擬似乱数生成・管理方法（特願２００８－２１３３０５）

本願の発明は認証、識別用ＩＤ、パスワード（ＰＷ）のような、限られた長さ（例えば１２８ビット）の乱数を生成・管理する方法である。

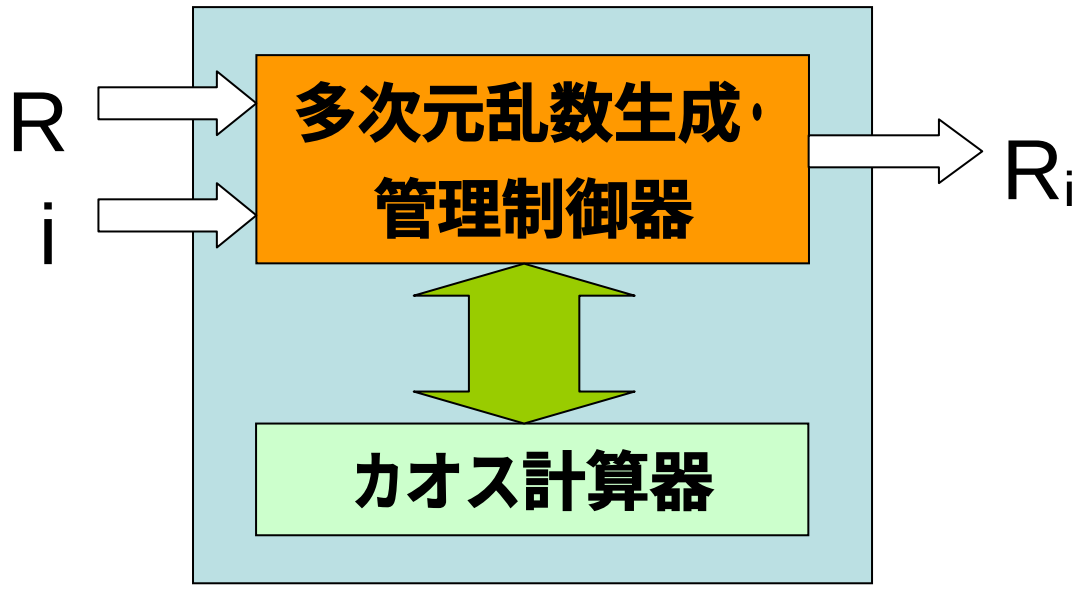
①必要性と現状

コンピュータシミュレーションのような短い時間で大量な乱数を消費する場合もあれば、認証、識別用ＩＤ、パスワード（ＰＷ）のような、限られた長さ（例えば128 ビット）の乱数を生成する場合もある。ＩＤ、ＰＷのような数列は強いセキュリティーの元で管理される必要があるとされるが、現状では装置による有効な管理方法に関する報告はあまりない。顧客のＩＤなどの情報を保存した記録媒体を紛失したような報道がときおり聴かされる。　ＩＤ、ＰＷのような乱数列の管理は難しく、現状ではメモリに保存する方法しかない。

②原理

擬似乱数は再生可能である。シミュレーションで再び同じ乱数を必要となったとき、その乱数を生成するときの初期値（seed）を保存していれば、同じ乱数の生成は可能である。即ち、この長い乱数列は初期値を管理することにより、管理されていると考えてもよい。

この考え方に基づき、本願が提案する乱数生成・管理方法は、一つのＮビットの２進数列Ｒ(初期値)とＭ（Ｍは１以上の整数）個の規則のある次元座標情報ｉによるＭ個の規則のないＮビットの２進数列R_iを生成・管理できる（図１）



$i=i_1,i_2,\ldots i_K$　R_iはK次元座標空間に配置されている。

図１

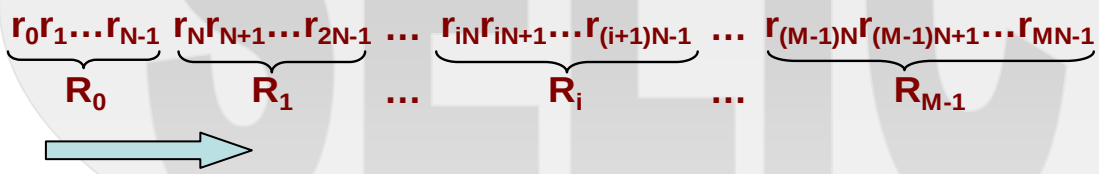
③特徴：多次元乱数生成法とカオス関数の利用

多次元乱数生成

多次元乱数生成法とは：

初期値：R、多次元乱数列のビット長：N、2 値系列の生成速度：S mbps　とする：

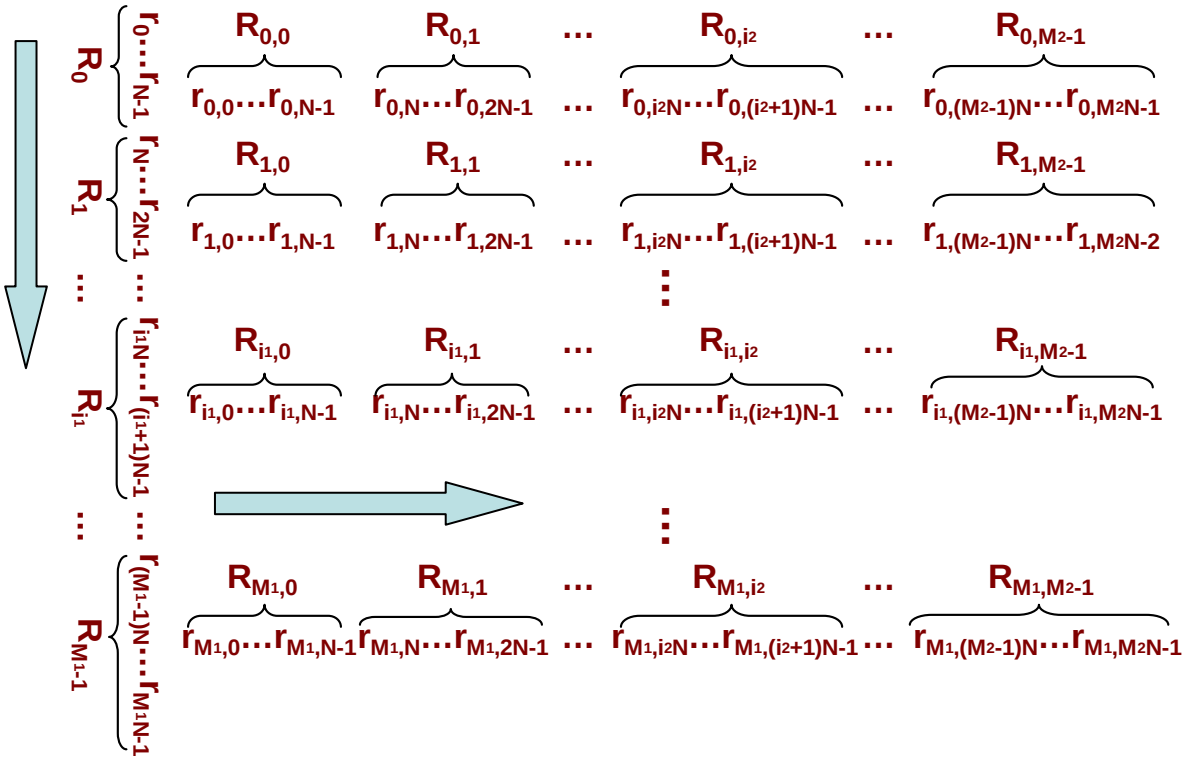
一次元乱数生成：



R_iの生成の所要時間：$T=(N\times(i+1))/S$

i=0,1,…,M-1,　M:1,2,…

二次元乱数生成：



R_i の生成の所要時間：$T=N\times(i_1+i_2+2)/S$

$i=i_1,i_2$,　i_1:0,1,…,M_1-1,　i_2:0,1,…,M_2-1,　M_1,M_2:1,2,…

多（K)次元乱数生成

二次元乱数生成と同じように、K 回初期値の繰り返し生成することは、K 次元乱数生成方法という。

多次元乱数の三要素：

（管理）初期値 R、（管理）次元座標 i、 多次元乱数 R_i

R_i の生成の所要時間：$T=N\times(i_1+\ldots+i_K+K)/S$

次元座標 $i=i_1,i_2,\ldots,i_k,\ldots,i_K$ 、次元数 K(K:1,2,…)、各次元の座標値 i_k(k:1,2,…,K)

次元空間サイズ M、各次元 i_k のサイズ M_k、$M=M_1\times M_2\times\ldots\times M_K$、$i_k$: 0,1,…,M_k-1

Ri の生成に要する最大時間：

一次元のとき： $T=(N\times(M_1\times M_2\times\ldots\times M_K+1))/S$

多次元のとき： $T=(N\times(M_1+M_2+\ldots+M_K+K))/S$

カオス関数の利用

本発明は擬似乱数生成において、関数 $x_{t+1}=4x_t(1-x_t)\qquad(0<x_t<1,\quad t=0,1,2,...)$ を用いた。ロジスティック写像の計算には整数演算による固定小数点演算で計算する手法を用いた。

④効果

本発明の乱数生成において、Rと規則あるｉによるR_i の生成であるが、特定のｉとR_iを用いて、他のR_iを推測することも、Rを推測することもできない性質を持つ。このような性質を持つ乱数生成器は、情報セキュリティーなどの分野で幅広く応用できる。

使い捨て認証（ＩＤ、ＰＷ）システムの構築

本発明の乱数生成法を用いれば、ＩＤ、ＰＷの使い捨てシステムの構築が可能となる。即ち、システム側とユーザー側が持つ秘密な（ＩＤ、ＰＷ）をＲにして、認証を行う度にユーザー側は新しいｉとＲを用いて、R_i（認証用ＩＤ、ＰＷ）を生成し、ｉとR_iをシステム側へ送る。システム側は受け取ったｉと該当ユーザーのＲを用いて、R_iを生成し、送られたものと照合し認証を行う。一つのｉは一度しか使われないため、盗聴されても問題が生じない。秘密なＲ（ＩＤ、ＰＷ）は通信路上など、外へ出すことはないため、安全である。Ｒは身体から採取した情報（指紋、静脈など）などを使えば記憶する必要もない。

暗号鍵生成・管理システムに応用：使い捨て鍵暗号方式の実現

本発明の乱数生成法を暗号システムの暗号鍵生成・管理システムに応用すると、最も強い暗号と言われる使い捨て鍵暗号方式が実現可能となる。次元座標情報ｉを使い捨て（一度しか使わない）によって、同じ暗号鍵が使われることはない。

使い捨て鍵の暗号化通信

本発明の乱数生成法を共通鍵暗号化通信に応用すると、同じ秘密鍵Ｒを持つ者の間に、使い捨て鍵の暗号化通信ができる。情報を送る度に、Ｒと新しいｉにより暗号鍵R_iを生成し、情報を暗号化する。暗号化した情報とｉを相手に送るだけで、Ｒを送る必要はない。暗号化した情報とｉを受け取った相手側は、持っているＲとｉでR_iを生成し、暗号化した情報を復号する。Ｒは通信路上に出ないから、安全である。

各種「性能―コスト」の組合せを持ち、幅広い産業分野への応用が可能

本発明は乱数の生成において、ロジスティック写像を固定小数点演算で行うため、整数を用いた計算で実行できる。整数の分割計算が容易であるから、異なるシステム（汎用計算機（各種のＯＳ）、専用ハードウェア、マイクロコンピュータなど）であっても、最も基本的な整数演算（加算、乗算、ビットシフト、ビットごとの論理演算）ができるのであれば、同じ入力による同じ出力が得られる。そして、集積回路化も容易に実現でき、更なる高速化も容易である。従って、本発明の乱数生成装置は様々なニーズに対応できる「性能―コスト」の組合せを持ち、拡張性も富み、セキュリティー分野を中心とする幅広い産業の分野での応用が可能である。

R_iの生成速度の一例

i(i1,…,i14)	t（秒）
0,…,0(最小値)	0.000421
4,D,4,3,2,C,4,4,3,0,A,7,7,B	0.002781
F,…,F(最大値)	0.006234

(Genuine Intel(R) CPU 1.5GHz 0.99GB RAM)

⑤応用システム例

- **認証（ID・パスワード）**：認証コードの使い捨て
  電子鍵（IC カード、磁気カード、リモコン）
  ネット取引、電子マネー
  IC タグ
- **暗号鍵生成・管理**
  使い捨て暗号鍵
- **製品管理・確認**
  予測できない製品 ID（コピー製品の検出・排除）