【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成20年6月5日(2008.6.5)

【公開番号】特開2007-41199(P2007-41199A)
【公開日】平成19年2月15日(2007.2.15)
【年通号数】公開・登録公報2007-006
【出願番号】特願2005-223999(P2005-223999)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ
Ｇ０６Ｆ　12/14　５１０Ｆ
Ｇ０６Ｆ　12/14　５４０Ａ

【手続補正書】
【提出日】平成20年4月21日(2008.4.21)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
元データを所望の処理単位ビット長に基づいて４以上の分割数の分割データに分割するデータ分割装置であって、
元データを処理単位ビット長毎に区分けして、複数の元部分データを生成する元部分データ生成手段と、
この複数の元部分データの各々に対応して、元データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成する乱数生成手段と、
各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成する分割部分データ生成手段と、
所望の分割数の分割データを複数の分割部分データから生成することにより、各分割データのみからでは元データを復元不能であるが、生成した分割データのうちの所定の個数の分割データから元データが復元可能であるように、かつ、いずれかの分割データのみを用いてそれを構成する分割部分データ間の排他的論理和を行うことによって乱数成分が失われないようにする分割データ生成手段と、
を有することを特徴とするデータ分割装置。
【請求項２】
元データを所望の処理単位ビット長に基づいて４以上の分割数の分割データに分割するデータ分割装置であって、
元データを処理単位ビット長毎に区分けして、複数の元部分データを生成する元部分データ生成手段と、
この複数の元部分データの各々に対応して、元データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成する乱数生成手段と、
各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成する分割部分データ生成手段と、

所望の分割数の分割データを複数の分割部分データから生成することにより、各分割データのみからでは元データを復元不能であるが、生成した分割データのうちの所定の個数の分割データから元データが復元可能であるようにする分割データ生成手段と、を有し、

前記分割部分データ生成手段は、いずれかの分割データのみを用いてそれを構成する分割部分データ間の排他的論理和を行うことによって乱数成分が失われないように、当該各分割部分データをそれぞれに対応する他の分割データにおける各分割部分データと入れ替えることを特徴とするデータ分割装置。

【請求項３】

前記分割部分データ生成手段は、分割部分データの生成に際し、元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれS,R,D,nおよびbで表すとともに、変数としてi(=1～n)およびj(=1～n-1)を用いて複数(n-1)個の元部分データ、複数(n-1)個の乱数部分データ、複数(n)個の分割データおよび各分割データの複数(n-1)個の分割部分データのそれぞれのうちの１つをそれぞれS(j),R(j),D(i)およびD(i,j)で表わし、変数jを１からn-1まで変えて、各元部分データS(j)を元データSのb×(j-1)+1ビット目からbビット分のデータとして作成し、U[n,n]を

ｎ×n行列でi行j列の値u(i,j)が

i+j≦n+1 のとき u(i,j)=1

i+j＞n+1 のとき u(i,j)=0

である行列とし、P[n,n]をn×n行列でi行j列の値p(i,j)が

j=i+1 のとき p(i,j)=1

i=n,j=1 のとき p(i,j)=1

上記以外のとき p(i,j)=0

である行列としたとき、c(j,i,k)を(n-1)×(n-1)行列であるU[n-1,n-1]×P[n-1,n-1]＾(j-1)のi行k列の値と定義し、ただしU[n-1,n-1]×P[n-1,n-1]＾(j-1)とは行列U[n-1,n-1]とj-1個のP[n-1,n-1]の積を表し、Q(j,i,k)をc(j,i,k)=1のとき、Q(j,i,k)=R(k)、c(j,i,k)=0のとき、Q(j,i,k)=0 と定義したとき、各分割部分データD(i,j)を、変数iを１からnまで変えながら各変数iにおいて変数jを１からn-1まで変え、排他的論理和の演算子＊を用いて、i<nのとき、

【数１】

$$D(i,j) = S(j)*\left(\prod_{k=1}^{n-1} Q(j,i,k)\right)$$

ただし、

【数２】

$$\prod_{k=1}^{n-1} Q(j,i,k) = Q(j,i,1)*Q(j,i,2)*\cdots\cdots*Q(j,i,n-1)$$

とし、i=nのとき、

D(i,j)=R(j)

として生成するものであって、当該各分割部分データのうちD(1,j)を削除することを特徴とする請求項２記載のデータ分割装置。

【請求項４】

元データを所望の処理単位ビット長に基づいて４以上の分割数の分割データに分割するデータ分割方法であって、

元データを処理単位ビット長毎に区分けして、複数の元部分データを生成し、

この複数の元部分データの各々に対応して、元データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成し、

各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成し、

いずれかの分割データのみを用いてそれを構成する分割部分データ間の排他的論理和を

行うことによって乱数成分が失われないように、当該各分割部分データをそれぞれに対応する他の分割データにおける各分割部分データと入れ替え、
所望の分割数の分割データを複数の分割部分データから生成することにより、各分割データのみから元データを復元不能であるが、生成した分割データのうちの所定の個数の分割データから元データが復元可能であるようにする
ことを特徴とするデータ分割方法。
【請求項５】
元データを所望の処理単位ビット長に基づいて４以上の分割数の分割データに分割するデータ分割用のコンピュータプログラムであって、
元データを処理単位ビット長毎に区分けして、複数の元部分データを生成する処理と、
この複数の元部分データの各々に対応して、元データのビット長と同じまたはこれより短い長さの乱数から処理単位ビット長の複数の乱数部分データを生成する処理と、
各分割データを構成する各分割部分データを元部分データと乱数部分データの排他的論理和によって処理単位ビット長毎に生成する処理と、
いずれかの分割データのみを用いてそれを構成する分割部分データ間の排他的論理和を行うことによって乱数成分が失われないように、当該各分割部分データをそれぞれに対応する他の分割データにおける各分割部分データと入れ替える処理と、
所望の分割数の分割データを複数の分割部分データから生成する処理と、
をコンピュータに実行させることにより、各分割データのみから元データを復元不能であるが、生成した分割データのうちの所定の個数の分割データから元データが復元可能であるようにすることを特徴とするコンピュータプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
上記データ分割装置において、前記分割部分データ生成手段は、分割部分データの生成に際し、元データ、乱数、分割データ、分割数および処理単位ビット長をそれぞれS,R,D,nおよびbで表すとともに、変数としてi(=1～n)およびj(=1～n-1)を用いて複数(n-1)個の元部分データ、複数(n-1)個の乱数部分データ、複数(n)個の分割データおよび各分割データの複数(n-1)個の分割部分データのそれぞれのうちの１つをそれぞれS(j),R(j),D(i)およびD(i,j)で表わし、変数jを１からn-1まで変えて、各元部分データS(j)を元データSのb×(j-1)+1ビット目からbビット分のデータとして作成し、U[n,n]を
ｎ×n行列でi行j列の値u(i,j)がi+j≦n+1 のとき u(i,j)=1
i+j＞n+1 のとき u(i,j)=0
である行列とし、P[n,n]をn×n行列でi行j列の値p(i,j)が
j=i+1 のとき p(i,j)=1
i=n,j=1 のとき p(i,j)=1
上記以外のとき p(i,j)=0
である行列としたとき、c(j,i,k)を(n-1)×(n-1)行列であるU[n-1,n-1]×P[n-1,n-1]＾(j-1)のi行k列の値と定義し、ただしU[n-1,n-1]×P[n-1,n-1]＾(j-1)とは行列U[n-1,n-1]とj-1個のP[n-1,n-1]の積を表し、Q(j,i,k)をc(j,i,k)=1のとき、Q(j,i,k)=R(k)、c(j,i,k)=0のとき、Q(j,i,k)=0 と定義したとき、各分割部分データD(i,j)を、変数iを１からnまで変えながら各変数iにおいて変数jを１からn-1まで変え、排他的論理和の演算子＊を用いて、i<nのとき、
【数３】

$$D(i,j) = S(j) * \left(\prod_{k=1}^{n-1} Q(j,i,k) \right)$$

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】変更
【補正の内容】
【００３９】
（４）P[n,n]とは、n×n行列であって、i行j列の値をp(i,j)で表すと、
j=i+1　のとき p(i,j)=1
i=n,j=1　のとき p(i,j)=1
上記以外のとき　p(i,j)=0
である行列を意味するものとし、「回転行列」ということとする。具体的には下記のような行列であり、他の行列の右側からかけると当該他の行列の１列目を２列目へ、２列目を３列目へ、…,n-1列目をn列目へ、n列目を１列目へ移動させる作用がある。つまり、行列Pを他の行列に右側から複数回かけると、その回数分だけ各列を右方向へ回転させるように移動させることができる。
【数７】

$$P[3,3] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$P[4,4] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$