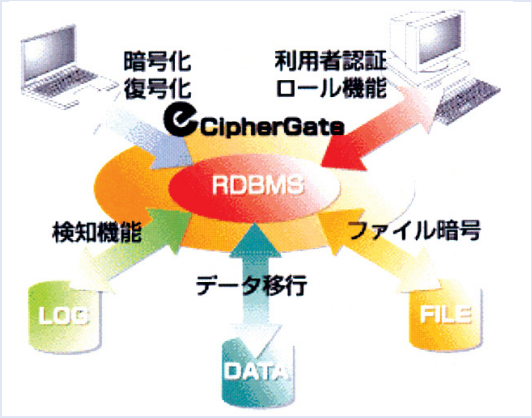
特許第3030341号

ランダムなベクトル列の出力装置、出力方法、および、情報記録媒体

発明者
梅野　健



eCipherGate

技術の概要

従来、乱数を得るために、ある決まった漸化式を用いて１次元の乱数列を得る手法が一般的に用いられていました。最近、乱数を用いるアプリケーションとしては、１回限りの乱数列を必要とするだけではなく、同時に複数の互いに独立な乱数列を必要とされるものが増えてきました。これは、従来方法がこの新たなニーズに対しては適当ではなく、従来方法とは異なる新しいタイプの乱数生成器、すなわち、すべての成分が互いに独立な乱数列である乱数ベクトル列の生成が必要であることを意味します。このような乱数生成器は、画像等の情報量の多いデータを一度に暗号化するといったアプリケーションに特に必要とされます。本発明は、このようなネットワークのブロードバンド化に対応する高いバンド幅を持つ乱数列生成列を可能にするものです。図１は、本発明が生成するランダムなベクトル列を生成するフローチャートを示しています。本発明は、任意次元のランダムなベクトル列発生を初めて可能にする基本的技術を提供し、画像の暗号化、多次元データベースの暗号化、モンテカルロ法、マルチキャリアCDMAにおけるスクランブリング符号、公開鍵暗号システムの初期鍵生成などで利用することができます。

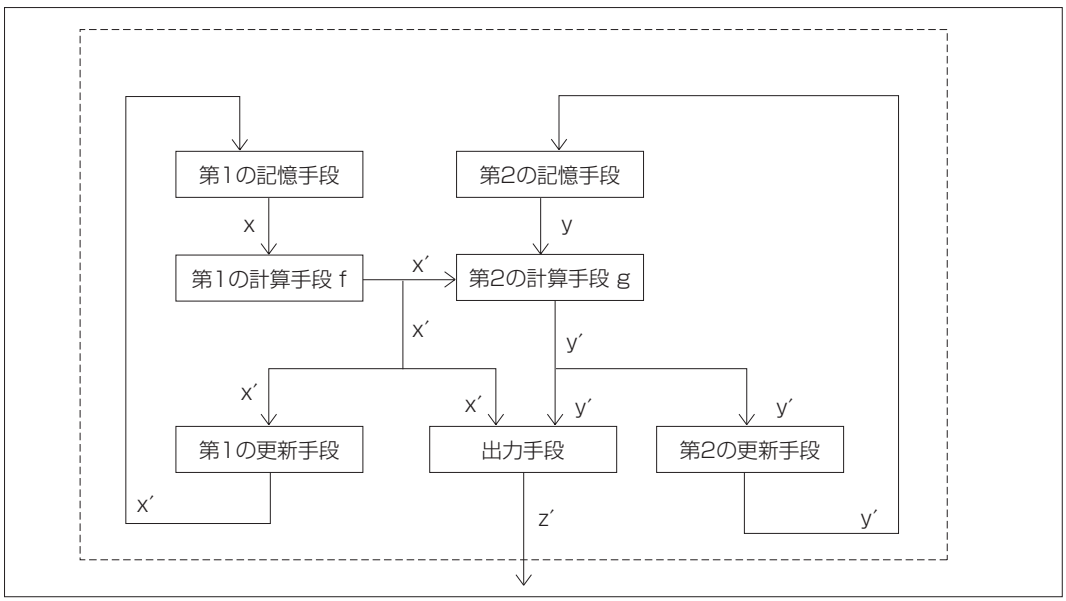


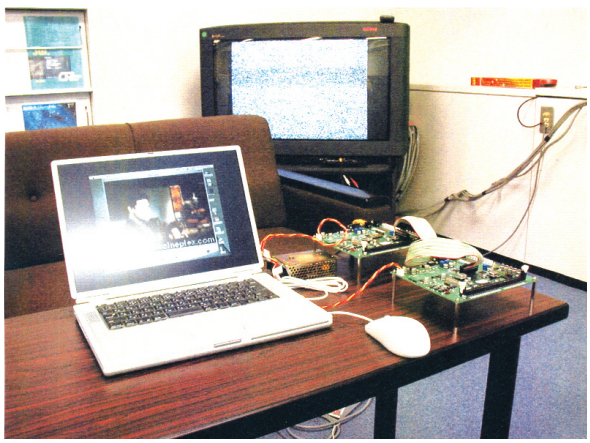
図1

研究者自ら製品化へ

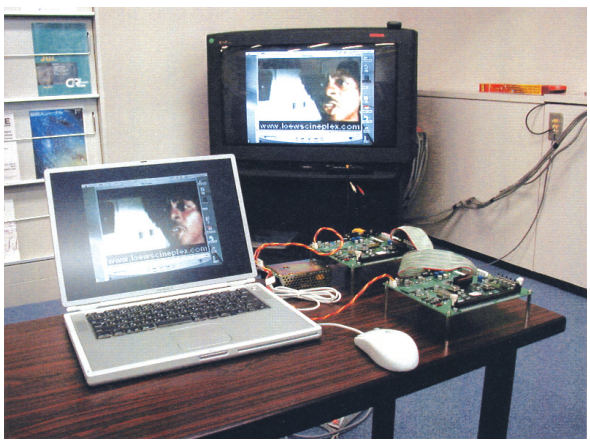
この特許は、昨年度から始まった所内起業支援策「プレベンチャー制度」で行われている課題「カオス暗号チップの研究開発」のベクターストリーム暗号（Vector Stream Cipher）という新しい暗号アルゴリズム（＝ベクター・ストリーム暗号）の基本アーキテクチャを与えるものです。CRLのプレベンチャー制度とは、自分の研究成果の起業化を支援する制度で、起業化直前までのプロトタイプの開発や実証実験をCRLにおける自分の業務として専念することができるというもので、このベクターストリーム暗号のチップ化も本プレベンチャー制度の下で行われております。現在、回路が書き替え可能なLSIチップであるFPGA（Field Programming Gate Array）を用いたカオス暗号チップのプロトタイプが完成し、ビデオ信号等の動画を1Gbpsといった非常に速い処理速度でリアルタイムに暗号化・復号化することができます。この場合、図1にあるようなランダムなベクトル列の発生アルゴリズムは、容易に並列化でき、パイプライン処理に適しているので、チップ化することで非常に高速化することができます。

ベンチャー企業への技術移転

本特許を用いたベクターストリーム暗号は、世界で初めてデータベースの部分暗号化を行うeCipherGateとして、開発元のジャパン・インフォーメーション・テクノロジー株式会社と2000年5月に本特許のライセンス契約をすることで、2002年春に製品化されました。現在同製品は、伊藤忠テクノサイエンス株式会社等5社の販売会社を通して、2002年上半期で6本納品され、大手製薬会社の開発データの暗号化等、実際に運用されています。今後、住基ネット、金融データ、医療データ等、データベースの部分暗号化等による現代社会の基幹システムの安全性向上に、本特許が利用できます。



暗号化したビデオ信号



復号化したビデオ画像

図2　カオス暗号チップによるビデオ信号暗号化

CRLの取得した特許は有償で利用できます。
これらの特許権の実施及び技術情報についてのお問い合わせは
通信総合研究所 企画部研究連携室 知的財産グループ
Tel. 042-327-7464　E-mail: ip@ml.crl.go.jp
までお願いいたします。