(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 11 月 22 日(22.11.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/157279 A1

(51) 国際特許分類:
H04L 9/06 (2006.01) *G09C 1/00* (2006.01)

(21) 国際出願番号: PCT/JP2012/003239

(22) 国際出願日: 2012 年 5 月 17 日(17.05.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2011-111599 2011 年 5 月 18 日(18.05.2011) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社(NEC Corporation) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 寺西 勇 (TERANISHI, Isamu) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(74) 代理人: 岩壁 冬樹, 外(IWAKABE, Fuyuki et al.); 〒1040031 東京都中央区京橋二丁目８番７号 読売中公ビル６階 サンライズ国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: ORDER-PRESERVING ENCRYPTION SYSTEM, DEVICE, METHOD, AND PROGRAM

(54) 発明の名称 : 順序保存暗号化システム、装置、方法及びプログラム

[図2]

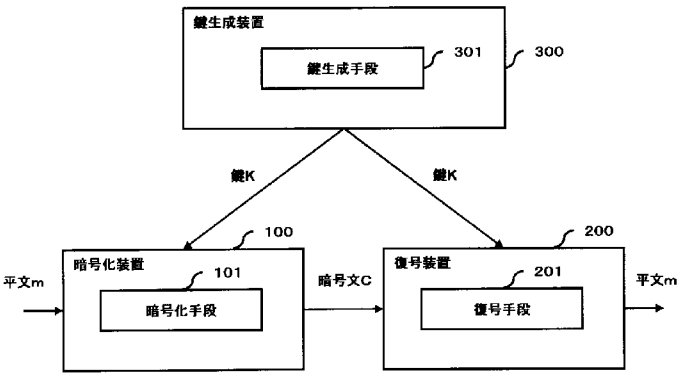


FIG. 2:
100 Encryption device
101 Encryption means
200 Decryption device
201 Decryption means
300 Key generation device
301 Key generation means
c Encrypted text
K Key
m Plain text

(57) **Abstract**: The order-preserving encryption system includes an encryption means that generates an encrypted text in the form of a sum of data in accordance with a predetermined distribution (X). The encryption means generates the encrypted text using, as the distribution (X), a distribution by which data having a randomly determined bit length are randomly selected in accordance with a distribution that corresponds to the bit length.

(57) 要約: 順序保存暗号化システムは、暗号文を事前に定められた分布 X に従うデータの和として生成する暗号化手段を含み、暗号化手段は、分布 X として、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する。

WO 2012/157279 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

順序保存暗号化システム、装置、方法及びプログラム

技術分野

[0001] 本発明は、順序保存暗号化システム、暗号化装置、順序保存暗号化方法及び順序保存暗号化プログラムに関する。

背景技術

[0002] 暗号方式は通信におけるデータの秘匿性を保障する為に用いられている。関連する技術として、例えば非特許文献１に記載された方式がある。

先行技術文献

非特許文献

[0003] 非特許文献1：Alexandra Boldyreva, Nathan Chenette, Younho Lee and Adam O'Neill. Order-Preserving Symmetric Encryption. EUROCRYPT 2009. pp. 224-241.

発明の概要

発明が解決しようとする課題

[0004] 暗号方式は通信におけるデータの秘匿性を保障する為に用いられるが、データを完全に秘匿する事が常に応用上有用になるとは限らず、データを秘匿しすぎた事が原因で逆に有用性を損ねる場合がある。

[0005] 例えば、２つの数値データの大小を比較したい場合には問題となる。２つのデータm、m'を直接読み込む事ができれば、mとm'の大小を比較できるが、mとm'がAESやDESなどの暗号方式により暗号化された状態で保管されていると、これらの暗号文を読み込んでもmとm'の大小を比較する事ができない。もちろん、これらの暗号文を復号してmとm'を復元すればmとm'の大小を比較できるが、暗号文を復号するには秘密鍵が必要であるので、秘密鍵を知らないユーザは大小比較ができない。また復号には計算コストがかかるので、秘密鍵を知っているユーザであっても、多数のデータの大小比較をするのは容易で

はない。

[0006] 特にセキュア・データベースでは、上記の事が大きな問題となる。というのも安全性の観点から平文をそのままデータベースに保管するのは望ましくない為、平文を暗号化して保管する必要があるからである。これら暗号文の鍵自身をデータベースに保存してしまうと暗号化した意味がなくなってしまうので、鍵の無い状態で暗号化されたデータを大小比較する必要が生じる。また鍵が手に入る状態であったとしても、データベースには数多くのデータが保管されている為、これら多くのデータを全て復号して大小比較するのは効率の面から現実的ではない。

[0007] また、近年のクラウドコンピューティング技術の発展により、ユーザが自身のデータをクラウド上のデータベースに預ける事がこれまで以上に増えるものと予想される。したがってデータベースにあるデータを暗号化されたまま大小比較する技術は今後非常に重要になる可能性が高い。

[0008] 非特許文献１で提案されている方式は、非特許文献１の著者達も認めているように、安全性に対する考察が不完全にしかなされておらず、この事がこの方式を実用化する際に障害となる。

[0009] そこで、本発明は、安全性が保障できる順序保存暗号化をする順序保存暗号化システム、暗号化装置、順序保存暗号化方法および順序保存暗号化プログラムを提供することを目的とする。

課題を解決するための手段

[0010] 本発明による順序保存暗号化システムは、暗号文を事前に定められた分布Xに従うデータの和として生成する暗号化手段を含み、暗号化手段は、分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成することを特徴とする。

[0011] 本発明による暗号化装置は、暗号文を事前に定められた分布Xに従うデータの和として生成する暗号化手段を含み、暗号化手段は、分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダム

に選択されるという形式であらわされる分布を用いて暗号文を生成することを特徴とする。

[0012] 本発明による順序保存暗号化方法は、暗号文を事前に定められた分布Xに従うデータの和として生成し、分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成することを特徴とする。

[0013] 本発明による順序保存暗号化プログラムは、コンピュータに、暗号文を事前に定められた分布Xに従うデータの和として生成する暗号化処理を実行させ、暗号化処理で、分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する処理を実行させることを特徴とする。

発明の効果

[0014] 本発明によれば、安全性が保障できる順序保存暗号化をすることができる。

図面の簡単な説明

[0015] [図1]本発明の装置の構成例を表すブロック図である。

[図2]本発明の装置間の関係を示した説明図である。

[図3]第一の実施形態の鍵生成処理を示すフローチャートである。

[図4]第一の実施形態の暗号化処理を示すフローチャートである。

[図5]第一の実施形態の復号処理を示すフローチャートである。

[図6]第二の実施形態の鍵生成処理を示すフローチャートである。

[図7]第二の実施形態におけるRecEncアルゴリズム示すフローチャートである。

[図8]第二の実施形態の暗号化処理を示すフローチャートである。

[図9]第二の実施形態におけるRecDecアルゴリズム示すフローチャートである。

[図10]第二の実施形態における復号処理を示すフローチャートである。

[図11]第三の実施形態の暗号化処理を示すフローチャートである。

[図12]第三の実施形態の復号処理を示すフローチャートである。

[図13]順序保存暗号化システムの最小の構成例を示すブロック図である。

発明を実施するための形態

[0016] まず後述する第一～第三の実施形態の全てに共通するアイデアを説明する。{1,...,N}を平文空間とする。また、Xをほとんどの場合に正の値を出力する確率分布とし、ζを定数とする。各i∈{-ζ,...,N}に対し、第一～第三の実施形態において平文m∈{1,...,N}の暗号文は、$Enc(K,m)=\Sigma_{i=-\zeta,...,m}\alpha[i]$という形で書ける。ここでα[i]は確率分布Xに従う乱数であり、秘密鍵Kを知っている人のみがα[i]を計算できる。

[0017] 暗号文Cを復号するには、$C=\Sigma_{i=-\zeta,...,m}\alpha[i]$を満たすmを平文として出力する。本発明ではEnc(K,m)は-ζからmまでの和であるが、これを0からmまでの和にしてしまうと、1の暗号文Enc(K,1)がEnc(K,1)=α[1]という非常に簡単な形になってしまい、安全性が保証されない為である。

[0018] 本発明では、$Enc(K,m)=\Sigma_{i=-\zeta,...,m}\alpha[i]$の右辺はmが大きければ大きいほど加えられるα[i]の数が増える。そのため、mが大きければ大きいほどEnc(K,m)は大きくなる。したがってm＜m'ならEnc(K,m)＜Enc(K,m')が成立する。

[0019] 本発明は原理的には任意のXに対して実行する事ができるが、安全性上の観点からいえば、低い確率でビット数が大きくなる分布である事が望ましい。Xがこのような性質を満たすと、各α[m]はXに従って選ばれるので、α[m]は低い確率でα[m+1], α[m+2], ...よりも長いビット長を持つ。この場合ビット長の長い乱数であるα[m]がビット長がより短い乱数であるα[m+1], α[m+2], ...を隠すので、α[m], α[m]+α[m+1], α[m]+α[m+2], ...はほぼ同じ値となり、識別ができない。よって$Enc(K,m)=\Sigma_{i=-\zeta,...,m}\alpha[i]$, $Enc(K,m+1)=\Sigma_{i=-\zeta,...,m+1}\alpha[i]$, $Enc(K,m+2)=\Sigma_{i=-\zeta,...,m+2}\alpha[i]$, ...も識別できず、安全性が保証される。

[0020] 前述した性質を満たすXとして、例えば以下のように定義される分布を用いる事ができる。p[1],...,p[U]を、p[1]+…+p[U]=1となる非負整数とし、さらにn[1],...,n[U]を非負整数とする。D[p[1],...,p[U]]を整数jを出力する確

率分布で、確率p[i]でj=iとなるものとする。B[1]を長さn[1]以下のビット長を持つ非負整数を出力する確率分布とし、B[U]を長さn[U]以下のビット長を持つ非負整数を出力する確率分布とする。Xは「D[p[1],...,p[U]]に従って整数jが選び、次にB[j]に従ってαを選ぶ」という方法でαを選んだときαが従う分布である。

[0021] 以上のようにXを定義すると、Xは確率p[1]で長さn[1]以下のビット長を持つ非負整数を出力し、確率p[2]でn[1]よりも大きいビット長n[2]を持つ非負整数を出力し、確率p[3]でn[2]よりも大きいビット長n[3]を持つ非負整数を出力し...となる。よってp[1],...,p[U], n[1],...,n[U]を適切に選べば、Xは前述した性質を満たす。

[0022] 次に、後述する第一の実施形態の概要について説明する。第一の実施形態では、秘密鍵KをK=(α[-ζ],...,α[N])により定義し、暗号化の際にはα[1],...,α[m]の和を計算する事によって暗号文$Enc(K,m)=\Sigma_{i=-\zeta,...,m}\alpha[i]$を得る。

[0023] また、与えられた暗号文Cを復号するには、各mに対して$\Sigma_{i=-\zeta,...,m}\alpha[i]$を計算し、$C=\Sigma_{i=-\zeta,...,m}\alpha[i]$となるmを見つけ出す。

[0024] 第一の実施形態では、mを暗号化する際に、m+ζ+1個のデータα[-ζ],...,α[m]を足しあわせる必要があるので、暗号化の計算量がmの大きさに比例してしまう。また、同様の複号の計算量もmの大きさに比例してしまう。従って第一の実施形態は、mが小さければ効果を得ることができるが、mが大きい場合には、後述する他の実施形態と比較して効率的ではないともいえる。

[0025] 次に、後述する第二の実施形態の概要について説明する。第二の実施形態も第一の実施形態のそれと同じく、mの暗号文Enc(K,m)は、$Enc(K,m)=\Sigma_{i=-\zeta,...,m}\alpha[i]$であるが、より効率的な方法で暗号化および復号がなされる。第二の実施形態では、効率的な暗号化および復号を実現する為、分布B[j]を二項分布B(τ[j],q)とする。

[0026] ここでτ[1],...,τ[U]およびqをパラメータとする。また、二項分布B(k,p')とは表が出る確率がp'であるコインをk枚ふった時に表が出る枚数が従う分

布である。

[0027] 第二の実施形態の詳細を述べる為記号を定義し、本発明の暗号文の性質を示す。B[j]に従ってα[i]が選ばれているiの集合をS[j]とし、S[j]の元でm以下のものの集合をS[m,j]とし、$\Sigma_{i\in S[m,j]}\alpha[i]$をC[m,j]とすると、mの暗号文Enc(K,m)をC[m]と書くと、C[m]の定義から、$C[m]=\Sigma_{i=1,\ldots,U}C[m,j]$が成立する。

[0028] S[m,j]の元の個数をn[m,j]とする。iがS[m,j]に属する場合、各α[i]は分布B[j]に従い、S[m,j]はn[m,j]個の元を持つので、二項分布の再生性より、$C[m,j]=\Sigma_{i\in S[m,j]}\alpha[i]$は、分布B(τ[j]n[m,j],q)に従うという事実が分かる。

[0029] vecn[m]=(n[m,1],...,n[m,U])とし、ベクトルvecu=(u[1],...,u[U])に対し、s(vecu)を$\Sigma_{j=1,\ldots,U}\tau[j]u[m]$とする。$C[m]=\Sigma_{i=1,\ldots,U}C[m,j]$だったので、二項分布の再生性より、C[m]は、分布B(s(vecn[m]),q)に従うという事実が分かる。

[0030] 従って、C[m]の従う分布は、vecn[m]に依存して決まる事が分かる。同様に平文m,m'＜mに対し、C[m]-C[m']は分布B(s(vecn[m]-vecn[m']),q)に従うという事実が分かる。そこで以下、vecn[m]-vecn[m']を{m'+1,...,m}上の「分布決定パラメータ」と呼ぶ。vecn[m]=vecn[m]-vec[-ζ-1]なので、vecn[m]自身は{-ζ-1,...,m}上の分布決定パラメータである。そこでvecn[m]の事も分布決定パラメータと呼ぶ。

[0031] $\Sigma_{i=1,\ldots,U}p'[i]=1$を満たすvecp'=(p'[1],...,p'[U])に対し、vecB(k,vecp')を「数値iが出る確率がp'[i]である確率変数Xに従ってk個の値a[1],...,a[k]を独立に選んだとき、値a[1],...,a[k]のうちjに等しいものの個数をn'[j]とする」という方法で出力vecn'=(n'[1],...,n'[U])を決める分布とする。B[j]に従ってα[i]が選ばれる確率はp[j]だったので、vecp=(p[1],...,p[U])とすると、二項分布の再生性よりvecn[m]=(n[m,1],...,n[m,U])は、分布vecB(m+ζ+1,vecp)に従うという事実が分かる。

[0032] Algo(k,p')を二項分布B(k,p')に従って出力を選ぶアルゴリズムとし、vecAlgo(k,vecp')を分布vecB(k,vecp')に従って出力を選ぶアルゴリズムとする。

[0033] 第二の実施形態では、以上で説明した事実を用いて、平文空間に属する最

大の元最大のMの暗号文C[M]を以下のように求める。

[0034] まずvecAlgo(M+ζ+1,vecp)に従ってMに対する分布決定パラメータvecn[M]を選ぶ。次いで、分布Algo(s(vecn[M]),q)に従ってC[M]を選ぶ。

[0035] 他の暗号文を使って再帰的に求める。本発明における再帰は何らかの平文u, v>uが以下の条件を満たしている状態で用いられる。

[0036] ・uの暗号文C[u]とvの暗号文C[v]とが求まっている。

・{u+1,...,v}上の分布決定パラメータvecnが求まっている。

・暗号文を算出したい平文mは区間{u+1,...,v}に属している。

[0037] 初期状態では、uとvとはそれぞれ-ζ-1とMとにセットされる。初期状態では、C[u]は0であり、C[v]とvecnとは、それぞれすでに求めたC[M]とvecn[M]とである。また初期状態では区間{u+1,...,v}は平文空間に一致するので、暗号文を算出したい平文mは区間{u+1,...,v}に属している。よって初期状態では上述の条件が満たされている。

[0038] mの暗号文は以下のように関数RecEnc(K',u,v,C[u],C[v],vecn,m)を用いて二分法により再帰的に計算される。ここでK'は秘密鍵の一部である乱数列である。また、Ceil(x)は入力された実数xの小数点以下を切り上げた値を出力する関数である。

[0039] ・m=uであれば、C[u]を出力し、m=vであれば、C[v]を出力する。

・w=Ceil(u+v/2)を計算する。

・{u+1,...,w}上の分布決定パラメータvecn'を関数Dist(u,v,w,vecn)に従って計算する。ただしここでvecDist(u,v,w,vecn)が用いる乱数として、K'を使って選ばれた擬似乱数列を用いる。

・vecn'を用いる事で、「uの暗号文とvの暗号文とがそれぞれC[u], C[v]であるという条件下wの暗号文が従う」分布Dist(C[u],C[v],vecn,vecn')に従ってC[w]を選ぶ。Dist(C[u],C[v],vecn,vecn')に従ってC[w]を選ぶ際に用いる乱数は、K'を使って選ばれた擬似乱数列を用いる。

・m≦wであれば、RecEnc(K',u,w,C[u],C[w],vecn',m)を再帰的に実行する。

・そうでなければRecEnc(K',w,v,C[w],C[v],vecn-vecn',m)を再帰的に実行す

る。

[0040] 上述のアルゴリズムでDist(C[u],C[v],vecn,vecn')から元を選ぶ際に擬似乱数を用いるのは、同じ(C[u],C[v],vecn,vecn')に対しては常に同じ暗号文C[w]が出力される事を保証する為である。上述のアルゴリズムは様々な入力mに対して実行され、その度にC[w]が計算される。C[w]はwに対する暗号文であるから、値C[w]はmによらず常に同じ値になる必要がある。しかし、Dist(C[u],C[v],vecn,vecn')の計算に真の乱数を用いると常に同じ値になる事が保証されない。一方擬似乱数列は確定的に値が決まる為、真の乱数の代わりに擬似乱数列を用いる事でDist(C[u],C[v],vecn,vecn')が常に同じ値C[w]を出力する事が保証される。

[0041] 関数HG(k,t,l)、およびvecHG(k,vect,l)を以下のように定義する。ここでk,t,lは非負の整数である。また、vect=(t[1],...,t[U])は$=\Sigma_{i=1,...,U}t[i]$を満たす非負整数t[1],...,t[U]からなるベクトルである。

[0042] ・HG(k,t,l):k-t個の白いボールとt個の黒いボールとが入った瓶からl個のボールを選んだときに、選ばれたボールの中にある黒いボールの数の従う分布(超幾何分布)に従って出力を決める確率的アルゴリズムである。

・vecHG(k,vect,l):以下の分布に従って出力n'=(n'[1],...,n'[U])を決める確率的アルゴリズム:瓶にk個のボールが入っている。ボールには1,...,Uのいずれかのマークが書かれており、iのマークのついたボールの数はt[i]個であるという状況下でこの瓶からl個のボールを選んだとき、選ばれたボールに含まれているマークiのボールの数をn'[j]とする。

[0043] このとき、前述したvecDist(u,v,w,vecn)およびDist(C[u],C[v],vecn,vecn')は、vecDist(u,v,w,vecn)=vecHG(v-u,vecn,w-u;cc)、Dist(C[u],C[v],vecn,vecn')=C[u]+HG(s(vecn),C[v]-C[u],s(vecn');cc')となる。ここで記号「A(x;r)」は「乱数としてrを使ってA(x)を実行したときの出力」の意味である。ccおよびcc'は、K'を使って選ばれた擬似乱数列である。

[0044] 第二の実施形態における復号アルゴリズムは以上で説明した暗号化アルゴリズムと同様、二分法的かつ再帰的に実行される。第二の実施形態における

暗号化アルゴリズムと復号アルゴリズムとの違いは以下のものである。

[0045] 暗号化アルゴリズムにおける「m=uならC[u]を出力し、m=vならC[v]を出力する」の部分が「C=C[u]ならuを出力し、C=C[v]ならvを出力し、u=vならCが不正な暗号文であると言う趣旨のメッセージを出力する」に変わる。ここでCは復号したい暗号文である。また、RecEncを再帰的に呼び出す代わりにRecDecを再帰的に呼び出す点で異なる。

[0046] 次に、後述する第三の実施形態の概要について説明する。第三の実施形態においては、B[j]として二項分布B(τ[j],q)を用いた場合を説明するが、原理的には以下の性質を満たす分布であれば第二の実施形態と同様の動作を行う。

[0047] ・α[j],...,α[k]をB[j],...,B[k]に従って選んだときにα[j]+…+α[k]の従う分布から元を選ぶのが容易である。

・「各jに対しS[j]の元で区間{u+1,...,v}に属しているものの個数がn[j]である」という条件下、「S[j]の元で区間{u+1,...,Ceil(u+v/2)}に属しているものの個数」の従う分布から元を選ぶのが容易である。

・uの暗号文がC[u]であり、vの暗号文がC[v]であり、しかも「各jに対しS[j]の元で区間{u+1,...,v}に属しているものの個数がn[j]である」という条件下、w=Ceil(u+v/2)の暗号文が従う分布から元を選ぶのが容易である。

[0048] たとえばB[j]として正規分布N(τ[j],V[j])で、τ[j]=V[j]=$2^{j\lambda}/2$としたものを用いる事ができる。ここでN(μ,V)は平均がμで分散がVの正規分布を表す。このときは、第二の実施形態におけるAlgo, Distを適切な関数Algo', Dist'に置き換える、さらに擬似乱数列cc, cc'のビット数を変更する事で動作を行う。

[0049] 最後に第二の実施形態の安全性について述べる。前述したように第二の実施形態の暗号文は第一の実施形態の発明の暗号文と同一となる。よって第二の実施形態の安全性も第一の実施形態の安全性と同様となる。前述したように第一の実施形態では安全性が担保できているので、この事は第二の実施形態の安全性を保証する。

[0050] 第一の実施形態.

本発明による順序保存暗号化システムの構成を図１、図２を参照して説明する。図１に示すように、本実施形態の各装置（図２に示す暗号化装置１００、復号装置２００および鍵生成装置３００）は、それぞれ入出力部１１、演算部１２、記憶部１３および通信部１４を備えている。これらの装置は、例えばプログラムに従って動作するパーソナルコンピュータ等の情報処理装置によって実現される。また、この場合、入出力部１１、演算部１２、記憶部１３および通信部１４は、例えば、それぞれキーボード、CPU、メモリ、およびネットワークインタフェース部によって実現される。また、図２に示すように、本実施形態では、順序保存暗号化システムは、暗号化装置１００、復号装置２００および鍵生成装置３００を含む。

[0051] 本実施形態では、暗号化装置１００は、暗号化手段１０１を含む。また、復号装置２００は、復号手段２０１を含む。なお、ここでは暗号化装置１００と、復号装置２００との二種類の装置を用いる場合を想定して説明するが、一つの装置が暗号化手段と復号手段との両方を含むように構成してもよい。また、以降、暗号化アルゴリズムや復号アルゴリズムについて記載するが、具体的には、順序保存暗号化システムを実現する１つ又は複数の情報処理装置のCPUがこれらのアルゴリズムに従って処理を実行する。

[0052] 暗号化装置１００および復号装置２００の記憶部１３には、事前に鍵というビット列K（以下、鍵Kという）が記憶されているものとする。鍵Kは鍵生成手段、という手段により生成される。図２に示す例では、鍵生成装置３００を暗号化装置１００や復号装置２００とは別に用意し、この装置が鍵生成手段３０１を含み、鍵Kを生成する処理を実行する場合を想定している。しかしながら、この例に限らず、鍵生成手段を暗号化装置１００、復号装置２００、またはそれらとは異なる第三の装置のいずれかが含み、鍵Kを生成する処理を実行するように構成してもよい。ただし安全性上の観点から言えば、暗号化装置１００または復号装置２００以外の装置に鍵Kを明かすべきではないので、暗号化装置１００または復号装置２００が鍵生成手段を含み、鍵Kを生成

する処理を実行する事が望ましい。

[0053] 図２に示される各手段が入出力するデータは以下のとおりである。

[0054] 鍵生成手段３０１は、鍵Kを生成し、生成した鍵Kを出力する。鍵生成手段３０１は、具体的には、プログラムに従って動作する情報処理装置のCPUによって実現される。

[0055] 暗号化手段１０１は、鍵Kと平文mとを入力として受け取り、受け取った平文mを鍵Kを用いて暗号化し、暗号文Cを出力する。暗号化手段１０１は、具体的には、プログラムに従って動作する情報処理装置のCPUによって実現される。

[0056] 復号手段２０１は、鍵Kと暗号文Cとを入力として受け取り、受け取った暗号文Cを鍵Kを用いて復号し、平文mを出力する。復号２０１手段は、具体的には、プログラムに従って動作する情報処理装置のCPUによって実現される。

[0057] 本実施形態では、以下の手順で処理が実施される。なお、事前に鍵生成手段３０１によって生成された鍵Kが暗号化装置１００および復号装置２００の記憶部１３に書き込まれているものとする。

[0058] まず、暗号化装置１００は、入出力部１１で入力した平文mを、記憶部１３に書き込む。

[0059] 次いで、暗号化装置１００は、記憶部１３から鍵Kと平文mとを読み込み、これらを入力として暗号化手段１０１によって暗号化処理を実行し、その出力として暗号文Cを計算する。

[0060] 次いで、暗号化装置１００は、通信部１４から暗号文Cを復号装置２００に送信する。

[0061] 復号装置２００は、通信部１４を使って暗号文Cを受信する。そして、復号装置２００は、記憶部１３から鍵Kを読み込み、鍵Kと暗号文Cとを入力として復号手段２０１によって復号処理を実行し、その出力として平文mを計算する。

[0062] 次に、順序保存暗号化装置が実行する処理の詳細について説明する。ここでは、{1,...,M}を平文空間とし、Uとλとζとを定数とする。i=1,...,Uに対

し、B[i]を確率分布とする。B[j]としては、例えば、区間{0,...,τ[j]}上の一様分布や、二項分布B(τ[j],p[j])、正規分布N(τ[j],V[j])を用いる事ができる。

[0063] 安全性上の観点から言えば、λは80以上の値とする事が望ましい。τ[j], p[j], V[j]としては、例えば、τ[j]=V[j]=$2^{j\lambda}$, p[j]=qとすればよい。

[0064] 二項分布および正規分布を計算するアルゴリズムについては、例えば文献（四辻哲章，計算機シミュレーションのための確率分布乱数生成法。プレアデス出版。2010年6月発売）に記載されている。

[0065] p[1],...,p[U]を非負の実数で$\Sigma_{i=1,...,U}p[i]=1$を満たすものとし、vecp=(p[1],...,p[U])とする。vecBernoulli(vecp)を、1以上U以下の値を出力するアルゴリズムで、jを出力する確率がp[j]であるものとする。vecBernoulli(vecp)はどのような方法で実現してもよいが、例えば以下の方法で実現できる。ここではP[k]=$\Sigma_{i=1,..,k}p[i]$である。ただしP[0]=0である。

[0066] ・区間{0,...,2^{λ}}から一様かつランダムにxを選ぶ。

・2^{λ}P[j-1]＜x≦2^{λ}P[j]となるjを見つけ、そのようなjを出力する。

[0067] パラメータM, U, ζ, λおよびvecpは各装置の記憶部１３に記憶されており、各装置は必要に応じてこれらの値を使う事ができる。

[0068] 次に、鍵生成手段が実行する処理について説明する。本実施形態において鍵生成手段３０１が実行する処理の詳細は以下のとおりである。

[0069] 鍵生成手段３０１は、i=-ζ,...,Nに対して以下の処理を実行する(図３のステップ1K1)。

[0070] ・鍵生成手段３０１は、vecBernoulli(vecp)を実行し、その出力j[i]を得る(1K1)。

・鍵生成手段３０１は、B[j[i]]に従ってα[i]を選択する(1K1)。

[0071] 次いで、鍵生成手段３０１は、K=(α[-ζ],...,α[N])を鍵Kとして出力する(図３のステップ1K2)。本実施形態では、鍵生成手段３０１は、暗号化装置１００および復号装置２００に鍵Kを出力する。

[0072] 次に、暗号化手段が実行する処理について説明する。本実施形態において

暗号化手段１０１が実行する処理の詳細は以下のとおりである。

[0073] 暗号化手段１０１は、鍵K=(α[-ζ],...,α[N])と平文mとを記憶部１３から読み込む(図４のステップ1E1)。

[0074] 次いで、暗号化手段１０１は、$C=\Sigma_{i=-\zeta,...,m}\alpha[i]$を計算する(図４のステップ1E2)。

[0075] 次いで、暗号化手段１０１は、Cを暗号文Cとして出力する(図４のステップ1E3)。本実施形態では、暗号化手段１０１は、復号装置２００に暗号文Cを出力する。

[0076] 次に、復号手段が実行する処理について説明する。本実施形態において復号手段２０１が実行する処理の詳細は以下のとおりである。

[0077] 復号手段２０１は、鍵K=(α[-ζ],...,α[N])と暗号文Cとを記憶部１３から読み込む(図５のステップ1D1)。

[0078] 復号手段２０１は、$S=\Sigma_{i=-\zeta,...,0}\alpha[i]$を計算する(図５のステップ1D2)。

[0079] 次いで、C≦Sであれば、復号手段２０１は、不正な暗号文である事を示すメッセージを出力して異常停止する(ステップ1D2)。一方、C≦Sでなければ、復号手段２０１は、i=1,...,Nに対して以下の（１），（２）の処理を実行する(ステップ1D2)。

（１）S+α[i]を新しくSとする(ステップ1D2)。

（２）C≦Sなら復号結果としてiを出力して正常停止する(ステップ1D2)。

また、復号手段２０１は、入力が不正なデータだった場合には、不正な暗号文である事を示すメッセージを出力して異常停止する(ステップ1D2)。なお、不正な暗号文である事を示すことができれば、メッセージの出力に限らず、どのような通知であってもよい。

[0080] 以上に説明したように、本実施形態では、安全性が保障された暗号化状態で平文の大小比較を効率的に行う事ができる。

[0081] 第二の実施形態.

第二の実施形態の装置構成、およびパラメータM，U，ζ，λ，vecpは第一の実施形態のそれと同一である。ただし、本実施形態では、第一の実施形態

と比較して、各手段の機能が異なる。

[0082] 本実施形態では、第一の実施形態の構成に加えて、ρをパラメータとする。安全性上の観点から言えば、ρは160ビット以上である事が望ましい。また、本実施形態では、τ[1],...,τ[U]をパラメータとする。安全性上の観点から言えば、τ[j+1]/τ[j]は2^{λ}以上である事が望ましい。例えばτ[j]=$2^{j\lambda}$とすると、この性質が満たされる。各パラメータは各装置の記憶部１３に記憶されており、各装置は必要に応じてこれらの値を使う事ができる。

[0083] ベクトルvecu=(u[1],...,u[U])に対し、s(vecu)を$\Sigma_{j=1,...,U}\tau[j]u[m]$とする。Algo, vecAlgo, Dist, vecDistを次のようなアルゴリズムとする。

[0084] ・Algo(k,p'):二項分布B(k,p')に従って出力を選ぶ。

・vecAlgo(k,vecp'): 上述の概要で説明した分布vecB(k,vecp')に従って出力を選ぶ。

・Dist(C1,C2,vecn,vecn'):C1+HG(s(vecn),C2-C1,s(vecn'))を出力する。ここでHGは上述の概要で説明した関数である。

・vecDist(u,v,w,vecn):vecHG(v-u,vecn,w-u)を出力する。ここでvecHGは上述の概要で説明した関数である。

[0085] 二項分布およびHGを計算するアルゴリズムについては文献（四辻哲章，計算機シミュレーションのための確率分布乱数生成法。プレアデス出版。2010年6月発売）に記載されている。

[0086] vecAlgo(k,vecp')は例えば以下の方法で計算できる。ただしここでvecp'=(p'[1],...,p'[U]), $\Sigma_{j=1,...,U}p'[j]=1$である。

[0087] １．k'=kとする。

２．j=1,...,U-1に対して以下の（１）（２）を実行する。

（１）二項分布B(k,p'[j])に従ってn[j]を選ぶ。

（２）k'にk'-n[j]を上書きする。

３．n[U]=k'とする。

４．vecn=(n[1],...,n[U])を出力する。

[0088] vecHG(k,vect,l)は、例えば以下の方法で計算できる。ただしここでvect=(

t[1],...,t[U]), $\Sigma_{j=1,...,U}t[j]=k$である。

[0089] １．k'=k, l'=lとする。

２．j=1,...,U-1に対して以下の（１）（２）を実行する。

（１）HG(k',t[j],l')を実行し、出力n[j]を得る。

（２）k'-t[j]をk'に上書きし、l'-n[j]をl'に上書きする。

３．n[U]=l'とする。

４．vecn=(n[1],...,n[U])を出力する。

[0090] 次に、鍵生成手段が実行する処理について説明する。本実施形態において鍵生成手段３０１が実行する処理の詳細は以下のとおりである。

[0091] 鍵生成手段３０１は、ρビットのビット列K'をランダムに選択する(図６のステップ2K1)。

[0092] 次いで、鍵生成手段３０１は、vecAlgo(M+ζ+1,vecp)を実行し、出力vecn[M]を得る(図６のステップ2K2)。

[0093] 次いで、鍵生成手段３０１は、Algo(s(vecn[M]),q)を実行し、出力C[M]を得る(図６のステップ2K3)。

[0094] 次いで、鍵生成手段３０１は、K=(K',vecn[M],C[M])を出力する(図６のステップ2K4)。

[0095] Ceil(x)を入力された実数xの小数点以下を切り上げた値を出力する関数とし、アルゴリズムDist, vecDistが計算に用いる乱数のビット数をそれぞれL, L'とし、PRF(K,・)をKを鍵として用いる擬似ランダム関数で出力がLビットの擬似乱数であるものとし、PRF'(K,・)をKを鍵として用いる擬似ランダム関数で出力がL'ビットの擬似乱数であるものとする。さらに記号「a||b」でビット列aとbの連結を表し、アルゴリズムAに対し「A(x;r)」で「乱数としてrを使ってA(x)を実行したときの出力」を表す。

[0096] アルゴリズムRecEnc(K',u,v,C[u],C[v],vecn,m)を以下のように再帰的に定義する。

[0097] m=uであれば、C[u]を、m=vであれば、C[v]を出力する(図７のステップ2RE1)。

[0098] 次いで、w=Ceil((u+v)/2)を計算する(図７のステップ2RE2)。

[0099] 次いで、cc=PRF(K',(v-u||vecn||w-u)を計算する(図７のステップ2RE3)。また、vecn'=vecDist(u,v,w,vecn;cc)を計算する(図７のステップ2RE3)。

[0100] 次いで、cc'=PRF'(K',s(vecn)||(C[v]-C[u])||s(vecn'))を計算する(図７のステップ2RE4)。また、C[w]=Dist(C[u],C[v],vecn,vecn';cc')を計算する(図７のステップ2RE4)。

[0101] 次いで、m≦wであれば、RecEnc(K',u,w,C[u],C[w],vecn',m)を出力する(図７のステップ2RE5)。

[0102] 一方、m>wであれば、RecEnc(K',w,v,C[w],C[v],vecn-vecn',m)を出力する(図７のステップ2RE6)。

[0103] 次に、暗号化手段が実行する処理について説明する。本実施形態において暗号化手段１０１が実行する処理の詳細は以下のとおりである。

[0104] 暗号化手段１０１は、K=(K',C[M],vecn[M])を入力として受け取る(図８のステップ2E1)。

[0105] 次いで、暗号化手段１０１は、RecEnc'(K',-ζ-1,M,0,C[M],vecn[M],m)を実行する(図８のステップ2E2)。

[0106] アルゴリズムRecDec(K',u,v,C[u],C[v],vecn,m)を以下のように再帰的に定義する。

[0107] u≦0なら次の処理を行う(図９のステップ2RD1)。具体的には、C=C[u]ならuを、m=C[v]ならvを出力し、u=vなら暗号文が不正である事を示すメッセージを出力する(2RD1)。

[0108] 次いで、w=Ceil((u+v)/2)を計算する(図９のステップ2RD2)。

[0109] 次いで、cc=PRF(K',(v-u||vecn||w-u)を計算する(図９のステップ2RD3)。また、vecn'=vecDist(u,v,w,vecn;cc)を計算する(図９のステップ2RD3)。

[0110] 次いで、cc'=PRF'(K',s(vecn)||(C[v]-C[u])||s(vecn'))を計算する(図９のステップ2RD4)。また、C[w]=Dist(C[u],C[v],vecn,vecn';cc')を計算する(図９のステップ2RD4)。

[0111] 次いで、m≦wであれば、RecDec(K',u,w,C[u],C[w],vecn',m)を出力する(図

９のステップ2RD5)。

[0112] 一方、m>wであれば、RecDec(K',w,v,C[w],C[v],vecn-vecn',m)を出力する(図９のステップ2RD6)。

[0113] 次に、復号手段が実行する処理について説明する。本実施形態において復号手段２０１が実行する処理の詳細は以下のとおりである。

[0114] 復号手段２０１は、K=(K',C[M],vecn[M])を入力として受け取る(図１０のステップ2D1)。

[0115] 次いで、復号手段２０１は、RecDec'(K',-ζ-1,M,0,C[M],vecn[M],m)を実行する(図１０のステップ2D2)。

[0116] 以上に説明したように、本実施形態では、安全性が保障された暗号化状態で平文の大小比較を効率的に行う事ができる。また、本実施形態では、第一の実施形態と比較して、より効率的な方法で暗号化および復号処理を行うことができる。

[0117] 第三の実施形態.

第三の実施形態の装置構成、およびパラメータM, U, ζ, λ, vecpは第一の実施形態のそれと同一である。ただし、本実施形態では、第一の実施形態と比較して、各手段の機能が異なる。

[0118] 本実施形態では、第一の実施形態の構成に加えて、V[1],...,V[n]をパラメータとし、vecu=(u[1],...,u[U])に対し、$t(vecn[M])=\Sigma_{i=1,\ldots,U}u[i]V[i]$とする。

[0119] V[j]は例えばV[j]=$2^{j\lambda}$と設定できる。Normal(μ,V)を、平均μ, 分散Vの正規分布に従って出力を選ぶアルゴリズムとする。第三の実施形態における鍵生成処理は、第二の実施形態の鍵生成手段によるAlgo(s(vecn[M]),q)を以下のアルゴリズムAlgo'(s(vecn[M]),t(vecn[M]))に変更したものである。

[0120] ・Normal(s(vecn[M]),t(vecn[M]))に従ってC[M]を選ぶ。

・C[M]を出力する。

[0121] アルゴリズムDist'(C[u],C[v],vecn,vecn')を以下のように定義する。

[0122] C=C[u]+s(vecn')+Normal(2(C[v]-C[u]-s(vecn))$\sqrt{}$(t(vecn')/t(vecn)),$\sqrt{}$(

t(vecn')t(vecn-vecn')/t(vecn)))とし、Cを出力する。

[0123] アルゴリズムDist'が計算に用いる乱数のビット数をL''とし、PRF''(K,・)をKを鍵として用いる擬似ランダム関数で出力がL''ビットの擬似乱数であるものとする。RecEnc'(K',u,v,C[u],C[v],vecn,m)を、第二の実施形態におけるRecEnc(K',u,v,C[u],C[v],vecn,m)の(ステップ2RE4)を以下の手続きにかえたものとする。

[0124] cc'=PRF''(K',s(vecn)||(C[v]-C[u])||s(vecn'))を計算する。また、C[w]=Dist'(C[u],C[v],vecn,vecn';cc')を計算する。

[0125] 次に、暗号化手段が実行する処理について説明する。本実施形態において暗号化手段１０１が実行する処理の詳細は以下のとおりである。

[0126] 暗号化手段１０１は、K=(K',C[M],vecn[M])を入力として受け取る(図１１のステップ3E1)。

[0127] 暗号化手段１０１は、RecEnc'(K',-ζ-1,M,0,C[M],vecn[M],m)を実行する(図１１のステップ3E2)。

[0128] ここでは、RecDec'(K',u,v,C[u],C[v],vecn,m)を、第二の実施形態におけるRecDec(K',u,v,C[u],C[v],vecn,m)の(ステップ2RD4)を以下の手続きにかえたものとする。

[0129] cc'=PRF''(K',s(vecn)||(C[v]-C[u])||s(vecn'))を計算する。また、C[w]=Dist'(C[u],C[v],vecn,vecn';cc')を計算する。

[0130] 次に、復号手段が実行する処理について説明する。本実施形態において復号手段２０１が実行する処理の詳細は以下のとおりである。

[0131] 復号手段２０１は、K=(K',C[M],vecn[M])を入力として受け取る(図１２のステップ3D1)。

[0132] 復号手段２０１は、RecDec'(K',-ζ-1,M,0,C[M],vecn[M],m)を実行する(図１２のステップ3D2)。

[0133] 以上に説明したように、本実施形態では、安全性が保障された暗号化状態で平文の大小比較を効率的に行う事ができる。また、本実施形態では、第一の実施形態と比較して、より効率的な方法で暗号化および復号処理を行うこ

とができる。

[0134] 第四の実施形態.

第四の実施形態の暗号文は第一の実施形態の暗号文に乱数Rを加えたものである。乱数Rを加える事で暗号文が撹拌される為、より高い安全性が保証される。第四の実施形態の装置構成は第一の実施形態のそれと同一である。ただし、本実施形態では、第一の実施形態と比較して、各手段の機能が異なる。

[0135] なお、本実施形態では、ζを0にセットしてもよい。それ以外のパラメータは第一の実施形態のそれと同一である。

[0136] 次に、鍵生成手段が実行する処理について説明する。本実施形態において鍵生成手段３０１が実行する処理の詳細は以下のとおりである。

[0137] 第一の実施形態における鍵生成処理と同様に、鍵生成手段３０１は、鍵K'を生成する。

[0138] 次いで、鍵生成手段３０１は、ρビットの乱数Rを選択する。

[0139] 次いで、鍵生成手段３０１は、鍵K=(K',ρ)を出力する。

[0140] 次に、暗号化手段が実行する処理について説明する。本実施形態において暗号化手段１０１が実行する処理の詳細は以下のとおりである。

[0141] 暗号化手段１０１は、K=(K',ρ)と平文mとを記憶部１３から読み込む。

[0142] 次いで、暗号化手段１０１は、K'とmとを入力して第一の実施形態と同様の暗号化処理を行う事で、その出力C'を得る。

[0143] 次いで、暗号化手段１０１は、暗号文C=C'+Rを出力する。

[0144] 次に、復号手段が実行する処理について説明する。本実施形態において復号手段２０１が実行する処理の詳細は以下のとおりである。

[0145] 復号手段２０１は、鍵K=(K',R)と暗号文Cとを記憶部１３から読み込む。

[0146] 次いで、復号手段２０１は、C'=C-Rを計算する。

[0147] 次いで、復号手段２０１は、K'とC'とを入力して、第一の実施形態と同様の復号処理を行う事でその出力mを得る。

[0148] 次いで、復号手段２０１は、平文mを出力する。

[0149] 以上に説明したように、本実施形態では、安全性が保障された暗号化状態

で平文の大小比較を効率的に行う事ができる。また、本実施形態では、乱数Rを加える事で暗号文が撹拌される為、第一の実施形態と比較して、より高い安全性が保証される。

[0150] 第五の実施形態.

第五の実施形態は、第四の実施形態中にある「第一の実施形態」の構成を「第二の実施形態」の構成にかえたものである。すなわち、第二の実施形態で示した構成に第四の実施形態で示した構成を適用したものである。これによって、本実施形態では、第四の実施形態と比較して、より効率的な方法で暗号化および復号処理を行うことができる。

[0151] 第六の実施形態.

第六の実施形態は、第四の実施形態中にある「第一の実施形態」の構成を「第三の実施形態」の構成にかえたものである。すなわち、第三の実施形態で示した構成に第四の実施形態で示した構成を適用したものである。これによって、本実施形態では、第四の実施形態と比較して、より効率的な方法で暗号化および復号処理を行うことができる。

[0152] 以上に説明したように、本発明は、例えばセキュア・データベースにおいて安全性を担保しつつ順序によるデータ検索を可能にする。よって本発明はデータを不正に読まれないという有用性と、検索によるデータ利用という有用性とを持つ。

[0153] 新規性に関しては、非特許文献１に記載された方式でも、本発明の第二の実施形態と同様に、二分法的な再帰を行っているが、分布決定パラメータが本発明の新規性を保証する。非特許文献１に記載された方式には、本発明における分布決定パラメータvecnに相当するデータは無い。本発明では分布決定パラメータによって分布を決定する事ではじめて再帰をまわす事ができる為、本発明と非特許文献１に記載された方式とは大きく異なり、新規性があるといえる。

[0154] また、分布決定パラメータは本発明の進歩性をも保証する。分布決定パラメータを使った再起を使った事により、第二の実施形態の暗号文は第一の実

施形態の暗号文と同一となり、したがって前述したように第二の実施形態の発明も安全性が担保される。非特許文献１に記載された方式は安全性が担保されていなかったので、本発明には進歩性があるといえる。

[0155] 次に、本発明による順序保存暗号化システムの最小構成について説明する。図１３は、順序保存暗号化システムの最小の構成例を示すブロック図である。図１３に示すように、順序保存暗号化システムは、最小の構成要素として、暗号化手段１０１を含む。

[0156] 図１３に示す最小構成の順序保存暗号化システムでは、暗号化手段１０１は、暗号文を事前に定められた分布Xに従うデータの和として生成する。また、暗号化手段１０１は、分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する。

[0157] 従って、最小構成の順序保存暗号化システムによれば、安全性が保障できる順序保存暗号化を実現することができる。

[0158] なお、本実施形態では、以下の（１）～（７）に示すような順序保存暗号化システムの特徴的構成が示されている。

[0159] （１）順序保存暗号化システムは、暗号文を事前に定められた分布Xに従うデータ(例えば、α[j])の和として生成する暗号化手段（例えば、暗号化手段１０１によって実現される）を含み、暗号化手段は、分布Xとして、ランダムに決められたビット長(例えば、j[i])のデータ(例えば、α[j])がビット長に応じた分布(例えば、B[j])に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成することを特徴とする。

[0160] （２）順序保存暗号化システムにおいて、平文空間の元の数に比例した数のデータを選択し（例えば、(α[-ζ],...,α[N])）、選択したデータを全て含む組を鍵として生成し出力する鍵生成手段（例えば、鍵生成手段３０１）を含み、鍵生成手段は、データを選択する際には、データの長さを決定する乱数を選択し、選択した乱数に従ったビット長のデータを選択するように構成されていてもよい。

[0161] （３）順序保存暗号化システムにおいて、暗号化手段は、複数のデータの組を含む鍵（例えば、K=(α[-ζ],...,α[N])）を暗号化に用い、平文を暗号化するために、平文の大きさに比例した数のデータを足しあわせて（例えば、$C=\Sigma_{i=-\zeta,...,m}\alpha[i]$）暗号化するように構成されていてもよい。

[0162] （４）順序保存暗号化システムにおいて、複数のデータの組を含む鍵（例えば、K=(α[-ζ],...,α[N])）を用いて暗号化された暗号文を復号する復号手段（例えば、復号手段２０１によって実現される）を含み、復号手段は、暗号文を復号するために、各mに対してmの大きさに比例した数のデータを足しあわせた値を計算し（例えば、$\Sigma_{i=-\zeta,...,m}\alpha[i]$）、足しあわせた値が暗号文と一致するmを出力し、暗号文と一致するmが存在しない場合には暗号文が不正なものである事を通知するように構成されていてもよい。

[0163] （５）順序保存暗号化システムにおいて、複数のデータの組を含む鍵を暗号化に用いる暗号化手段を含む暗号化装置と、鍵を用いて暗号化された暗号文を復号する復号手段を含む復号装置とを備え、平文空間の元の数に比例した数のデータを選択し、選択したデータを全て含む組を鍵として生成し出力する鍵生成手段を含み、鍵生成手段は、データを選択する際には、データの長さを決定する乱数を選択し、選択した乱数に従ったビット長のデータを選択し、暗号化手段は、鍵と平文とを入力して該平文の大きさに比例した数のデータを足しあわせて暗号化する暗号文を計算し、復号手段は、鍵と暗号文とを入力して、各mに対してmの大きさに比例した数のデータを足しあわせたものを計算し、足しあわせたものが暗号文と一致するmを出力し、暗号文と一致するmが存在しない場合には暗号文が不正なものである事を通知するように構成されていてもよい。

[0164] （６）順序保存暗号化システムにおいて、K'をランダムに選択し、分布を決めるパラメータvecn[M]を事前に定められたアルゴリズムに従って選択し、vecn[M]をパラメータとして入力して分布に従って暗号文C[M]を選択し、K'とvecn[M]とC[M]とを含む組を鍵として出力する鍵生成手段を含むように構成されていてもよい。

[0165] （７）順序保存暗号化システムにおいて、vecn[M]は、複数のデータを含む組であり、鍵生成手段は、vecn[M]に含まれるデータを、それらの総和が事前に定められた値になるという条件下で二項分布に従って選択するように構成されていてもよい。

[0166] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[0167] （付記１）vecn[M]は、複数のデータを含む組であり、鍵生成手段は、前記vecn[M]に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で正規分布に従って選択する請求項６記載の順序保存暗号化システム。

[0168] （付記２）暗号化手段は、鍵と平文とを入力として受け取ってサブルーチンを実行し（例えば、RecEnc'）、前記サブルーチンは、前記平文を含む区間を入力として受け取り（例えば、u,v）、さらに前記区間の両端の値に対応する暗号文も入力として受け取り（例えば、C[u],C[v]）、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文を計算し、さらに前記区間をwによって２つに分割し、前記平文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力平文がすでに暗号文を計算された値のいずれかと一致するときには該暗号文を出力する請求項１記載の順序保存暗号化システム。

[0169] （付記３）vecn'は、複数のデータを含む組であり、サブルーチンは、前記vecn'に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で超幾何分布に従って選択する付記２記載の順序保存暗号化システム。

[0170] （付記４）定められた分布は、超幾何分布に区間の端に対応する暗号文を加えたものである付記３記載の順序保存暗号化システム。

[0171] （付記５）定められた分布は、正規分布である付記３記載の順序保存暗号化システム。

[0172] （付記６）復号手段は、鍵と暗号文とを入力として受け取ってサブルーチンを実行し(例えば、RecEnc')、前記サブルーチンは、暗号文空間の区間で前記入力暗号文がその区間に属しているものを入力として受け取り（例えば、C[u],C[v]）、さらに前記区間の両端に当たる暗号文に対応する平文も入力として受け取り（例えば、u,v．）、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文C[w]を計算し、さらに前記区間をC[w]によって２つに分割し、前記入力暗号文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力暗号文がすでに暗号文を計算された値のいずれかと一致するときは該暗号文を出力する請求項１記載の順序保存暗号化システム。

[0173] （付記７）定められた分布は、超幾何分布に区間の端に対応する暗号文を加えたものである付記６記載の順序保存暗号化システム。

[0174] （付記８）定められた分布は、正規分布である付記６記載の順序保存暗号化システム。

[0175] （付記９）暗号化手段を含む暗号化装置と、復号手段を含む復号装置とを備え、K'をランダムに選択し、分布を決めるパラメータvecn[M]を事前に定められたアルゴリズムに従って選択し、前記vecn[M]をパラメータとして入力して前記分布に従って暗号文C[M]を選択し、前記K'と前記vecn[M]と前記C[M]とを含む組を鍵として出力する鍵生成手段を含み、前記暗号化手段は、前記鍵と

平文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、前記平文を含む区間を入力として受け取り、さらに前記区間の両端の値に対応する暗号文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文を計算し、さらに前記区間をwによって２つに分割し、前記平文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力平文がすでに暗号文を計算された値のいずれかと一致するときには該暗号文を出力し、前記復号手段は、前記鍵と前記暗号文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、暗号文空間の区間で前記入力暗号文がその区間に属しているものを入力として受け取り、さらに前記区間の両端に当たる暗号文に対応する平文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文C[w]を計算し、さらに前記区間をC[w]によって２つに分割し、前記入力暗号文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力暗号文がすでに暗号文を計算された値のいずれかと一致するときは該暗号文を出力することを特徴とする順序保存暗号化システム。

[0176] （付記１０）暗号化手段を含む暗号化装置と復号手段を含む復号装置とを備

え、K'をランダムに選択し、分布を決めるパラメータvecn[M]を事前に定められたアルゴリズムに従って選択し、前記vecn[M]をパラメータとして入力して前記分布に従って暗号文C[M]を選択し、前記K'と前記vecn[M]と前記C[M]とを含む組を鍵として出力する鍵生成手段を含み、前記vecn[M]は、複数のデータを含む組であり、前記鍵生成手段は、前記vecn[M]に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で二項分布に従って選択し、前記暗号化手段は、前記鍵と平文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、前記平文を含む区間を入力として受け取り、さらに前記区間の両端の値に対応する暗号文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文を計算し、さらに前記区間をwによって２つに分割し、前記平文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力平文がすでに暗号文を計算された値のいずれかと一致するときには該暗号文を出力し、前記vecn'は、複数のデータを含む組であり、前記暗号化手段は、前記vecn'に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で超幾何分布に従って選択し、前記復号手段は、前記鍵と前記暗号文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、暗号文空間の区間で前記入力暗号文がその区間に属しているものを入力として受け取り、さらに前記区間の両端に当たる暗号文に対応する平文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文C[w]を計算し、さらに前記区間をC[w]によって２つに分割し、前記入力暗号文が前記分割された区間のいずれに属しているかに応じ

て、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力暗号文がすでに暗号文を計算された値のいずれかと一致するときは該暗号文を出力し、前記定められた分布は、超幾何分布に区間の端に対応する暗号文を加えたものであることを特徴とする順序保存暗号化システム。

[0177] （付記１１）暗号化手段を含む暗号化装置と復号手段を含む復号装置とを備え、K'をランダムに選択し、分布を決めるパラメータvecn[M]を事前に定められたアルゴリズムに従って選択し、前記vecn[M]をパラメータとして入力して前記分布に従って暗号文C[M]を選択し、前記K'と前記vecn[M]と前記C[M]とを含む組を鍵として出力する鍵生成手段を含み、前記vecn[M]は、複数のデータを含む組であり、前記鍵生成手段は、前記vecn[M]に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で二項分布に従って選択し、前記暗号化手段は、前記鍵と平文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、前記平文を含む区間を入力として受け取り、さらに前記区間の両端の値に対応する暗号文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文を計算し、さらに前記区間をwによって２つに分割し、前記平文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力平文がすでに暗号文を計算され

た値のいずれかと一致するときには該暗号文を出力し、前記定められた分布は、超幾何分布に区間の端に対応する暗号文を加えたものであり、前記復号手段は、鍵と暗号文とを入力として受け取ってサブルーチンを実行し、前記サブルーチンは、暗号文空間の区間で前記入力暗号文がその区間に属しているものを入力として受け取り、さらに前記区間の両端に当たる暗号文に対応する平文も入力として受け取り、さらに前記区間における分布決定パラメータvecnも入力として受け取り、値wを指定してwに対応する暗号文C[w]を計算し、さらに前記区間をC[w]によって２つに分割し、前記入力暗号文が前記分割された区間のいずれに属しているかに応じて、属している方の区間を入力として該サブルーチンを再帰的に実行し、前記wに対応する前記暗号文を計算する際には、まず分布決定パラメータvecn'を事前に定められたアルゴリズムに従って選択し、次に前記vecnと前記vecn'と前記区間の両端の値に対応する前記暗号文とを使って選択された分布に従って前記wに対応する前記暗号文を選択し、さらに前記分布に従ってデータを選択する際には擬似乱数を用い、さらに前記入力暗号文がすでに暗号文を計算された値のいずれかと一致するときは該暗号文を出力し、前記定められた分布は、正規分布であることを特徴とする順序保存暗号化システム。

[0178] 以上、実施形態及び実施例を参照して本願発明を説明したが、本願発明は上記実施形態および実施例に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

[0179] この出願は、２０１１年５月１８日に出願された日本特許出願２０１１－１１１５９９を基礎とする優先権を主張し、その開示の全てをここに取り込む。

産業上の利用可能性

[0180] 本発明は、例えばセキュア・データベースに利用できる。データベースに本発明で暗号化されたデータを保管すれば、データの秘密を保持しつつ、順序によるデータ検索が可能になるので産業上有用である。近年のクラウド技

術の発展により、データベースの利用がこれまで以上に増える事が予想されるので、本発明の有用性は今後さらに増すものと思われる。

符号の説明

[0181] １００　暗号化装置

１０１　暗号化手段

２００　復号装置

２０１　復号手段

３００　鍵生成装置

３０１　鍵生成手段

請求の範囲

[請求項1] 暗号文を事前に定められた分布Xに従うデータの和として生成する暗号化手段を含み、

前記暗号化手段は、前記分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する

ことを特徴とする順序保存暗号化システム。

[請求項2] 平文空間の元の数に比例した数のデータを選択し、選択した前記データを全て含む組を鍵として生成し出力する鍵生成手段を含み、

前記鍵生成手段は、前記データを選択する際には、前記データの長さを決定する乱数を選択し、選択した前記乱数に従ったビット長のデータを選択する

請求項１記載の順序保存暗号化システム。

[請求項3] 暗号化手段は、複数のデータの組を含む鍵を暗号化に用い、平文を暗号化するために、前記平文の大きさに比例した数の前記データを足しあわせて暗号化する

請求項１記載の順序保存暗号化システム。

[請求項4] 複数のデータの組を含む鍵を用いて暗号化された暗号文を復号する復号手段を含み、

前記復号手段は、暗号文を復号するために、各mに対してmの大きさに比例した数の前記データを足しあわせた値を計算し、前記足しあわせた値が前記暗号文と一致する前記mを出力し、前記暗号文と一致する前記mが存在しない場合には前記暗号文が不正なものである事を通知する

請求項１記載の順序保存暗号化システム。

[請求項5] 複数のデータの組を含む鍵を暗号化に用いる暗号化手段を含む暗号化装置と、

前記鍵を用いて暗号化された暗号文を復号する復号手段を含む復号

装置とを備え、

平文空間の元の数に比例した数のデータを選択し、選択した前記データを全て含む組を鍵として生成し出力する鍵生成手段を含み、

前記鍵生成手段は、前記データを選択する際には、前記データの長さを決定する乱数を選択し、選択した前記乱数に従ったビット長のデータを選択し、

前記暗号化手段は、前記鍵と平文とを入力して該平文の大きさに比例した数の前記データを足しあわせて暗号化する暗号文を計算し、

前記復号手段は、前記鍵と前記暗号文とを入力して、各mに対してmの大きさに比例した数の前記データを足しあわせた値を計算し、前記足しあわせた値が前記暗号文と一致する前記mを出力し、前記暗号文と一致する前記mが存在しない場合には前記暗号文が不正なものである事を通知する

請求項１記載の順序保存暗号化システム。

[請求項6] K'をランダムに選択し、

分布を決めるパラメータvecn[M]を事前に定められたアルゴリズムに従って選択し、

前記vecn[M]をパラメータとして入力して前記分布に従って暗号文C[M]を選択し、

前記K'と前記vecn[M]と前記C[M]とを含む組を鍵として出力する鍵生成手段を含む

請求項１記載の順序保存暗号化システム。

[請求項7] vecn[M]は、複数のデータを含む組であり、

鍵生成手段は、前記vecn[M]に含まれる前記データを、それらの総和が事前に定められた値になるという条件下で二項分布に従って選択する

請求項６記載の順序保存暗号化システム。

[請求項8] 暗号文を事前に定められた分布Xに従うデータの和として生成する

暗号化手段を含み、

前記暗号化手段は、前記分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する

ことを特徴とする暗号化装置。

[請求項9] 暗号文を事前に定められた分布Xに従うデータの和として生成し、

前記分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する

ことを特徴とする順序保存暗号化方法。

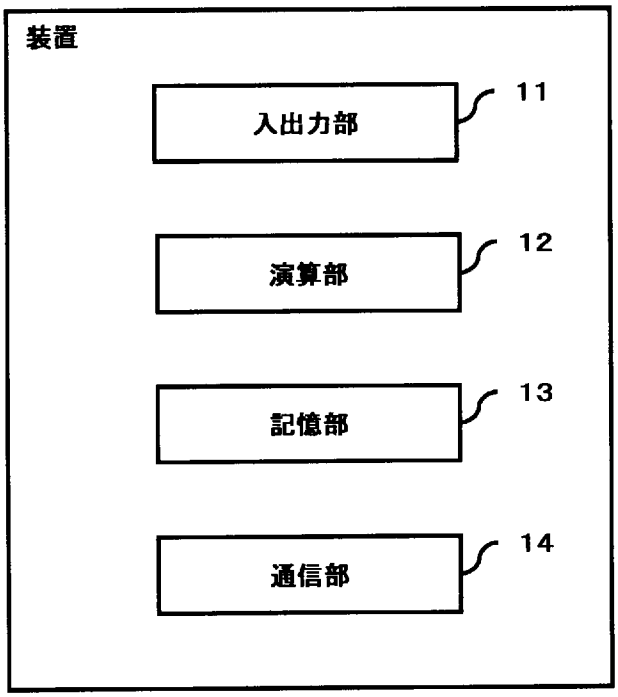
[請求項10] コンピュータに、

暗号文を事前に定められた分布Xに従うデータの和として生成する暗号化処理を実行させ、

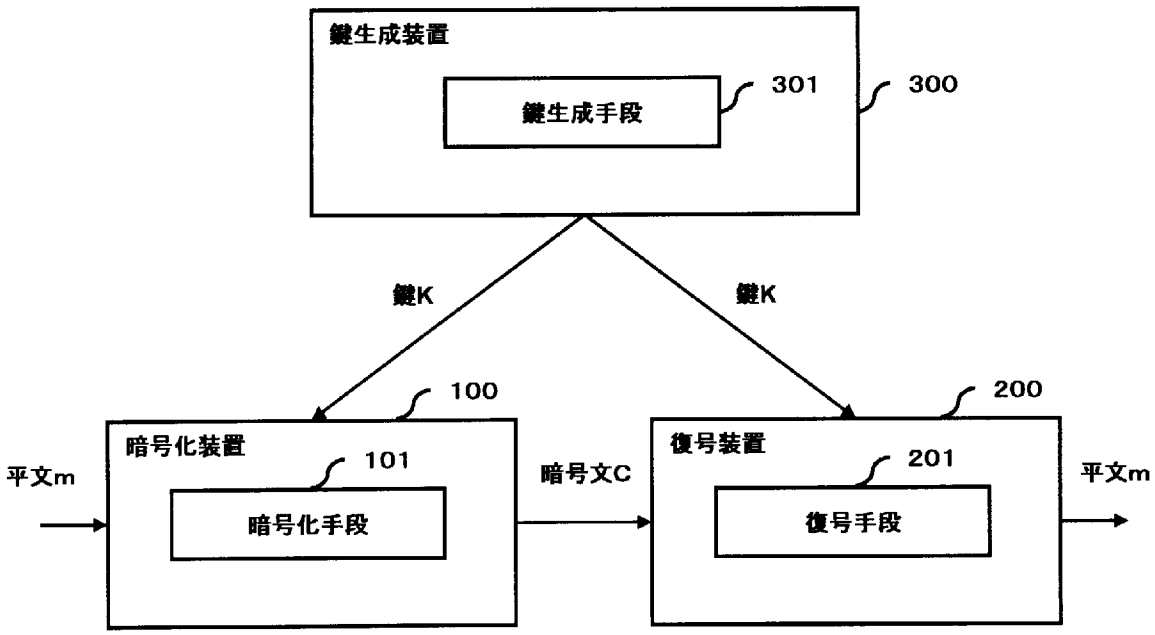
前記暗号化処理で、前記分布Xとして、ランダムに決められたビット長のデータがビット長に応じた分布に従ってランダムに選択されるという形式であらわされる分布を用いて暗号文を生成する処理を

実行させるための順序保存暗号化プログラム。

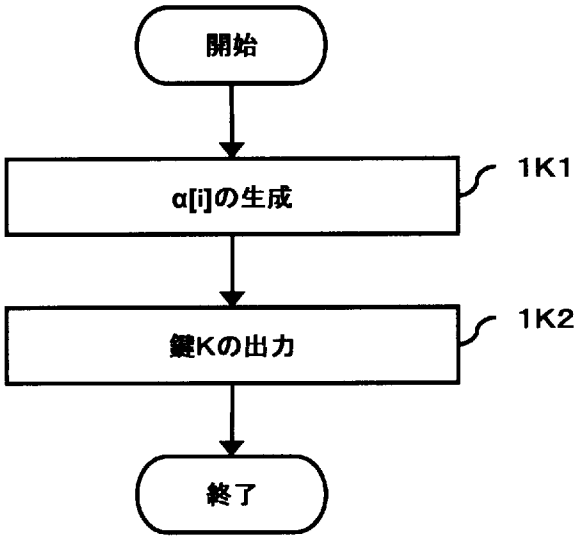
[図1]


装置
入出力部
11
演算部
12
記憶部
13
通信部
14

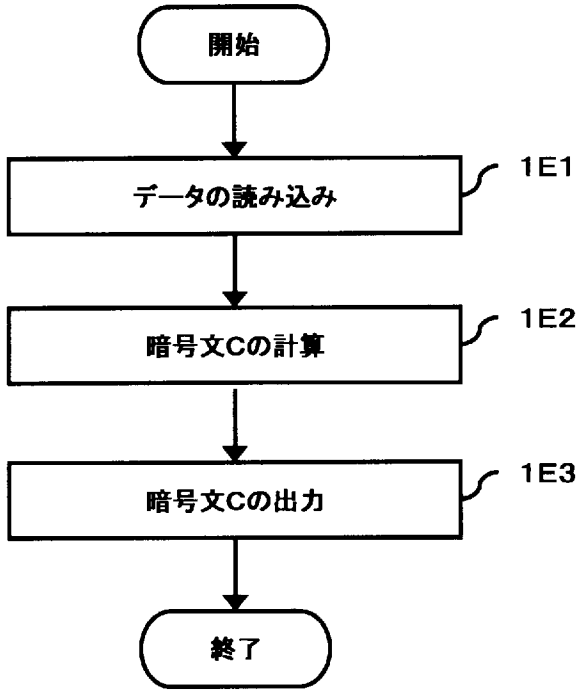
[図2]


鍵生成装置
鍵生成手段
301
300
鍵K
鍵K
100
200
暗号化装置
101
暗号化手段
復号装置
201
復号手段
平文m
暗号文C
平文m

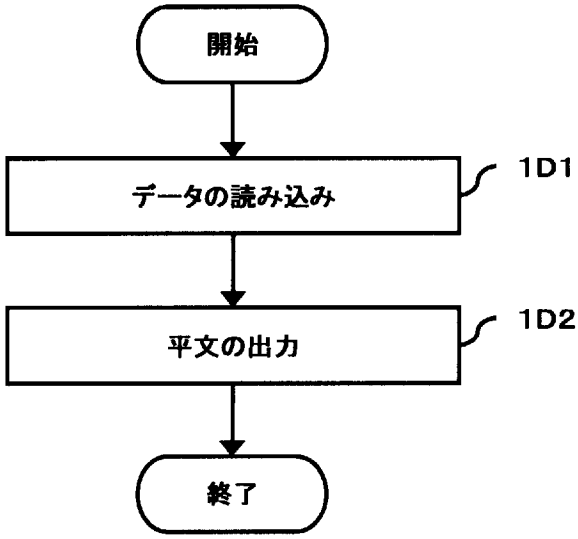
[図3]


開始
α[i]の生成
1K1
鍵Kの出力
1K2
終了

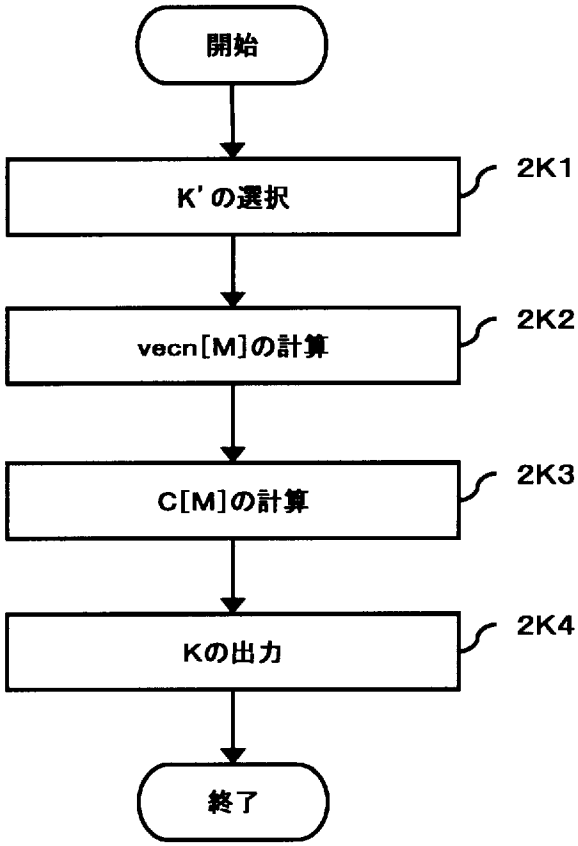
[図4]


開始
データの読み込み
1E1
暗号文Cの計算
1E2
暗号文Cの出力
1E3
終了

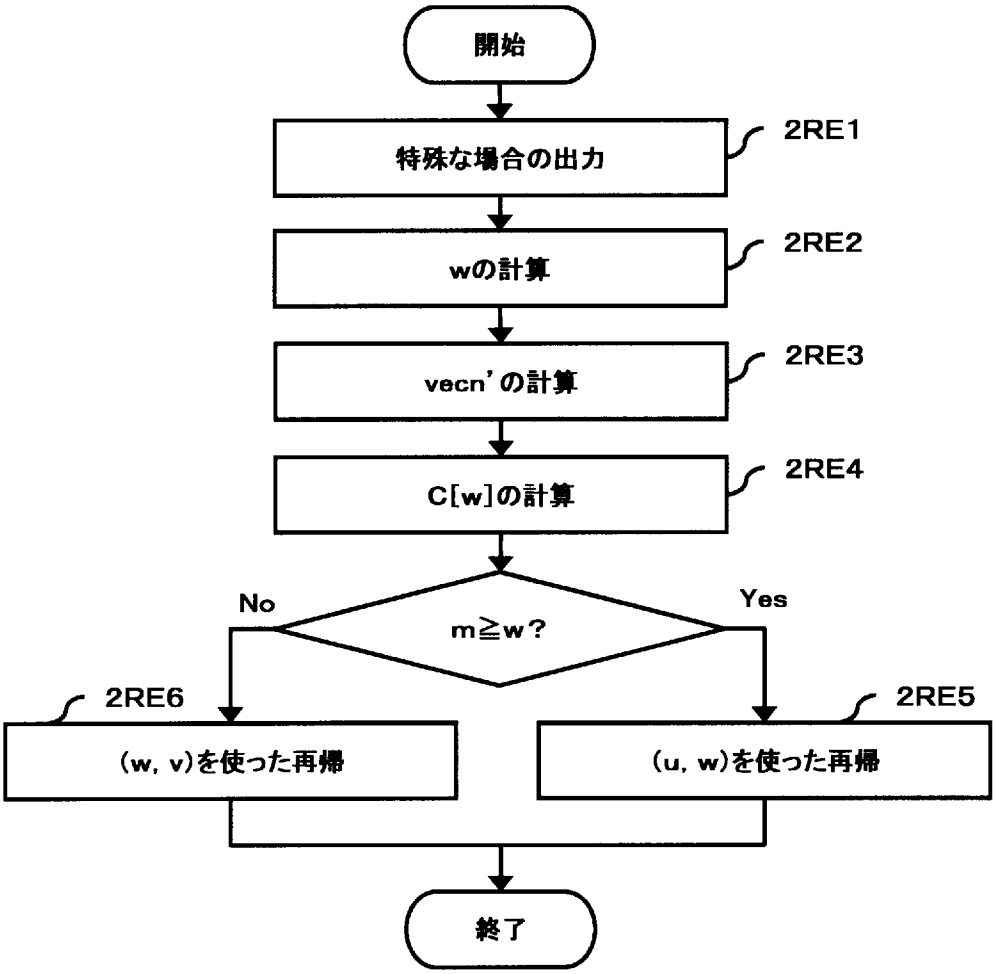
[図5]


開始
データの読み込み
1D1
平文の出力
1D2
終了

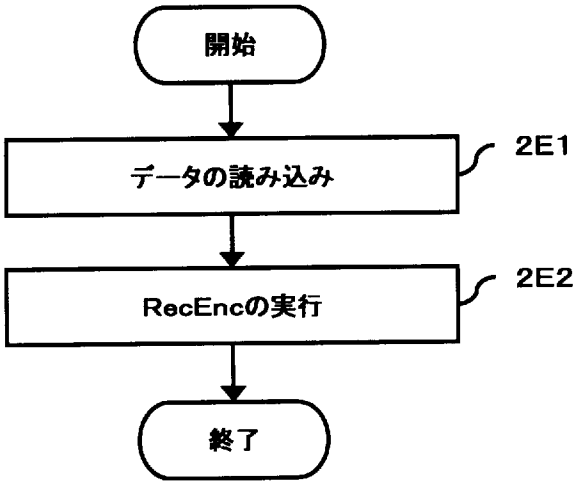
[図6]


開始
K'の選択
2K1
vecn[M]の計算
2K2
C[M]の計算
2K3
Kの出力
2K4
終了

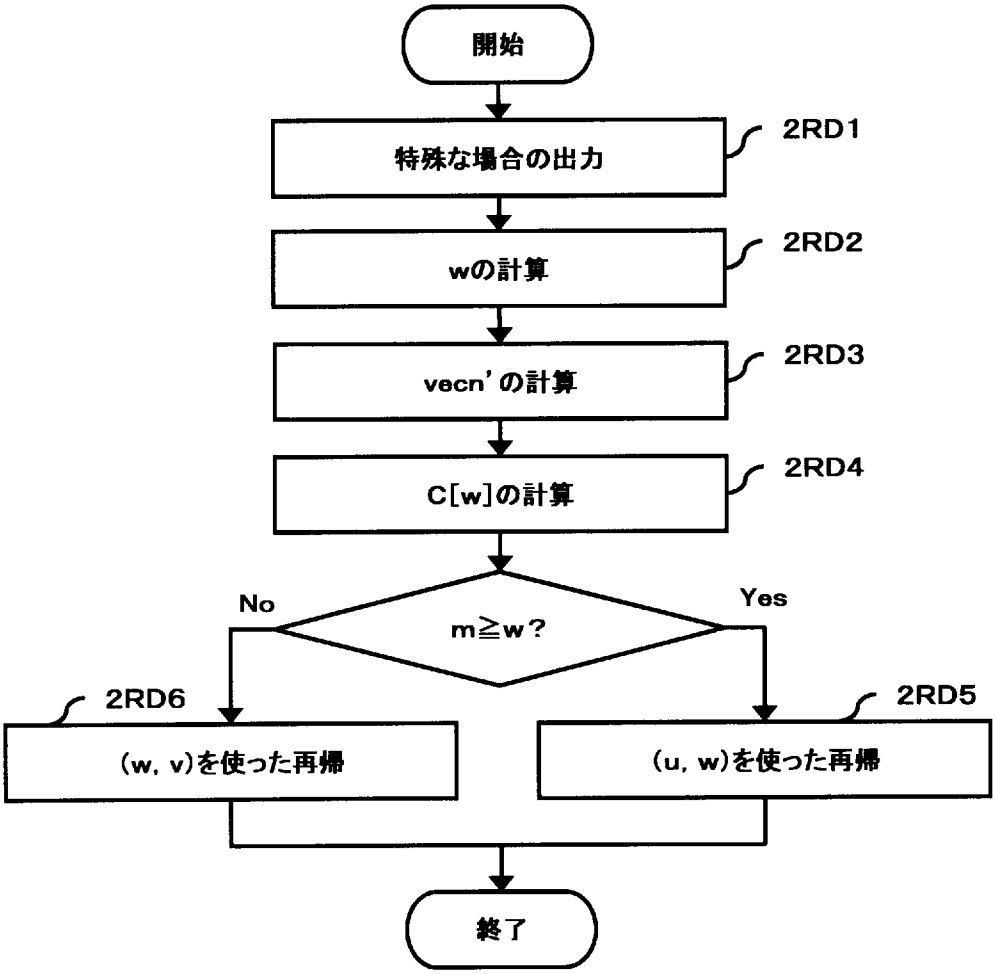
[図7]


開始
特殊な場合の出力
2RE1
wの計算
2RE2
vecn'の計算
2RE3
C[w]の計算
2RE4
No
m≧w?
Yes
2RE6
(w, v)を使った再帰
2RE5
(u, w)を使った再帰
終了

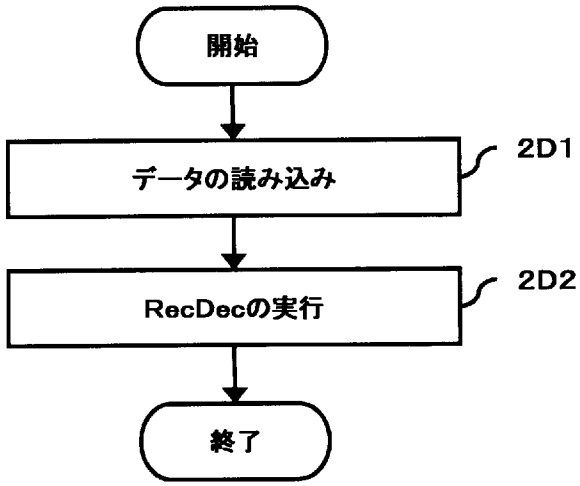
[図8]


開始
データの読み込み
2E1
RecEncの実行
2E2
終了

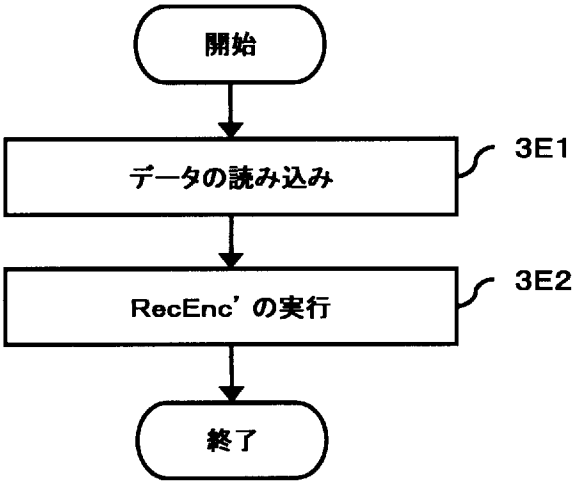
[図9]


開始
特殊な場合の出力
2RD1
wの計算
2RD2
vecn'の計算
2RD3
C[w]の計算
2RD4
No
m≧w?
Yes
2RD6
(w, v)を使った再帰
2RD5
(u, w)を使った再帰
終了

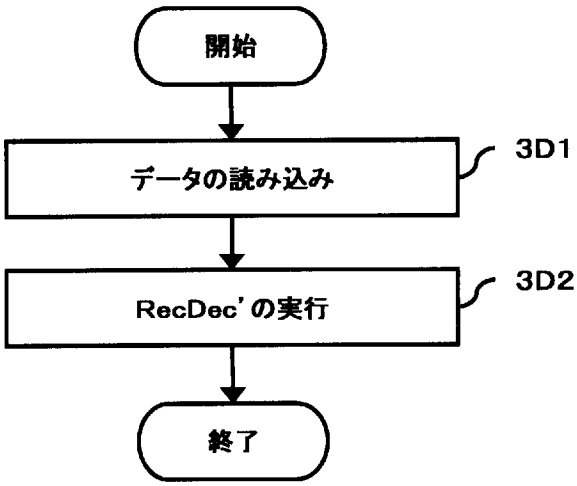
[図10]


開始
データの読み込み
2D1
RecDecの実行
2D2
終了

[図11]


開始
データの読み込み
3E1
RecEnc' の実行
3E2
終了

[図12]


開始
データの読み込み
3D1
RecDec' の実行
3D2
終了

[図13]


暗号化手段
101

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/003239

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/06(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/06, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII) order preserving encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/0147240 A1 (Agrawal, R. et al.), 07 July 2005 (07.07.2005), paragraphs [0055] to [0075] & US 2008/0282096 A1	1-10
A	Boldyreva, A. et al., Order-Preserving Symmetric Encryption, Lecture Notes in Computer Science, Vol.5479, 2009, p.224-241, especially 5.2 Our OPE Scheme and its Analysis, 6.1 Construction of the NGHD-based OPE Scheme	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July, 2012 (10.07.12)	17 July, 2012 (17.07.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／００３２３９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/06(2006.01)i, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/06, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII) order preserving encryption

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 2005/0147240 A1 (Agrawal, R. et al.) 2005.07.07, 55-75段落 & US 2008/0282096 A1	1-10
A	Boldyreva, A. et al., Order-Preserving Symmetric Encryption, Lecture Notes in Computer Science, Vol.5479, 2009, p.224-241, especially 5.2 Our OPE Scheme and its Analysis, 6.1 Construction of the NGHD-based OPE Scheme	1-10

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１０．０７．２０１２	１７．０７．２０１２

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６