(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4623623号
(P4623623)
(45)発行日　平成23年2月2日(2011.2.2)　(24)登録日　平成22年11月12日(2010.11.12)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601A
G06F 21/24	(2006.01)	G06F	12/14	510F
G09C 1/00	(2006.01)	G09C	1/00	660D
H04L 9/32	(2006.01)	H04L	9/00	673A

請求項の数 4　(全 19 頁)

(21)出願番号　特願2003-366538 (P2003-366538)
(22)出願日　平成15年10月27日 (2003.10.27)
(65)公開番号　特開2005-130404 (P2005-130404A)
(43)公開日　平成17年5月19日 (2005.5.19)
審査請求日　平成18年3月30日 (2006.3.30)

前置審査

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100121669
弁理士　本山　泰
(74)代理人　100127535
弁理士　豊田　義元
(72)発明者　廣田　啓一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　北原　亮
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】復元制御型秘密情報分散装置

(57)【特許請求の範囲】
【請求項１】
秘密情報Ｓについて、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、秘密情報の復元を制御した分散情報を生成する復元制御型秘密情報分散装置であって、
分散したい秘密情報Ｓについて、分散条件として、秘密情報Ｓの復元に必要な分散情報の個数の最低数である閾値ｋと、閾値ｋに対して分散情報の数が足りなくても秘密情報Ｓの部分的な復元を許容する分散情報の個数（ｋ－ｄ＋１）を決定するための分割数ｄと、秘密情報Ｓをｄ個に分割した分割情報S_0，S_1，…，S_{d-1}を入力する分散条件入力部と、
閾値ｋと分割数ｄに基づいて、最大の値を持つ分割情報S_t（$0 \leqq t \leqq d-1$）よりも大きな値の素数ｐと、素数ｐよりも小さく０でない（ｋ－ｄ）個の自然乱数r_i（$1 \leqq i \leqq k-d$）と、（ｋ（ｋ－１）／２）個の自然乱数a_j（$1 \leqq j \leqq k(k-1)/2$）を生成して、
$$f(x)=S_0+S_1(x-a_1)+\cdots+S_{d-1}(x-a_{(d-1)(d-2)/2+1})(x-a_{(d-1)(d-2)/2+2})\cdots(x-a_{(d-1)(d-2)/2+d-1})+r_1(x-a_{d(d-1)/2+1})(x-a_{d(d-1)/2+2})\cdots(x-a_{d(d-1)/2+d})+\cdots+r_{k-d}(x-a_{(k-1)(k-2)/2+1})(x-a_{(k-1)(k-2)/2+2})\cdots(x-a_{(k-1)(k-2)/2+k-1})$$

mod p
の式で表現される秘密情報Ｓの分散関数ｆ（ｘ）を生成する分散関数生成部と、
分散関数ｆ（ｘ）から特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、該係数行列のデータを変形して特定のｘの組み合わせから特定の分割情報$Ｓ_{t}$を復元可能とするための制約式を導出する復元条件導出部と、
上記生成された分散関数ｆ（ｘ）と、特定の分割情報$Ｓ_{t}$を復元可能な特定のｘの組み合わせを復元制御情報として出力する分散関数出力部と、
入力された分散条件、生成された分散関数、導出された制約式と復元制御情報を記憶する演算過程記憶部と、
を有する事を特徴とする復元制御型秘密情報分散装置。
【請求項２】
秘密情報Ｓについて、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、秘密情報の復元を制御した分散情報を生成する分散関数の復元制御情報を導出する復元制御型秘密情報分散装置であって、
分散したい秘密情報Ｓについて、分散関数ｆ（ｘ）を入力する分散関数入力部と、
上記入力された分散関数ｆ（ｘ）から、特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、この係数行列のデータを変形して特定のｘの組み合わせから特定の分割情報$Ｓ_{t}$を復元可能とするための制約式を導出する復元条件導出部と、
上記入力された分散関数ｆ（ｘ）に対して特定の分割情報$Ｓ_{t}$を復元可能な特定のｘの組み合わせを復元制御情報として出力する復元制御情報出力部と、
入力された分散関数、導出された制約式と復元制御情報を記憶する演算過程記憶部と、
を有する事を特徴とする復元制御型秘密情報分散装置。
【請求項３】
請求項１に記載の復元制御型秘密情報分散装置であって、
閾値ｋと分割数ｄに対応する、分散関数ｆ（ｘ）の一般形と一般形から導出される制約式を記憶した復元条件記憶部と、
入力された分散条件ないしは分散関数ｆ（ｘ）に従って、条件に合致する分散関数ｆ（ｘ）および制約式を検索する復元条件検索部と、
を有する事を特徴とする復元制御型秘密情報分散装置。
【請求項４】
請求項１から３のいずれか１項に記載の復元制御型情報分散装置であって、
秘密情報Ｓについて、分散情報を生成する個数である分散数ｎに従って、分散関数ｆ（ｘ）と復元制御情報に基づいてｎ個の分散情報を生成する分散情報生成部と、
生成したｎ個の分散情報を、分散情報を計算したｘの値とともに出力する分散情報出力部と、
を有する事を特徴とする復元制御型秘密情報分散装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パスワードや個人情報などの秘密情報を複数の個所に分散共有し、これらの内幾つか以上の分散された情報により元の秘密情報を復元可能とする秘密分散法を用いたセキュリティ技術に関する。
【背景技術】
【０００２】
ネットワーク上でパスワードや個人情報、暗号鍵情報といった各種情報のセキュリテイ（安全性）を保つために、暗号技術が用いられる。この際、ユーザ（利用者）の認証に用いられるパスワードや個人情報、共通鍵暗号に用いる共通鍵や公開鍵暗号に用いる秘密鍵といった秘密情報の保管に関して、秘密情報の紛失や破壊、漏洩や盗難といった恐れがあ

り、特に単一の個所に保管する場合などは秘密情報の紛失や破壊、複数の個所に保管する場合などは秘密情報の漏洩や盗難の可能性が高くなってしまうという問題がある。これらの問題を解決し、各種秘密情報を安全に保管する方法の一つとして、秘密分散法がある。秘密分散法は、元の秘密情報を複数の情報に分散して複数の個所に保管し、この分散された情報（以下、分散情報）を全て、あるいは幾つか合わせる事により、元の秘密情報を復元可能とする方法である。

【０００３】

従来、秘密分散法の実現方法の一つとして、（ｋ，ｎ）閾値秘密分散法がある（例えば、非特許文献１参照）。これは、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋから、秘密情報Ｓを定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、

$$f(x)=S+r_1x+\cdots r_{k-1}x^{k-1} \mod p$$

（r_1，…，r_{k-1}：乱数、ｐ：素数）

として作成し、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（ｉ＝１，２，…，ｎ）に対して、分散情報W_i＝ｆ（ｉ）を分配するものである。

【０００４】

この（ｋ，ｎ）閾値秘密分散法は、ｎ個の分散情報の内、任意のｋ個の分散情報がそろえば、ｆ（ｘ）に関する連立方程式を解く事により元の秘密情報Ｓを復元できるが、任意の（ｋ－１）個までの分散情報がそろってもｆ（ｘ）に関する連立方程式を解く事はできないため、元の秘密情報Ｓは復元できないという特徴がある。したがって、（ｎ－ｋ）個までの分散情報が紛失や破壊により損なわれても元の秘密情報Ｓが復元可能であり、（ｋ－１）個までの分散情報が漏洩や盗難により得られても元の秘密情報Ｓは復元できないという、秘密情報を安全に保管する方法が実現できる。

【０００５】

さらに、（ｋ，ｎ）閾値秘密分散法の拡張として、（ｄ，ｋ，ｎ）閾値秘密分散法がある（例えば、非特許文献２参照）。これは、分散情報を配布する数である２以上の整数の分散数ｎと、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上ｎ以下の整数の閾値ｋと、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄから、秘密情報ＳをS_0，S_1，…，S_{d-1}に分割し、これらの分割した秘密情報（以下、分割情報）を定数項とする（ｋ－１）次の多項式ｆ（ｘ）を、

$$f(x)=S_0+S_1x+\cdots+S_{d-1}x^{d-1}+r_1x^d+\cdots+r_{k-d}x^{k-1} \mod p$$

（r_1，…，r_{k-d}：乱数、ｐ：素数）

として作成し、元の秘密情報Ｓを所有あるいは預託により分配する秘密情報分配者は、分散情報を保管する各分散情報保持者ｉ（１＝１，２，…，ｎ）に対して、分散情報W_i＝ｆ（ｉ）を分配するものである。

【０００６】

この（ｄ，ｋ，ｎ）閾値秘密分散法は、先の（ｋ，ｎ）閾値秘密分散法と同様に、ｎ個の分散情報の内、任意のｋ個の分散情報がそろえば、ｆ（ｘ）に関する連立方程式を解く事により元の秘密情報Ｓを復元できるが、任意の（ｋ－ｄ）個までの分散情報がそろってもｆ（ｘ）に関する連立方程式を解く事はできないため、元の秘密情報Ｓは復元できないという特徴がある。ただし、任意の（ｋ－ｄ＋１）個から（ｋ－１）個までの分散情報がそろった場合には、ｆ（ｘ）に関する連立方程式から分割情報S_0，S_1，…，S_{d-1}に関する関係式が求められるため、分割情報S_0，S_1，…，S_{d-1}として可能な値を得る事ができ、元の秘密情報Ｓを部分的に復元する事ができる。

【０００７】

【非特許文献１】Ａ．Ｓｈａｍｉｒ，“Ｈｏｗ ｔｏ Ｓｈａｒｅ ａ Ｓｅｃｒｅｔ”，Ｃｏｍｍｕｎ．ｏｆ ＡＣＭ，Ｖｏｌ．２２，Ｎｏ．１１，ｐｐ．６１２－６１３，１９７９

【非特許文献２】Ｇ．Ｒ．Ｂlakley, Ｃ．Meadows, “Ｓecurity of ramp schemes”, Proc. of Ｃrypto ’８４, Ｌecure Ｎotes on Ｃomput. Ｓci. , １９６, pp. ２４２－２６８, １９８４

【発明の開示】

【発明が解決しようとする課題】

【０００８】

従来の（ｋ，ｎ）閾値秘密分散法は、ｋ個以上の分散情報を集めて初めて完全な秘密情報Ｓを復元可能であり、（ｋ－１）個以上の分散情報を集めても秘密情報Ｓは復元不可能であるため、秘密情報Ｓに対して部分的に情報を復元するような構成は実現できない。

【０００９】

一方、従来の（ｄ，ｋ，ｎ）閾値秘密分散法は、任意の（ｋ－ｄ＋１）個から（ｋ－１）個までの分散情報がそろった場合には分割情報$Ｓ_{0}$，$Ｓ_{1}$，…，$Ｓ_{d-1}$に関する方程式が求められるため、分割情報$Ｓ_{0}$，$Ｓ_{1}$，…，として可能な値を得る事ができ、元の秘密情報Ｓを部分的に復元する事ができる。しかし、秘密情報Ｓに対して全ての分割情報$Ｓ_{t}$（０≦ｔ≦ｄ－１）を復元可能とするような構成は実現できない。

【００１０】

本発明は、従来の（ｄ，ｋ，ｎ）閾値秘密分散法の上述のような問題に鑑みなされたもので、その目的は、幾つかの特定の分散情報がそろった場合に、特定の分割情報$Ｓ_{t}$（０≦ｔ≦ｄ－１）のみ復元可能であり、他の分割情報$Ｓ_{u}$（０≦ｕ≦ｄ－１，ｕ≠ｔ）は復元不可能であるような、秘密情報Ｓの部分的な復元を制御可能な秘密情報分散装置を提供することにある。

【課題を解決するための手段】

【００１１】

分散情報からの秘密情報Ｓの復元は、各分散情報の番号ｉと分散情報の値$Ｗ_{i}$とを分散関数ｆ（ｘ）にあてはめた連立方程式を解く事により行われる。

【００１２】

従来の（ｄ，ｋ，ｎ）閾値秘密分散法では、例えばｋ＝３、ｄ＝２とした場合に分散関数ｆ（ｘ）は、

$$ｆ（ｘ）＝Ｓ_{0}＋Ｓ_{1}・ｘ＋ｒ・ｘ^{2} \quad \mathrm{mod}\ ｐ$$

で表現され、任意の２個の分散情報$Ｗ_{x}$と$Ｗ_{x+b}$（ｘ，ｂ，ｘ＋ｂ≠０）についての連立方程式は以下のような行列式で表わされる。

【数１】

$$\begin{bmatrix} 1 & x & x^{2} \\ 1 & x+b & (x+b)^{2} \end{bmatrix} \begin{bmatrix} S_{0} \\ S_{1} \\ r \end{bmatrix} \equiv \begin{bmatrix} W_{x} \\ W_{x+b} \end{bmatrix}$$

【００１３】

行列式の左項を掃き出し法により変形すると、

【数２】

$$\begin{bmatrix} 1 & 0 & -x(x+b) \\ 0 & 1 & 2x+b \end{bmatrix}$$

となり、ｘ，ｘ＋ｂ≠０より－ｘ（ｘ＋ｂ）≠０であって、連立方程式からは$Ｓ_{0}$とｒ、$Ｓ_{0}$と$Ｓ_{1}$の関係式しか求める事ができず、したがって分割情報$Ｓ_{0}$を部分的に復元する事は原理的にできない。一方、２ｘ＋ｂ≡０となるｘ，ｂの組み合わせにおいては、$Ｓ_{0}$とｒの関係式及び$Ｓ_{1}$が求められるが、非常に大きな素数ｐの下ではｂ≡ｐ－ｘてある必要があり、そのようなｘ，ｂの組み合わせは現実的ではない。

【００１４】

図１に、本発明の復元制御型秘密情報分散手法の全体的な処理フロー図を示す。以下、

図１にもとづいて本発明の原理を説明する。

本発明は、秘密情報Ｓについて、秘密情報Ｓの完全な復元に必要な分散情報の最低数である２以上の整数の閾値ｋ、閾値ｋに対して秘密情報Ｓの部分的な復元を許容する分散情報の不足数を決定する２以上ｋ以下の整数の分割数ｄと、秘密情報Ｓをｄ個に分割した分割情報S_0，S_1，…，S_{d-1}などの秘密情報Ｓを分散するための条件を入力し（ステップ１）、

最大の分割情報S_t（$0 \leqq t \leqq d-1$）よりも大きな値の素数ｐと、素数ｐよりも小さく０でない（ｋ－ｄ）個の乱数r_i（$1 \leqq i \leqq k-d$）と、（ｋ（ｋ－１）／２）個の乱数a_j（$1 \leqq j \leqq k(k-1)/2$）を生成して、

$$f(x)=S_0+S_1(x-a_1)+\cdots+S_{d-1}(x-a_{(d-1)(d-2)/2+1})(x-a_{(d-1)(d-2)/2+2})\cdots(x-a_{(d-1)(d-2)/2+d-1})+r_1(x-a_{d(d-1)/2+1})(x-a_{d(d-1)/2+2})\cdots(x-a_{d(d-1)/2+d})+\cdots+r_{k-d}(x-a_{(k-1)(k-2)/2+1})(x-a_{(k-1)(k-2)/2+2})\cdots(x-a_{(k-1)(k-2)/2+k-1}) \mod p$$

の式で表現される秘密情報Ｓの分散関数ｆ（ｘ）を生成する（ステップ２）、

ことを第１の特徴とする。ここで、乱数r_i，a_jは自然乱数である。

また、この式を展開すれば、次のような式でも表現できる。

【数３】

$$\begin{aligned}f(x)=&S_0+S_1(x-a_1)+\cdots+S_{d-1}(x^{d-1}-a_{(d-1)(d-2)/2+1}x^{d-2}-a_{(d-1)(d-2)/2+2}x^{d-3}-\cdots-a_{(d-1)(d-2)/2+d-1})\\&+r_1(x^{d}-a_{d(d-1)/2+1}x^{d-1}-a_{d(d-1)/2+2}x^{d-2}-\cdots-a_{d(d-1)/2+d})\\&+\cdots+r_{k-d}(x^{k-1}-a_{(k-1)(k-2)/2+1}x^{k-2}-a_{(k-1)(k-2)/2+2}x^{k-3}\\&-\cdots-a_{(k-1)(k-2)/2+k-1}) \mod p\end{aligned}$$

【００１５】

本発明の第１の特徴によれば、例えばｋ＝３、ｄ＝２とした場合に生成される分散関数ｆ（ｘ）は、

$f(x)=S_0+S_1(x-a_1)+r(x-a_2)(x-a_3) \mod p$

で表現され、任意の２個の分散情報W_xとW_x+bについての連立方程式は以下のような行列式で表現できる。

【数４】

$$\begin{bmatrix}1 & x-a_1 & (x-a_2)(x-a_3)\\ 1 & x+b-a_1 & (x+b-a_2)(x+b-a_3)\end{bmatrix}\begin{bmatrix}S_0\\S_1\\r\end{bmatrix}\equiv\begin{bmatrix}W_x\\W_{x+b}\end{bmatrix}$$

【００１６】

行列式の左項を掃き出し法により変形すると、

【数５】

$$\begin{bmatrix}1 & 0 & -x^2+(2a_1-b)x+a_1b-a_1a_2-a_1a_3+a_2a_3\\ 0 & 1 & 2x+b-a_2-a_3\end{bmatrix}$$

となり、a_1，a_2，a_3の値によっては$-x^2+(2a_1-b)x+a_1b-a_1a_2-a_1a_3+a_2a_3\equiv 0$，$2x+b-a_2-a_3\equiv 0$を満たすｘとｂがある場合に、連立方程式から分割情報のS_0のみ、もしくはS_1のみを求める事ができる。

【００１７】
したがって、本発明の第１の特徴により生成される分散関数ｆ（ｘ）による秘密情報Ｓの分散情報は、幾つかの特定の分散情報がそろった場合に特定の分割情報S_t（$0 \leqq t \leqq d-1$）を復元可能とする事ができる。
【００１８】
本発明の第１の特徴により、ｋ個の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、ｋ個に足りなくても（ｋ－ｄ＋１）個以上の特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報S_tが復元可能であるように、秘密情報の復元を制御した分散情報を生成するための分散関数ｆ（ｘ）を得る事ができる。
【００１９】
本発明は、生成した分散関数ｆ（ｘ）から、特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、この係数行列のデータを掃き出し法により変形して得られる、特定の個数の分散情報から特定の分割情報S_tを復元可能とするような特定のｘの組み合わせを求めるための制約式を解いて、特定の個数の分散情報から特定の分割情報S_tを復元可能とする特定のｘの組み合わせである復元制御情報を導出する（ステップ３）ことを第２の特徴とする。
【００２０】
任意の閾値ｋ、分割数ｄから決定される分散関数ｆ（ｘ）の一般形から、（ｋ－ｄ＋１）個から（ｋ－１）個の任意のx_m（$1 \leqq m \leqq k-d+1 \sim k-1$）について$x_m = x + b_{m-1}$（$b_0 = 0$，$b_1 \neq b_2 \neq \cdots \neq b_{m-1} \neq 0$）とおいて、ｆ（ｘ）に関する連立方程式を表現する以下のような係数行列を作成する事ができる。
【数６】

$$\begin{bmatrix} 1 & x-a_{1,1} & (x-a_{2,1})(x-a_{2,2}) & \cdots & (x-a_{k-1,1})(x-a_{k-1,2})\cdots(x-a_{k-1,k-1}) \\ 1 & x+b_1-a_{1,1} & (x+b_1-a_{2,1})(x+b_1-a_{2,2}) & \cdots & (x+b_1-a_{k-1,1})(x+b_1-a_{k-1,2})\cdots(x+b_1-a_{k-1,k-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x+b_{m-1}-a_{1,1} & (x+b_{m-1}-a_{2,1})(x+b_{m-1}-a_{2,2}) & \cdots & (x+b_{m-1}-a_{k-1,1})(x+b_{m-1}-a_{k-1,2})\cdots(x+b_{m-1}-a_{k-1,k-1}) \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_{d-1} \\ r_1 \\ \vdots \\ r_{k-d} \end{bmatrix}$$

【００２１】
係数行列の左項を掃き出し法により変形すると、
【数７】

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & L_{1,1} & \cdots & L_{1,k-d} \\ 0 & 1 & \cdots & 0 & L_{2,1} & \cdots & L_{2,k-d} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & L_{m,1} & \cdots & L_{m,k-d} \end{bmatrix}$$

の形に変形でき、$L_{m,1} \equiv 0$，$L_{m,2} \equiv 0$，…，$L_{m,k-d} \equiv 0$の場合に連立方程式からS_{m-1}を求める事ができるようになる。
【００２２】
このように、本発明の第２の特徴は、秘密情報Ｓの分散情報を生成するための分散関数ｆ（ｘ）から、特定の個数のｘについての組み合わせの連立方程式を表現する行列式を生成し、この行列式を掃き出し法により変形して、ｘとb_mとa_jからなる関係式である$L_{u,v}$（$1 \leqq u \leqq m$，$1 \leqq v \leqq k-d$）について、$L_{t-1,v} \equiv 0$（$1 \leqq v \leqq k-d$）を解く事により、これを満たすｘおよびb_mの組み合わせを分割情報S_tを復元可能な分散情報の組み合わせとして算出するものである。
【００２３】
本発明の第２の特徴により、幾つかの特定の分散情報がそろった場合に復元可能となる

特定の分割情報S_t（$0 \leqq t \leqq d-1$）について、復元を可能とする特定のｘの組み合わせを求める事が可能となる。

【００２４】

（削除）

【００２５】

また、本発明は、分散条件を入力するステップ１にて、分散情報を生成する個数である分散数ｎを入力すると、ステップ２またはステップ４にて決定された分散関数ｆ（ｘ）から、所定の条件に従ったｎ個の分散情報を生成する（ステップ５）、ことを特徴とする。

また、本発明は、先のステップ２またはステップ４にて決定された分散関数ｆ（ｘ）、ステップ３にて求められた特定のｘの組み合わせから特定の分割情報S_tを復元可能とするための特定のｘの組み合わせである復元制御情報、ステップ５において生成された分散情報を出力する（ステップ６）、ことを特徴とする。

【００２６】

（削除）

【００２７】

本発明による復元制御型秘密情報分散装置は、

分散したい秘密情報Ｓについて、秘密情報Ｓの復元に必要な分散情報の個数の最低数である閾値ｋと、閾値ｋに対して分散情報の数が足りなくても秘密情報Ｓの部分的な復元を許容する分散情報の個数（ｋ－ｄ＋１）を決定する分割数ｄと、秘密情報Ｓをｄ個に分割した分割情報S_0，S_1，…，S_{d-1}の入力を受け付ける分散条件入力部と、

閾値ｋと分割数ｄに基づいて、最大の分割情報S_t（$0 \leqq t \leqq d-1$）よりも大きな値の素数ｐと、素数ｐよりも小さく０でない（ｋ－ｄ）個の自然乱数r_i（$1 \leqq i \leqq k-d$）と、（ｋ（ｋ－１）／２）個の自然乱数a_j（$1 \leqq j \leqq k(k-1)/2$）を生成して、

$$f(x)=S_0+S_1(x-a_1)+\cdots+S_{d-1}(x-a_{(d-1)(d-2)/2+1})(x-a_{(d-1)(d-2)/2+2})\cdots(x-a_{(d-1)(d-2)/2+d-1})+r_1(x-a_{d(d-1)/2+1})(x-a_{d(d-1)/2+2})\cdots(x-a_{d(d-1)/2+d})+\cdots+r_{k-d}(x-a_{(k-1)(k-2)/2+1})(x-a_{(k-1)(k-2)/2+2})\cdots(x-a_{(k-1)(k-2)/2+k-1}) \mod p$$

の式で表現される秘密情報Ｓの分散関数ｆ（ｘ）を生成する分散関数生成部と、

分散関数ｆ（ｘ）から特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、この係数行列のデータを変形して特定のｘの組み合わせから特定の分割情報S_tを復元可能とするための制約式を導出する復元条件導出部と、

上記生成された分散関数ｆ（ｘ）と、特定の分割情報S_tを復元可能な特定のｘの組み合わせを復元制御情報として出力する分散関数出力部と

上記入力された分散条件、生成した分散関数、導出した制約式と復元制御情報を記憶する演算過程記憶部とを有する事を特徴とする。

【００２８】

本発明装置により、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、秘密情報の復元を制御した分散情報を生成する分散関数と、その復元制御情報を導出する復元制御型秘密情報分散装置を実現することができる。

【００２９】

（削除）

【００３０】

（削除）

【００３１】

また、本発明による復元制御型秘密情報分散装置は、

分散したい秘密情報Ｓについて、分散関数ｆ（ｘ）を入力する分散関数入力部と、
入力された分散関数ｆ（ｘ）から、特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、この係数行列のデータを変形して特定のｘの組み合わせから特定の分割情報$Ｓ_{t}$を復元可能とするための制約式を導出する復元条件導出部と、
上記入力された分散関数ｆ（ｘ）に対して特定の分割情報$Ｓ_{t}$を復元可能な特定のｘの組み合わせを復元制御情報として出力する復元制御情報出力部と、
上記入力された分散関数、導出した制約式と復元制御情報を記憶する演算過程記憶部とを有する事を特徴とする。

【００３２】

本発明装置により、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、秘密情報の復元を制御した分散情報を生成する既知の分散関数について、特定の分割情報$Ｓ_{t}$を復元可能な特定のｘの組み合わせである復元制御情報を導出する復元制御型秘密情報分散装置を実現することができる。

【００３３】

また、本発明による復元制御型秘密情報分散装置は、
閾値ｋと分割数ｄに対応する、分散関数ｆ（ｘ）の一般形と一般形から導出される制約式を記録した復元条件記憶部と、
入力された分散条件ないしは分散関数ｆ（ｘ）に従って、条件に合致する分散関数ｆ（ｘ）および制約式を検索する復元条件検索部とを有する事を特徴とする。

【００３４】

本発明装置により、既知の分散条件の下での分散関数および既知の分散関数の一般形については、繁雑な計算を行う事なく分散関数および制約式および復元制御情報を得る復元制御型秘密情報分散装置を実現することができる。

【００３５】

また、本発明による復元制御型秘密情報分散装置は、
秘密情報Ｓについて、分散情報を生成する個数である分散数ｎに従って、分散関数ｆ（ｘ）と復元制御情報に基づいてｎ個の分散情報を生成する分散情報生成部と、
生成したｎ個の分散情報を、分散情報を計算したｘの値とともに出力する分散情報出力部とを有する事を特徴とする。

【００３６】

本発明装置により、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、分散情報を生成する復元制御型秘密情報分散装置を実現することができる。

【発明の効果】

【００３７】

本発明では、秘密情報Ｓについて、所定の数の任意の分散情報を集めると元の秘密情報Ｓが復元可能であって、所定の数に足りなくても特定の分散情報の組み合わせからは秘密情報Ｓの特定の部分情報が復元可能であるように、秘密情報の復元を制御した秘密情報分散を実現する事ができる。

【発明を実施するための最良の形態】

【００３８】

以下、本発明の実施の形態を具体的実施例により説明する。

【実施例１】

【００３９】

図２に本発明の実施例１における復元制御型秘密情報分散装置１００の機能構成例を示す。本装置は、分散条件入力部１１０、分散関数生成部１２０、復元条件導出部１３０、分散関数決定部１４０、分散関数出力部１５０、演算過程記憶部１６０、復元条件記憶部

１７０、復元条件検索部１８０、分散情報生成部１９０、分散情報出力部２００から構成される。なお、これら各部の動作を制御する制御部も具備するが、図２では省略してある。

【００４０】

本実施例では、部分的な分割情報S_0とS_1から構成される秘密情報Ｓを６個の分散情報に分散するものとして、６個の内任意の３個の分散情報を持ち寄れば秘密情報Ｓを完全に復元でき、１番目と２番目の分散情報を持ち寄ると分割情報S_0を、１番目と６番目の分散情報を持ち寄ると分割情報S_1を復元でき、これ以外の任意の２個の分散情報からは秘密情報Ｓを完全には復元できないように、秘密情報Ｓの分散情報を生成するとする。分散の対象とする秘密情報Ｓを４桁の１６進文字列、Ｓ＝３ＣＡＢとし、分割情報はS_0＝３Ｃ、S_1＝ＡＢとする。

【００４１】

まず、分散条件入力部１１０において、ユーザによる分散条件の入力を受け付ける。本実施例における分散条件は、３個の分散情報で完全な復元を許す事から閾値ｋ＝３、２個の分散情報でも部分的な復元を許す事から分割数ｄ＝２、および分割情報S_0＝３Ｃ、S_1＝ＡＢとする。また、分散情報の生成と復元に関する条件として、分散数ｎ＝６と、分割情報S_0を復元可能とする組み合わせ（１，２）、分割情報S_1を復元可能とする組み合わせ（１，６）が入力されたものとする。分散条件入力部１１０は演算過程記憶部１６０に入力された分散条件を記憶する。

【００４２】

なお、本実施例では、分散条件入力部１１０において入力される分散条件を、閾値ｋと分割数ｄ、秘密情報Ｓの分割情報S_0，S_1，…，S_{d-1}の三項目としているが、閾値ｋと分割情報S_0，S_1，…，S_{d-1}の二項目を入力する事で分割数ｄを求めるようにしたり、逆に閾値ｋと分割数ｄ、秘密情報Ｓの三項目の入力を受け付け、入力された秘密情報Ｓから自動的に分割情報S_0，S_1，…，S_{d-1}を生成するようにしても構わない。また、本実施例では秘密情報Ｓに対する分割情報を秘密情報Ｓの上位２桁と下位２桁で分割しているが、本発明は秘密情報Ｓの分割方法を規定するものではなく、例えば奇数ビットと偶数ビットのようにビット単位で分割しても構わないし、分割情報S_0とS_1の積などの演算結果が秘密情報Ｓとなるように分割しても構わない。さらに、本実施例は分散の対象とする秘密情報Ｓを１６進文字列に限定するものではなく、また単なる文字列に限定するものでもない。数値情報、文字列など分散関数による演算が可能であればどのような情報でも良く、また文書や画像データなどのマルチメディアなどを対象としても良い。

【００４３】

また、秘密情報Ｓの分割情報S_0とS_1、および分散情報の生成と復元に関する条件の入力の受け付けについて、説明の都合上、一括して入力されるように記述しているが、これらの値の入力は後の処理で必要となった時に初めて分散条件入力部１１０で入力されるようにしても良い。本実施例は、これら実際の分散情報を生成するための条件の入力を受け付けるタイミングを規定するものではない。また、本実施例は分散条件および分散情報の生成と復元に関する条件の入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。

【００４４】

次に、分散関数生成部１２０において、閾値ｋと分散数ｄおよび分割情報S_0とS_1に基づいて、S_0およびS_1よりも大きな値の素数ｐ、素数ｐよりも小さく０でない乱数ｒ、および３個の変数a_1、a_2、a_3による下記の式で表現される分散関数ｆ（ｘ）の一般形を生成し、これを演算過程記憶部１６０に記憶する。

$$f(x)=S_0+S_1(x-a_1)+r(x-a_2)(x-a_3) \mod p$$

【００４５】

さらに分散関数生成部１２０は、上記の式で表現される分散関数ｆ（ｘ）の一般形における素数ｐ、乱数ｒ、変数a_1、a_2、a_3の値を乱数発生器や素数算出器などを使って生成する。ここでは、素数ｐ＝ＦＢ、乱数ｒ＝１Ｆとａｌ＝０，ａ２＝２，ａ３＝５を生成したものとする。分散関数生成部１２０は処理の結果として、生成した各値、および一般形の分散関数ｆ（ｘ）に生成した各値を埋めた式を演算過程記憶部１６０に記憶する。

【００４６】

なお、本実施例では分散関数生成部１２０において素数ｐや乱数r_i、a_jなどを生成しているが、乱数および素数の生成方法を特に規定するものではない。また、これらの各値について分散条件入力部１１０において入力を受け付けるようにしても良い。

【００４７】

次に、復元条件導出部１３０において、分散関数生成部１２０が生成した分散関数ｆ（ｘ）について、特定の個数のｘについての組み合わせの連立方程式を表現する係数行列のデータを生成し、この係数行列のデータを掃き出し方により変形して特定のｘの組み合わせから特定の分割情報S_tを復元可能とするための制約式を導出する。

【００４８】

本実施例においては、特定の２個の分散情報で秘密情報Ｓの部分的な復元を許す事から、分散関数ｆ（ｘ）から生成される任意の２個の分散情報について、ｆ（ｘ）、ｆ（ｘ＋ｂ）とおいて、分散情報を生成する式の連立方程式を表現する係数行列のデータを、

【数８】

$$\begin{bmatrix} 1 & x-a_1 & (x-a_2)(x-a_3) \\ 1 & x+b-a_1 & (x+b-a_2)(x+b-a_3) \end{bmatrix}$$

のように生成し、演算過程記憶部１６０に記憶する。本実施例は、演算過程記憶部１６０に記憶する係数行列のデータの表現を規定するものではないが、例えば配列表現により記憶するものとして、１行１列目が１、１行２列目がｘ－a_1、…のように記憶したものとする。

【００４９】

さらに復元条件導出部１３０は、演算過程記憶部１６０に記憶した係数行列のデータを掃き出し法により変形を行う。１行１列目の値および２行１列目の値が１であるから、２行目の各列の値から１行目の対応する列の値を引いて、

【数９】

$$\begin{bmatrix} 1 & x-a_1 & (x-a_2)(x-a_3) \\ 0 & b & 2xb-a_2b-a_3b+b^2 \end{bmatrix}$$

【００５０】

２行２列目の値がｂであるから、２行目の各列値をｂで割って、

【数１０】

$$\begin{bmatrix} 1 & x-a_1 & (x-a_2)(x-a_3) \\ 0 & 1 & 2x-a_2-a_3+b \end{bmatrix}$$

１行２列目の値がｘ－a_1であるから、１行目の各列の値から２行目の対応する列の値にｘ－a_1をかけた値を引いて、

【数１１】

$$\begin{bmatrix} 1 & 0 & -x^2+2a_1x-bx+a_1b-a_1a_2-a_1a_3+a_2a_3 \\ 0 & 1 & 2x-a_2-a_3+b \end{bmatrix}$$

を得る。１行１列目および２行２列目の値が１、１行２列目および２行１列目の値が０になった事を判断して、掃き出し法の実行を終了する。

【００５１】
上記の掃き出し法による演算過程について、掃き出し法による行列式の演算は既知の処理である事から、本実施例は特に規定するものではない。また、本実施例では復元条件導出部１３０は演算過程記憶部１６０に記憶した値を操作して掃き出し法を実行しているが、内部メモリなどを用いて予め演算を行った後に演算過程記憶部１６０に記憶するようにしても良い。
【００５２】
上記掃き出し法の実行により演算過程記憶部１６０に記憶された係数行列のデータは、任意の２個の分散情報から得られる分割情報S_0，S_1と乱数値ｒの関係式を表わすものである。したがって、復元条件導出部１３０は、部分的にS_0を復元可能な特定の分散情報ｆ（ｘ）およびｆ（ｘ＋ｂ）を求めるための制約式として、１行３列目の値から、$-x^2+2a_1x-bx+a_1b-a_1a_2-a_1a_3+a_2a_3\equiv 0$を得る。同様に、部分的に$S_1$を復元可能な特定の分散情報ｆ（ｘ）およびｆ（ｘ＋ｂ）を求めるための制約式として、２行３列目の値から、$2x-a_2-a_3+b\equiv 0$を得る。これらの式は、閾値ｋ＝３、分割数ｄ＝２の場合の分散関数ｆ（ｘ）の一般形において、特定の分割情報S_tを復元可能な特定のｘの組み合わせを算出するための制約式である。
【００５３】
復元条件導出部１３０は、復元可能とする特定の分割情報S_0およびS_1と関連付けて、これらの制約式を演算過程記憶部１６０に記憶する。
【００５４】
なお、これらの制約式は分散関数ｆ（ｘ）の一般形が同じであれば常に同じであるため、復元条件導出部１３０で制約式を導出する代わりに、復元条件記憶部１７０において既知の制約式を記憶しておくようにしても良い。即ち、復元条件記憶部１７０は、閾値ｋと分割数ｄにより定まる分散関数ｆ（ｘ）の一般形とその制約式を関連付けて記憶し、復元条件検索部１８０は、入力された分散条件にしたがって、復元条件記憶部１７０に記憶された該当する分散関数ｆ（ｘ）の一般形とその制約式を取得する。これにより、閾値ｋと分割数ｄにより定まる分散関数ｆ（ｘ）の一般形とその制約式を簡易に得る事ができるようになる。復元条件記憶部１７０に該当するものがない場合には、復元条件導出部１３０で制約式を求めておいて復元条件記憶部１７０に記憶し、以後の処理において、復元条件検索部１８０にて検索できるようにしても良い。
【００５５】
分散関数決定部１４０は、復元条件導出部１３０で導出した制約式を解いて、最終的な分散関数ｆ（ｘ）を決定する。まず、分散関数決定部１４０は、S_0に関する制約式$-x^2+2a_1x-bx+a_1b-a_1a_2-a_1a_3+a_2a_3\equiv 0$に対し、３個の変数$a_1=0$，$a_2=2$，$a_3=5$を代入して、$-x^2-bx+10\equiv 0$を得る。さらに、$S_0$を復元可能なｘ，ｂの組み合わせとして、ｘ≧０，ｂ≧１の条件下で制約式を解いて（ｘ，ｂ）＝（１，９），（２，３）を得る。次に、S_0に関する制約式$2x-a_2-a_3+b\equiv 0$に対し、３個の変数$a_1=0$，$a_2=2$，$a_3=5$を代入して、$2x+b-7\equiv 0$を得る。さらに、S_1を復元可能なｘ，ｂの組み合わせとして、ｘ≧０，ｂ≧１の条件下で制約式を解いて（ｘ，ｂ）＝（１，５），（２，３），（３，１）を得る。すなわちS_0を復元可能な分散情報の組み合わせは例えばｆ（１）とｆ（１０），ｆ（２）とｆ（５）であり、S_1を復元可能な分散情報の組み合わせは例えばｆ（１）とｆ（６），ｆ（２）とｆ（５），ｆ（３）とｆ（４）である。これらの組み合わせは、生成した分散関数ｆ（ｘ）により生成される分散情報について、特定の分割情報Ｓｔを復元可能な特定のｘの組み合わせを表わす復元制御情報である。
【００５６】
分散関数決定部１４０は、S_0を復元可能な分散情報の組み合わせとしてｆ（１）とｆ（１０），ｆ（２）とｆ（５）を演算過程記憶部１６０に記憶し、S_1を復元可能な分散情報の組み合わせとしてｆ（１）とｆ（６），ｆ（２）とｆ（５），ｆ（３）とｆ（４）を同じく演算過程記憶部１６０に記憶する。なお、分散情報の組み合わせではなくｘ，ｂ

の組み合わせをそのまま記憶するようにしても良い。

【００５７】

また、分散関数決定部１４０は、演算過程記憶部１６０に記憶した分散条件および分散関数ｆ（ｘ）の一般形から最終的な分散関数ｆ（ｘ）を決定する。本実施例においては、分割情報S_0＝３Ｃ、S_1＝ＡＢ、素数ｐ＝ＦＢ、乱数ｒ＝１Ｆであり、変数a_1、a_2、a_3の値はa_1＝０，a_2＝２，a_3＝５であるから、分散関数ｆ（ｘ）は、ｆ（ｘ）＝３Ｃ＋ＡＢｘ＋１Ｆ（ｘ－２）（ｘ－５）（mod　ＦＢ）と定まる。分散関数決定部１４０は、この最終的な分散関数ｆ（ｘ）を演算過程記憶部１６０に記憶する。

【００５８】

なお、本実施例では分割情報S_0、S_1をはじめとする各種の変数を予め分散条件として入力を受け付け、あるいは決定していたため最終的な分散関数ｆ（ｘ）が定まるが、分割情報S_0、S_1、素数ｐ、乱数ｒなどを予め入力あるいは決定する事なく、分散関数ｆ（ｘ）の一般形あるいは一部の変数を許した式を最終的な分散関数ｆ（ｘ）と定めるようにしても良い。

【００５９】

分散関数出力部１５０は、分散関数決定部１４０において決定した分散関数ｆ（ｘ）およびその復元制御情報を出力する。本実施例においては、分散関数ｆ（ｘ）として、ｆ（ｘ）＝３Ｃ＋ＡＢｘ＋１Ｆ（ｘ－２）（ｘ－５）（mod　ＦＢ）、その復元制御情報として、S_0を復元可能な分散情報の組み合わせｆ（１）とｆ（１０），ｆ（２）とｆ（５）、S_1を復元可能な分散情報の組み合わせｆ（１）とｆ（６），ｆ（２）とｆ（５），ｆ（３）とｆ（４）を出力する。

【００６０】

なお、本実施例では最終的な分散関数ｆ（ｘ）と各分割情報S_0、S_1を復元可能な分散情報の組み合わせを出力しているが、本発明は出力する情報の種類を規定するものではない。他に分散関数の一般形や各変数を独立して出力するようにしても良い。また、本実施例は分散関数ｆ（ｘ）およびその復元制御情報の出力の方法および形式を規定するものではない。画面出力やファイル出力の他に、インターネットなどの接続回線を介して他の装置に出力するようにしても良いし、また必要がなければ出力をしないようにしても良い。

【００６１】

分散情報生成部１９０は、分散関数決定部１４０において決定した分散関数ｆ（ｘ）により、所定の条件に従って分散情報を生成する。本実施例における復元許可条件は、１番目と２番目の分散情報を持ち寄ると分割情報S_0を、１番目と６番目の分散情報を持ち寄ると分割情報S_1を復元できる組み合わせであり、そのような復元が可能な分散情報の組み合わせは、演算過程記憶部１６０に記憶された分散情報の組み合わせからS_0に関してｆ（１）とｆ（１０）、S_1に関してｆ（１）とｆ（６）のみであり、分散情報生成部１９０は１番目の分散情報としてｆ（１）、２番目の分散情報としてｆ（１０）、６番目の分散情報としてｆ（６）を決定する。また、生成する分散情報の数はｎ＝６である事から、残りの分散情報について、特定の分割情報を復元可能な組み合わせを避けて選択し、３番目、４番目、５番目の分散情報としてｆ（７），ｆ（８），ｆ（９）と決定する。分散情報生成部１９０は分散情報の順番をｆ（１），ｆ（１０），ｆ（７），ｆ（８），ｆ（９），ｆ（６）として、演算過程記憶部１６０に記憶する。

【００６２】

さらに分散情報生成部１９０は、分散関数決定部１４０において決定した分散関数ｆ（ｘ）にしたがって、実際の分散情報の値を算出する。本実施例においては、ｆ（１）＝６８，ｆ（１０）＝Ｆ９，ｆ（７）＝３Ｄ，ｆ（８）＝Ｅ５，ｆ（９）＝ＤＯ，ｆ（６）＝ＣＥとなり、分散情報生成部１９０は分散情報の順番に対応付けて分散情報の値を演算過程記憶部１６０に記憶する。

【００６３】

なお、本実施例において、分散関数ｆ（ｘ）から分散情報を算出する際のｘの値を１０

進数の数字により記述しているが、可能なｘの値を１０進数の数字に規定するものではない。分散関数ｆ（ｘ）に則って分散情報を算出できれば良く、例えば１６進数であったり文字列であったりしても構わない。本実施例においては、秘密情報Ｓおよびその分割情報S_0、S_1が１６進文字列である事から、算出される分散情報の値も１６進文字列となっている。

【００６４】

分散情報出力部２００は、分散情報生成部１９０において生成した分散情報を、分散情報を算出したｘの値と組にして出力する。本実施例における出力は、（１，６８），（１０，Ｆ９），（７，３Ｄ〉，（８，Ｅ５），（９，ＤＯ），（６，ＣＥ）となる。本実施例における分散情報の出力の例を図３に示す。

【００６５】

なお、本実施例は分散情報出力部２００における分散情報の出力の方法および形式を規定するものではない。画面出力やファイル出力の他に、インターネットなどの接続回線を介して他の装置に出力するようにしても良い。ただし、出力した分散情報を複数組み合わせると元の秘密情報Ｓないしはその部分的な情報S_0，S_1が算出可能な事から、個々の分散情報を別個に出力する事が望ましい。また分散情報は直接各分散情報保持者または名分散情報保持装置に出力するようにし、出力の際に個々の保持者ないしは装置に合わせて暗号化するなどの手段も考える事もできる。

【００６６】

以下では、本実施例により生成した分散情報から、分割情報S_0およびS_1、さらに秘密情報Ｓを復元する方法について説明する。

【００６７】

任意の２個の分散情報からの秘密情報の復元については、不明な分割情報S_0、S_1、乱数ｒとおいた分散関数ｆ（ｘ）の式に、実際のｘの値および分散情報の値をあてはめた連立方程式を解く事により求められる。

【００６８】

例えば、１番目と２番目の分散情報からは、ｆ（１）＝６８，ｆ（１０）＝Ｆ９より

$f(1)=S_0+S_1\cdot 1+r\cdot(1-2)(1-5)=S_0+S_1+4r\equiv 68 \pmod{FB}$

$f(10)=S_0+S_1\cdot 10+r\cdot(10-2)(10-5)=S_0+10S_1+40r\equiv F9 \pmod{FB}$

の連立方程式を得る事ができる。これを解くと、$S_0\equiv 3C$、$S_1+4r\equiv 2C$が求められ、秘密情報Ｓの分割情報S_0が得られる。

【００６９】

一方、１番目と６番目の分散情報からは、ｆ（１）＝６８，ｆ（６）＝ＣＥより

$f(1)=S_0+S_1\cdot 1+r\cdot(1-2)(1-5)=S_0+S_1+4r\equiv 68 \pmod{FB}$

$f(6)=S_0+S_1\cdot 6+r\cdot(6-2)(6-5)=S_0+6S_1+4r\equiv CE \pmod{FB}$

の連立方程式が得られる。これを解くと、$S_1\equiv AB$、$S_0+4r\equiv B8$が求められ、秘密情報Ｓの分割情報S_1が得られる。

【００７０】

ただし、これ以外の任意の分散情報の組からは、例えばｆ（１０）＝Ｆ９，ｆ（６）＝ＣＥより

$f(10)=S_0+S_1\cdot 10+r\cdot(10-2)(10-5)=S_0+10S_1+40r\equiv F9 \pmod{FB}$

$f(6)=S_0+S_1\cdot 6+r\cdot(6-2)(6-5)=S_0+6S_1+4r\equiv CE \pmod{FB}$

の連立方程式が得られるが、これを解いても、$9S_0+50S_1\equiv 36 \pmod{FB}$という分割情報$S_0$と$S_1$の関係式が得られるのみで、秘密情報Ｓを完全には復元できない

。本実施例における分散情報の組み合わせにより得られる分割情報の関係式を図４に示す。

【００７１】

なお、任意の３個の分散情報からは、例えばｆ（７）＝３Ｄ，ｆ（８）＝Ｅ５，ｆ（９）＝Ｄ０より

ｆ（７）＝S_0＋S_1・７＋ｒ・（７－２）（７－５）＝S_0＋７S_1＋１０ｒ≡３Ｄ

ｆ（８）＝S_0＋S_1・８＋ｒ・（８－２）（８－５）＝S_0＋８S_1＋１８ｒ≡Ｅ５

ｆ（９）＝S_0＋S_1・９＋ｒ・（９－２）（９－５）＝S_0＋９S_1＋２８ｒ≡ＤＯ

のような連立方程式が得られ、これを解くと、S_0≡３Ｃ，S_1≡ＡＢ，ｒ≡１Ｆが求められ、秘密情報Ｓが完全に復元される。

【００７２】

以上のように、本実施例により生成した秘密情報Ｓの分散情報は、６個の内任意の３個の分散情報を持ち寄れば秘密情報Ｓを完全に復元でき、１番目と２番目の分散情報を持ち寄ると分割情報S_0を、１番目と６番目の分散情報を持ち寄ると分割情報S_1を復元でき、これ以外の任意の２個の分散情報からは秘密情報Ｓを完全には復元できないように生成されている。

【実施例２】

【００７３】

図５は、本発明の実施例２における復元制御型秘密情報分散装置３００の機能構成例を示す。本復元制御型秘密情報装置３００は、分散関数入力部３１０、復元条件導出部３２０、復元制御情報出力部３３０、演算過程記憶部３４０から構成される。図５でも、各部の動作を制御するための制御部は省略する。

【００７４】

本実施例は、秘密情報Ｓを分散するための既知の分散関数ｆ（ｘ）を入力として、秘密情報Ｓの分割情報S_0，S_1，…，S_{d-1}について部分的な復元の可否および部分的な復元が可能な組み合わせである復元制御情報を算出するものである。

【００７５】

分散関数入力部２１０において、復元制御情報を求める分散関数ｆ（ｘ）の入力を受け付ける。本実施例では、分散関数ｆ（ｘ）として、

ｆ（ｘ）＝S_0＋S_1（ｘ－６）＋ｒ（ｘ－３）（ｘ－４）mod　ｐ

が入力されたものとする。分散関数入力部２１０は、入力された分散関数ｆ（ｘ）を演算過程記憶部３４０に入力された式を記憶する。

【００７６】

なお、本実施例は、分散関数入力部３１０における分散関数ｆ（ｘ）の入力の方法および形式を規定するものではない。キーボード入力やファイル入力の他に、インターネットなどの接続回線を介して他の装置から入力するようにしても構わない。また、具体的な値を一切含む事なく、分散関数ｆ（ｘ）の一般形を入力として受け付けるようにしても良い。また、本実施例では入力された分散関数ｆ（ｘ）の式について、分割情報S_0、S_1や乱数ｒ、素数ｐの値の入力はなかったものとしたが、予め入力を受け付けるようにしても良い。また分散関数入力部２１０が演算過程記憶部３４０に記憶する形式は、分散関数ｆ（ｘ）の式だけでなく、各変数や項の値を記録するようにしても良い。

【００７７】

復元条件導出部３２０は、入力された分散関数ｆ（ｘ）から特定の個数のｘについての組み合わせの連立方程式を表現する行列式を生成し、この行列式を変形して特定のｘの組み合わせから特定の分割情報S_tを復元可能とするための制約式を導出する。

【００７８】

本実施例においては、分散関数ｆ（ｘ）が分割情報S_0、S_1とｒの式で表現される事から、

【数１２】

$$\begin{bmatrix} 1 & x-a_1 & (x-a_2)(x-a_3) \\ 1 & x+b-a_1 & (x+b-a_2)(x+b-a_3) \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ r \end{bmatrix}$$

のように生成し、この左項を掃き出し法により変形して、

【数１３】

$$\begin{bmatrix} 1 & 0 & -x^2+2a_1x-bx+a_1b-a_1a_2-a_1a_3+a_2a_3 \\ 0 & 1 & 2x-a_2-a_3+b \end{bmatrix}$$

を得る。したがって、部分的にＳ$_0$を復元可能な特定の分散情報ｆ（ｘ）およびｆ（ｘ＋ｂ）に関する制約式は－ｘ^2＋２ａ$_1$ｘ－ｂｘ＋ａ$_1$ｂ－ａ$_1$ａ$_2$－ａ$_1$ａ$_3$＋ａ$_2$ａ$_3$≡０、部分的にＳ$_1$を復元可能な特定の分散情報ｆ（ｘ）およびｆ（ｘ＋ｂ）に関する制約式は２ｘ－ａ$_2$－ａ$_3$＋ｂ≡０である。

【００７９】

次に、復元条件導出部３２０は、演算過程記憶部３４０に記憶した分散関数ｆ（ｘ）の式から変数ａ$_1$、ａ$_2$、ａ$_3$の値を得て、制約式に代入してｘとｂの組み合わせを算出する。本実施例ではａ$_1$＝６，ａ$_2$＝３，ａ$_3$＝４であるから、Ｓ$_0$を復元可能なｘとｂの組み合わせの制約式は－ｘ^2＋１２ｘ－ｂｘ＋６ｂ－３０≡０となり、ｘ≧０，ｂ≧１の条件下で制約式を解くと、ｂがうまく割り切れない場合を除いて（ｘ，ｂ）＝（３，１），（７，５），（８，１）を得る。一方、Ｓ$_0$を復元可能なｘとｂの組み合わせの制約式は２ｘ＋ｂ－７≡０となり、同様にｘ≧０，ｂ≧１の条件下で制約式を解くと、（ｘ，ｂ）＝（１，５），（２，３），（３，１）を得る。復元制御情報は、Ｓ$_0$を復元可能な分散情報の組み合わせとして例えばｆ（３）とｆ（４），ｆ（７）とｆ（１２），ｆ（８）とｆ（９）、Ｓ$_1$を復元可能な分散情報の組み合わせとして例えばｆ（１）とｆ（６），ｆ（２）とｆ（５），ｆ（３）とｆ（４）となる。復元条件導出部３２０は、これらの組み合わせを演算過程記憶部３４０に記憶する。

【００８０】

（削除）

【００８１】

復元制御情報出力部３３０は、復元条件導出部３２０において得られた復元制御情報を出力する。本実施例では、Ｓ$_0$を復元可能な分散情報の組み合わせとしてｆ（３）とｆ（４），ｆ（７）とｆ（１２），ｆ（８）とｆ（９）、Ｓ$_1$を復元可能な分散情報の組み合わせとしてｆ（１）とｆ（６），ｆ（２）とｆ（５），ｆ（３）とｆ（４）を出力する。

【００８２】

なお、本実施例は分散関数ｆ（ｘ）およびその復元制御情報の出力の方法および形式を規定するものではなく、画面出力やファイル出力の他に、インターネットなどの接続回線を介して他の装置に出力するようにしても良いし、また必要がなければ出力をしないようにしても良い。また、分散関数入力部３１０において分割情報Ｓ$_0$、Ｓ$_1$や乱数ｒ、素数ｐの値が入力されていた場合には、各分散情報の値も算出して出力するようにしても良い。

【００８３】

以上のように、本実施例における復元制御型秘密情報分散装置３００は，分散関数ｆ（ｘ）を入力として、分散関数ｆ（ｘ）により生成される秘密情報Ｓの分散情報について、特定の分割情報Ｓ$_t$を復元可能とする特定のｘの組み合わせを求める事ができる。

【００８４】

なお、図２や図５で示した復元制御型秘密情報分散装置における各部の一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明装置を実現することができること、あるいは、図１で示したような処

理手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができることは言うまでもなく、コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、ＦＤ、ＭＯ、ＲＯＭ、メモリカード、ＣＤ、ＤＶＤ、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

【図面の簡単な説明】

【００８５】

【図１】本発明の復元制御型秘密情報分散方法の処理フロー図である。

【図２】本発明の復元制御型秘密情報分散装置の実施例１の機能構成図である。

【図３】実施例１における生成した分散情報の例である。

【図４】実施例１における分散情報の組み合わせと復元情報の例である。

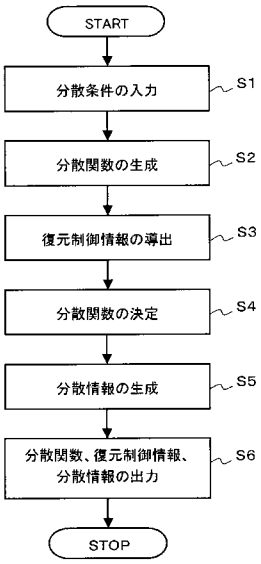
【図５】本発明の復元制御型秘密情報分散装置の実施例２の機能構成図である。

【符号の説明】

【００８６】

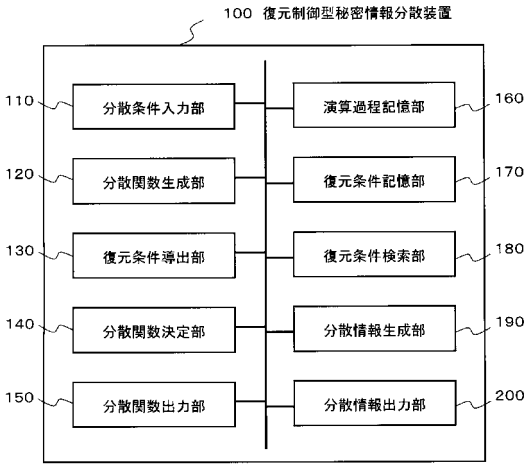
１００　復元制御型秘密情報分散装置
１１０　分散条件入力部
１２０　分散関数生成部
１３０　復元条件導出部
１４０　分散関数決定部
１５０　分散関数出力部
１６０　演算過程記憶部
１７０　復元条件記憶部
１８０　復元条件検索部
１９０　分散情報生成部
２００　分散情報出力部
３００　復元制御型秘密情報分散装置
３１０　分散関数入力部
３２０　復元条件導出部
３３０　復元制御情報出力部
３４０　演算過程記憶部

【図１】



本発明の復元制御型秘密情報分散方法の処理フロー図

【図２】



本発明の実施例1の復元制御型秘密情報分散装置の機能構成図

【図３】

順番 i	番号	分散情報
1	1	68
2	10	F9
3	7	3D
4	8	E5
5	9	D0
6	6	CE

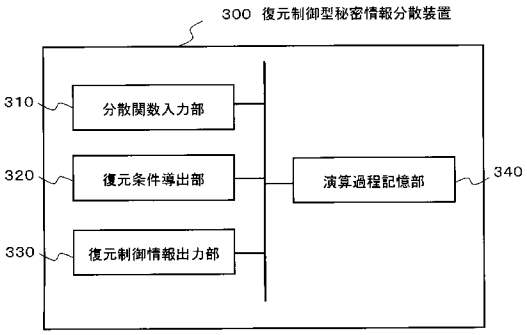
実施例1における生成した分散情報の例

【図４】

順番 i	1	2	3	4	5	6
6		S_1=AB S_0+4i=D8	$9S_0$+50S_1=36	$3S_0$+16S_1=9B	$7S_0$+38S_1=8D	$6S_0$+33S_1=E6
5		$6S_0$−2S_1=12	$3S_0$+20S_1=56	$9S_0$+53S_1=41	$5S_0$+31S_1=4F	
4		$7S_0$−7S_1=E3	$11S_0$+70S_1=50	$4S_0$+23S_1=9D		
3		$3S_0$−9S_1=93	$3S_0$+18S_1=F6			
2	S_0=3C S_1+4i=2C					
1						

実施例1における分散情報の組み合わせと復元情報の例

【図５】



本発明の実施例2の復元制御型秘密情報分散装置の機能構成図

フロントページの続き

(72)発明者　林　　良一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　遠藤　雅和
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山室　雅司
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　金沢　史明

(56)参考文献　圓藤康平、松村靖子、中川聰、福永茂，情報量的安全性に基づく分散計算法のランプ型秘密分散法を用いた効率化，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００３年　5月１４日，Vol.103、No.61，pp.57-62
岩本貢、山本博資、小川博久，（ｋ，ｎ）しきい値法と整数計画法による秘密分散法の一般的構成法，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００３年　5月１４日，Vol.103、No.61，pp.63-70
尾形わかは、黒沢馨，秘密分散共有法とその応用，電子情報通信学会誌，日本，社団法人電子情報通信学会，１９９９年１２月２５日，第82巻、第12号，pp.1228-1236
廣田啓一、北原亮、遠藤雅和、山室雅司，ランプ型閾値秘密分散法における部分情報の復元制御，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００３年１１月　6日，Vol.103、No.416，pp.57-64

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２４
ＣｉＮｉｉ
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）