏

論文内容要旨

第1章 序論

本論文は擬似ランダム系列（Pseudorandom Sequence）の通信分野への応用を検討するものであり，特に現代の通信系で問題となっているセキュリティ問題の解決に寄与することを目標にしている。

具体的には通信のセキュリティ問題を，雑音・干渉等の物理的要因からの保護問題と傍受・盗用等の人為的要因からの保護問題に大別し，それぞれの問題について擬似ランダム系列の応用による解決手法を提案する。

まず基礎的な議論として，第2章では擬似ランダム系列に関する従来の研究成果を総括し，第3章では擬似ランダム系列を含む全ての系列の相関関数の特性を統一的に表現する新たな手法を与える。

第4章では物理的要因からの保護手法としてスペクトル拡散通信を考え，耐雑音性能の観点から，長周期の擬似ランダム系列を拡散符号として実用化し得る相関器の構成手法を与える。また第5章では通信系の耐雑音性能を測定する際の雑音源を，擬似ランダム系列の応用によって与える。

第6章では人為的要因からの保護手法として公開鍵暗号方式を考え，擬似ランダム系列の理論とリンクする新たな公開鍵暗号のアルゴリズムを与える。

第7章は結論で，本論文を総括している。

第2章　擬似ランダム系列の一般論

擬似ランダム系列の定義を示し，主要な性質と系統的構成法に関する従来の研究成果をまとめた。周期Nの二値周期系列の自己相関関数がゼロシフト点で1，他の点で$-1/N$となるとき，この二値周期系列を擬似ランダム系列という。M系列，平方剰余系列，双子素数系列，H系列，GMW系列の5つが系統的族の全てである。

一方，近年では擬似ランダム系列の定義を厳密に満足しない複素系列をも擬似ランダム系列と呼ぶ曖昧さがあるので，本論文ではこれを拡張擬似ランダム系列とし，新たな系列のクラスを定義した。

第3章　任意系列の相関関数の統一的表現法

擬似ランダム系列で典型的に示されるように，符号系列の相関特性は通信理論上重要な意味をもつが，従来は符号系列の相関関数の表現法が不統一であり，相関特性の共通の評価尺度は存在しなかった。そこで本論文では，あらゆる系列の周期的自己・相互相関関数と非周期的自己・相互相関関数を統一的に表現する「偏角表現法」を提案する。

偏角表現法においては複素数を成分とする符号語同士の相関関数を，まず実部および虚部に分離し，次にこれらを符号語のノルムで正規化したのち，一対の偏角ベクトルに全射する。そして実部に対応する偏角ベクトルの各成分を単位円上に角度で表示し，虚部に対応する偏角ベクトルの各成分は別の単位円上に角度で表示する。すなわち一対の単位円を用いて相関関数を偏角で表現するものである。

相関関数を一対の単位円で表現することにより，相関の程度や直交性をはじめとする符号系の幾何学的構造が直ちに評価できるようになる。さらに，符号長によらず一定の記述面積で相関関数を表現できる点が従来の表現形式にはない利点である。これらの特長は，いくつかの適用例を具体的な数値計算結果とともに示して確認した。

偏角表現法は，単にあらゆる符号語同士の相関関数を表現する手段としてだけでなく，符号系の構造を解析する場合や，所期の相関特性を持つ新しい符号系列を探索する場合に，これを支援する道具として応用しうる表現法である。

第4章　スペクトル拡散通信への応用

スペクトル拡散通信（SS，Spread Spectrum）方式においては，高速の拡散符号を用いて情報を広帯域信号に変調して送信し，受信側では拡散符号を相関検出して復調する。その符号化利得は，多くの場合，拡散符号長をMとして$\log M$に比例するので，大きな符号長の拡散符号を用いるほど耐雑音性能が高くなり，雑音や干渉等の物理的要因からの通信系の保護に寄与する通信方式と考えられる。

拡散符号としては主に擬似ランダム系列が用いられ，耐雑音性能の向上のためには長周期の擬似ランダム系列を選択するのが望ましいことになるが，そのような長周期の擬似ランダム系列を相関検出できるような相関器（トランスバーサルフィルタ）は従来は実現できなかった。本論文ではこ

の問題点を解決するため，「系列分割相関法」による相関器の構成を提案する。これは，短い遅延段数Nのアナログトランスバーサルフィルタをいくつか組合せて大きな符号長M（≫N）の拡散符号に対応可能な相関器を構成する手法である。

系列分割相関法の原理は，相関器の動作を代数的に記述した場合に，小行列を成分とするベクトル同士の内積に帰着できることにある。もとの行列は入力系列（即ち擬似ランダム系列）を巡回置換して各行としたものであり，行列の型に矛盾がなければ小行列への分割のしかたは任意である。これらの考察により，長大な符号長Mの拡散符号を予めいくつかの部分系列（長さ≦N）に分割し，各々の部分系列に対する相関器（トランスバーサルフィルタ）を，トランスバーサル構造になるように配置すれば，全体として符号長Mの拡散符号に対する相関器が構成できることを導いた。即ち，提案手法による相関器は二重のトランスバーサル構造を持つものである。なお，理論どおりの動作をすることは，実験によって確認した。

系列分割相関法により，ＳＳ方式で利用可能な拡散符号長は原理上無制限に大きくできることになり，符号化利得の増大によって耐雑音性能が向上し，物理的要因からの通信系の保護に寄与することが期待される。

第５章　雑音発生器への応用

通信系の耐雑音性能を試験するための雑音源に関し，本論文では擬似ランダム系列を応用した新しい装置を２種提案する。ひとつは「ディジタルガウス雑音発生器」（Ｄ－GAUSS），他方は「ディジタル複合ノイズ発生器」（Ｄ－CNG）である。

Ｄ－GAUSS では，擬似ランダム系列のうち生成ハードウェアが最も単純なM系列を応用している。まず，M系列を発生するシフトレジスタの内容をＤ／Ａ変換し，区間［０，１］の一様ランダム雑音を生成する。この出力を確率変数Xで表したとき，独立な多数のXの和：$Y = X_1 + \cdots + X_m$を考えると，X_i（$1 \leqq i \leqq m$）およびYはLindebergの条件を満足するために中心極限定理が適用でき，Yの分布は平均$\mu = m/2$，分散$\sigma^2 = m/12$の正規分布に近似的に従う。即ちガウス雑音が得られる。$m = 6$として試作した回路では，最大動作速度10MHz，出力の正規性は平均から$\pm 3.5\sigma$の範囲であった。

Ｄ－CNGはＤ－GAUSSを応用して非ガウス性雑音を発生させる回路である。即ち，D－GAUSSの動作クロックと出力の分散・時間長を同時変化させて組合せることにより，任意の振幅確率分布（APD）と平均交叉率（ACR）をもつ非ガウス性雑音を合成し，出力するものである。実際の動作は試作回路により確認した。

Ｄ－GAUSS は従来のガウス雑音発生器に比べて単純な構成でしかも高速動作が可能で，クロックパルスを他の通信機器に同期させて利用できる点で外部からの制御が容易であり，通信系の誤り率測定などにおける安定で再現性の良い雑音源として応用できる。またＤ－CNGは単なる非ガウス性雑音源というよりは，現実に存在する様々な雑音のシミュレータとしての応用に適している。

第6章　公開鍵暗号への応用

傍受や盗用等，通信系を脅かす人為的要因からの保護手法として公開鍵暗号方式を考え，暗号化と安全性に乱数が主要な役割を果たす新しい公開鍵暗号のアルゴリズムを2通り与える。第1の方式は「一般逆行列の非一意性に基づく公開鍵暗号方式」，第2の方式はこれをさらに発展させ，行行の行列ベキ乗演算を導入した「有限体の離散対数領域上の一般逆行列に基づく公開鍵暗号方式」である。一般逆行列の非一意性のみに注目した第1の方式は，公表後に解読アルゴリズムが発表されたが，秘密鍵系としては利用可能である。一方，第2のアルゴリズムは次のように与えられる。

まず，有限体GF(p)(p:素数)と剰余環Z／(p−1)の正則元の集合をそれぞれ$K^{\#}$，$R^{\#}$で表し，ある代数系Aの上のn行m列型行列の全体集合を$M(n, m; A)$で表すことにする。巡回群$K^{\#}$の元は，GF(p)の原始元を固定すれば，原始元のベキ乗によって剰余環Z／(p−1)の元(ベキ)と1対1に対応するので，本論文においてはZ／(p−1)をGF(p)の離散対数領域と呼ぶことにする。また，本論文で定義する行列ベキ乗演算は，$K^{\#}$上の行列B及び離散対数領域上の行列Aに対するものであり，B^{A}(右ベキ乗)，${}^{A}B$(左ベキ乗)などと表現される。なお，暗号系構成の都合上，素数pは充分大きく，10進級で100〜200桁程度とする。

さて，非正方行列$A \in M(n, m; Z/(p-1))(m > n)$のn次小行列式で$R^{\#}$に属するものが存在すれば$AA^{-} = I_n$を満足する一般逆行列$A^{-}$が存在することが導けるので，相異なる一般逆行列を$\Omega$，$\Omega'$とする。次に乱数を成分とする行列$R \in M(m, m; K^{\#})$を用いて，$\Lambda = (I_m - \Omega' A)R \in M(m, m; K^{\#})$を生成する。以上により，公開暗号化鍵を$\Omega$，$\Lambda$，pとし，$\Omega'$，R，Aを秘匿鍵とする。

平文を成分とする行列を$M \in M(n, n; K^{\#})$，乱数を成分とする行列を$N \in M(m, n; Z/(p-1))$としたとき，暗号化行列Xは$X = {}^{\Omega}M \otimes \Lambda^{N} \in M(m, n; K^{\#})$で与えられる。

復号化は，暗号行列Xに対して秘密の鍵Aを用いて，Xを左からA乗(即ち${}^{A}X$)すればよい。

本暗号の解読の困難さは素体上の離散対数問題の困難さで見積られる。その解読のための時間計算量は，素数pと同程度の大きさの合成数を素因数分解する計算量と同程度であることが示される。また，暗号化と安全性には乱数が深く関与しており，暗号用擬似ランダム系列の理論とリンクした方式でもある。本暗号を現実的時間内で解読するアルゴリズムは現在なお発見されていない。

第7章　結　　論

本論文では擬似ランダム系列に関する基礎的な議論を行った後に，通信系のセキュリティ問題の解決を目標とした応用を検討した。その結果を総括すれば，雑音・干渉等の物理的要因と傍受・盗用等の人為的要因の双方から現代の通信系を保護する手法として，スペクトル拡散通信方式と公開鍵暗号方式の併用というひとつのモデルが提案されたことになる。セキュリティ問題という視座からこのモデルを総合的に評価する作業が今後の課題と考えられる。

審　査　結　果　の　要　旨

高度情報化社会を迎えて，通信の役割は益々重要となっている。近年とくに通信情報の保護問題，いわゆる情報セキュリティ問題の重要性が叫ばれている。著者はこの問題に対して，通信系の耐雑音性向上のためのスペクトル拡散通信方式（SS方式）と情報セキュリティ向上のための公開鍵暗号系に，擬似ランダム系（PRS）を応用することを試み，有用な多くの提案を行った。本論文は，その成果をとりまとめたもので，全編7章よりなる。

第1章は序論である。次いで第2章では，PRSの定義，系統的な構成法など，従来の知見をとりまとめている。

第3章では，とくに，SS方式において重要な，符号の相関特性の統一的な表現法として，偏角表現法なる新しい表現法を提案している。これにより，従来不便であった，長い符号の相関関数の数値的評価が極めて容易となり，符号の選択が容易にできるようになった。これは有用な結果である。

第4章では，PRSのSS方式への応用について述べている。SS方式は使用するPRSの符号長が大きいことが耐雑音性の上から必要であるが，長符号の相関演算を高速で行う相関器は得難いのが現状である。著者はここで，系列分割相関法なる新しい相関演算法を発案した。これは短い符号長の相関器を組み合わせることによって実現でき，CCD相関器を用いてその効果を確かめている。

第5章では，通信系の耐雑音性の評価，あるいは，第6章で提案する乱数を用いた公開鍵暗号系などに用いる雑音源の構成と実験結果について述べている。すなわちM系列符号を多重に用いた，中心極限定理に基づくガウス雑音発生器と，これを用いた複合雑音発生器を実現している。これにより，振幅確率分布と発生頻度が任意に設定でき，また平均交差率も可変な雑音源を得ている。これは新しい雑音発生器である。

第6章では，乱数を用いるが，送受間で乱数を共有しない，公開鋳暗号方式を2つ提案している。そのひとつは，一般逆行列の非一意性を用いたものであり，他のひとつは，これを改良したもので，一般逆行列の非一意性に加えて，新しく，行列の行列べき乗演算法を定義することにより，離散対数問題を加えたものである。

第7章は結論である。

以上要するに本論文は，いわゆる情報セキュリティ問題に擬似ランダム系列を応用することを試み，スペクトル拡散通信方式における新しい相関器の提案と暗号系における新しい公開鍵暗号方式の提案，その他符号間相関特性の新しい表現法，新しい雑音発生器の提案など行ったもので，通信工学の発展に寄与するところが少なくない。

よって，本論文は工学博士の学位論文として合格と認める。