(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第5957120号
(P5957120)
(45)発行日　平成28年7月27日(2016.7.27)　(24)登録日　平成28年6月24日(2016.6.24)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 650Z

請求項の数 6 (全 15 頁)

(21)出願番号　特願2015-97278(P2015-97278)
(22)出願日　平成27年5月12日(2015.5.12)
審査請求日　平成27年5月12日(2015.5.12)

(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一丁目５番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(72)発明者　五十嵐　大
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】秘密分散方法、秘密分散システム、分散装置、およびプログラム

(57)【特許請求の範囲】
【請求項１】
xは拡大体GF(x^q)を生成する既約多項式f[X]の元Xであり、n，kは2以上の整数であり、n≧2k-1であり、p_0，…，p_{k-1}は0以上n未満の相異なる整数であり、Aは次式で定義されるn行k列の行列であり、
【数２３】

$$A_{ij}=\begin{cases}1 & \text{if } i=j \text{ and } i<k-1\\ 0 & \text{if } i\neq j \text{ and } i<k-1\\ x^{(i-k-1)j} & \text{if } i\geq k-1\end{cases}$$

ただし、

$$i\in\{0,\ldots,n-1\},j\in\{0,\ldots,k-1\}$$

分散装置が、乱数r_0，…，$r_{k-2}\in GF(x^q)$を生成する乱数生成ステップと、
上記分散装置が、上記乱数r_0，…，r_{k-2}と平文$s\in GF(x^q)$を要素とするベクトル$a=(r_0,\ldots,r_{k-2},s)$と上記行列Aとの乗算を計算することでシェアb_0，…，b_{n-1}を生成するシェア生成ステップと、
復元装置が、上記シェアb_0，…，b_{n-1}から選択したk個のシェアb_{p0}，…，b_{pk-1}を要素とするベクトル$b'=(b_{p0},\ldots,b_{pk-1})$を生成するシェア選択ステップと、
上記復元装置が、上記行列Aのp_0，…，p_{k-1}行目からなるk次正方行列の逆行列A'^{-1}を生

成する逆行列生成ステップと、
上記復元装置が、上記逆行列A'^{-1}のk行目とベクトルb'を乗算して上記平文sを復元する平文計算ステップと、
を含む秘密分散方法。
【請求項２】
請求項１に記載の秘密分散方法であって、
qは拡大体$GF(x^q)$の拡大次数であり、dは既約多項式f[X]から最高次項を除いた多項式f'の最高次項の次数であり、m=n-kであり、(m-1)(k-1)≦q-dであり、
上記シェア生成ステップは、i∈{0，…，m-1}について次式により値c_iを計算し、上記値c_iのq次以上の部分をX^qで割った多項式h_iと、上記値c_iのq次未満の部分である多項式g_iとを用いて、g_i-h_if'を計算して上記値c_iを更新し、上記値c_0，…，c_{m-1}を上記シェアb_0，…，b_{n-1}とするものである、
【数２４】

$$c_i = \sum_{0 \le j < k-1} r_j x^{ij} + s x^{i(k-1)}$$

秘密分散方法。
【請求項３】
請求項１に記載の秘密分散方法であって、
qは拡大体$GF(x^q)$の拡大次数であり、dは既約多項式f[X]から最高次項を除いた多項式f'の最高次項の次数であり、m=n-kであり、
上記シェア生成ステップは、j∈{0，…，k-1}について$a'_j=a_j$，$d_j=0$とし、i∈{0，…，m-1}について次式により値c_iを計算し、上記値c_iのq次以上の部分をX^qで割った多項式h_iと、上記値c_iのq次未満の部分である多項式g_iとを用いて、g_i-h_if'を計算して上記値c_iを更新し、i∈{0，…，m-1}，j∈{0，…，k-1}について、i≠m-1、かつ、(i+1)j-d≧q-dであれば、$a'_j:=a'_jx^{\alpha}$，$d_j:=d_j+\alpha$と更新し、上記値c_0，…，c_{m-1}を上記シェアb_0，…，b_{n-1}とするものである、
【数２５】

$$c_i = \sum_{0 \le j < k} a'_j x^{ij-d_j}$$

秘密分散方法。
【請求項４】
分散装置と復元装置とを含む秘密分散システムであって、
xは拡大体$GF(x^q)$を生成する既約多項式f[X]の元Xであり、n，kは2以上の整数であり、n≧2k-1であり、p_0，…，p_{k-1}は0以上n未満の相異なる整数であり、Aは次式で定義されるn行k列の行列であり、
【数２６】

$$A_{ij} = \begin{cases} 1 & \text{if } i = j \text{ and } i < k-1 \\ 0 & \text{if } i \neq j \text{ and } i < k-1 \\ x^{(i-k-1)j} & \text{if } i \geq k-1 \end{cases}$$

ただし、

$$i \in \{0,\ldots,n-1\}, j \in \{0,\ldots,k-1\}$$

上記分散装置は、
乱数r_0，…，$r_{k-2}\in GF(x^q)$を生成する乱数生成部と、
上記乱数r_0，…，r_{k-2}と平文$s\in GF(x^q)$を要素とするベクトルa=(r_0，…，r_{k-2}，s)と上記行列Aとの乗算を計算することでシェアb_0，…，b_{n-1}を生成するシェア生成部と、
を含み、

上記復元装置は、

上記シェアb_0，…，b_{n-1}から選択したk個のシェアb_{p0}，…，b_{pk-1}を要素とするベクトル$b'=(b_{p0}$，…，$b_{pk-1})$を生成するシェア選択部と、

上記行列Aのp_0，…，p_{k-1}行目からなるk次正方行列の逆行列A'^{-1}を生成する逆行列生成部と、

上記逆行列A'^{-1}のk行目とベクトルb'を乗算して上記平文sを復元する平文計算部と、

を含む秘密分散システム。

【請求項５】

xは拡大体$GF(x^q)$を生成する既約多項式f[X]の元Xであり、n，kは2以上の整数であり、$n \geqq 2k-1$であり、p_0，…，p_{k-1}は0以上n未満の相異なる整数であり、Aは次式で定義されるn行k列の行列であり、

【数２７】

$$A_{ij}=\begin{cases}1 & \text{if } i=j \text{ and } i<k-1\\ 0 & \text{if } i\neq j \text{ and } i<k-1\\ x^{(i-k-1)j} & \text{if } i\geq k-1\end{cases}$$

ただし、

$$i\in\{0,\ldots,n-1\},j\in\{0,\ldots,k-1\}$$

乱数r_0，…，$r_{k-2}\in GF(x^q)$を生成する乱数生成部と、

上記乱数r_0，…，r_{k-2}と平文$s\in GF(x^q)$を要素とするベクトル$a=(r_0$，…，r_{k-2}，s)と上記行列Aとの乗算を計算することでシェアb_0，…，b_{n-1}を生成するシェア生成部と、

を含む分散装置。

【請求項６】

請求項５に記載の分散装置としてコンピュータを機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、秘密分散技術に関し、特に、情報理論型秘密分散の計算量を低減する技術に関する。

【背景技術】

【０００２】

従来の情報理論型秘密分散には、例えば、非特許文献１に記載されたShamirの秘密分散や、非特許文献２に記載されたXORベースの秘密分散がある。

【０００３】

Shamirの秘密分散およびXORベースの秘密分散は(k,n)-秘密分散の一つである。(k,n)-秘密分散は、入力された平文をn個に分割した分散値をn個のパーティに分散して保持しておき、任意のk個のシェアが揃えば平文を復元でき、k個未満のシェアからは平文に関する一切の情報を得られないような秘密分散である。このとき、n，kは2以上の整数であり、$n \geqq 2k-1$である。

【先行技術文献】

【非特許文献】

【０００４】

【非特許文献１】A. Shamir，“How to share a secret”，Communications of the ACM, vol. 22(11), pp. 612-613, 1979.

【非特許文献２】J. Kurihara, S. Kiyomoto, K. Fukushima, and T. Tanaka，“On a Fast (k,n)-Threshold Secret Sharing Scheme”，IEICE Transactions, vol. 91-A(9), pp. 2365-2378, 2008.

【発明の概要】

【発明が解決しようとする課題】

【０００５】
非特許文献１に記載されたShamirの秘密分散では計算量が大きいという課題がある。具体的には、Shamirの秘密分散では(k-1)n回の体乗算を要する。非特許文献２に記載されたXORベースの秘密分散では対応できるk，nの値が限定されており、パラメータの柔軟性が欠ける。k，nの値はセキュリティ強度とデータ容量に直結するため、柔軟に対応できることが望ましい。
【０００６】
この発明の目的は、このような点に鑑みて、任意のk，nに対応し、従来よりも計算量を低減することができる秘密分散技術を提供することである。
【課題を解決するための手段】
【０００７】
上記の課題を解決するために、この発明の秘密分散方法は、xは拡大体$GF(x^q)$を生成する既約多項式f[X]の元Xであり、n，kは2以上の整数であり、$n \geqq 2k-1$であり、p_0，…，p_{k-1}は0以上n未満の相異なる整数であり、Aは次式で定義されるn行k列の行列であり、
【０００８】
【数１】

$$A_{ij}=\begin{cases}1 & \text{if } i=j \text{ and } i<k-1\\ 0 & \text{if } i\neq j \text{ and } i<k-1\\ x^{(i-k-1)j} & \text{if } i\geq k-1\end{cases}$$

ただし、

$$i\in\{0,\ldots,n-1\},j\in\{0,\ldots,k-1\}$$

【０００９】
分散装置が、乱数r_0，…，$r_{k-2}\in GF(x^q)$を生成する乱数生成ステップと、分散装置が、乱数r_0，…，r_{k-2}と平文$s\in GF(x^q)$を要素とするベクトル$a=(r_0,\ldots,r_{k-2},s)$と行列Aとの乗算を計算することでシェアb_0，…，b_{n-1}を生成するシェア生成ステップと、復元装置が、シェアb_0，…，b_{n-1}から選択したk個のシェアb_{p0}，…，b_{pk-1}を要素とするベクトル$b'=(b_{p0},\ldots,b_{pk-1})$を生成するシェア選択ステップと、復元装置が、行列Aのp_0，…，p_{k-1}行目からなるk次正方行列の逆行列A'^{-1}を生成する逆行列生成ステップと、復元装置が、逆行列A'^{-1}のk行目とベクトルb'を乗算して平文sを復元する平文計算ステップと、を含む。
【発明の効果】
【００１０】
この発明の秘密分散技術は、任意のk，nに対応し、従来よりも計算量が低い。
【図面の簡単な説明】
【００１１】
【図１】図１は、秘密分散システムの機能構成を例示する図である。
【図２】図２は、秘密分散装置の機能構成を例示する図である。
【図３】図３は、秘密分散方法の処理フローを例示する図である。
【発明を実施するための形態】
【００１２】
実施形態の説明に先立ち、この発明の原理について説明する。
【００１３】
前提として、以下の説明では、xは既約多項式を$f[X]=X^{64}+X^4+X^3+X^2+X+1$とする拡大体$GF(2^{64})$の元Xである。xを整数表現すると2である。
【００１４】
$GF(2^{64})$は多項式を、mod 2整数を係数とする64次多項式f(x)で割った（多項式としての割り算）余りの集合である。体であり四則演算を行うことができる。特殊な演算をもつビットの64次ベクトルと考えてもよい。$GF(2^{64})$は64ビット整数で表現でき、項x^iを2^iで表現する。例えば、$1+x+x^3$は、$2^0+2^1+2^3=11$と表現できる。

【００１５】
この発明の秘密分散は、誤り訂正符号のリード・ソロモン符号（Reed-Solomon Codes）を応用して構成されたものである。リード・ソロモン符号については、例えば下記参考文献１に記載されている。
〔参考文献１〕バァナード・スカラー著、「ディジタル通信 基本と応用」、ピアソン・エデュケーション、2006年
【００１６】
誤り訂正符号の符号化処理は、平文の入力ベクトルaに線形変換（つまり行列）Aを乗じて出力ベクトルbを得る処理として、式（１）により表現できる。すなわち、行列Aのi番目の行は、出力ベクトルbのi番目の要素b_iを生成するために入力ベクトルaの各要素に乗じる係数を表す。

$$b = Aa \qquad \cdots(1)$$

【００１７】
誤り訂正符号の復号処理も線形変換と見ることができる。A', b'をA, bのうち利用するk個の要素に対応する行だけを抜き出した行列もしくはベクトルとして、式（２）により表現できる。

$$b' = A'a \qquad \cdots(2)$$

【００１８】
したがって、行列Aに逆行列が存在すれば、式（３）により復号できる。

$$a = A'^{-1}b' \qquad \cdots(3)$$

【００１９】
誤り訂正符号の符号化では、入力ベクトルaは式（４）で表されるk次のベクトルとする。ただし、kは2以上の整数である。
【００２０】
【数２】

$$\boldsymbol{a}=\begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} \qquad \cdots(4)$$

【００２１】
出力ベクトルbは式（５）で表されるn次のベクトルとする。ただし、nは2以上の整数であり、n≧2k-1である。
【００２２】
【数３】

$$\boldsymbol{b}=\begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} \qquad \cdots(5)$$

【００２３】
行列Aは、式（６）で表されるk行k列の単位行列とm行k列のファンデルモンデ行列（Vandermonde matrix）を縦に連結した行列である。ただし、m=n-kである。ファンデルモンデ行列とは、行または列の行列要素に等比数列の各項が順番にならんでいる特別な構成の行列である。
【００２４】

【数４】

$$A_{ij}=\begin{cases}1 & \text{if } i=j\\ 0 & \text{if } i\neq j \text{ and } i<k\\ x^{(i-k)j} & \text{if } i\geq k\end{cases} \quad \cdots(6)$$

ただし、

$i\in\{0,\ldots,n-1\}, j\in\{0,\ldots,k-1\}$

【００２５】

つまり、行列Aは式（７）のようなn行k列の行列である。

【００２６】

【数５】

$$\underbrace{\left(\begin{array}{ccccc}1 & 0 & 0 & \cdots & 0\\ 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 1\\ \hline 1 & 1 & 1 & \cdots & 1\\ 1 & x & x^2 & \cdots & x^{k-1}\\ 1 & x^2 & x^4 & \cdots & x^{2(k-1)}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & x^{m-1} & x^{2(m-1)} & \cdots & x^{(m-1)(k-1)}\end{array}\right)}_{k\text{列}}\begin{array}{l}\left.\begin{array}{l}\\ \\ \\ \\ \\ \end{array}\right\} k\text{行}\\ \\ \left.\begin{array}{l}\\ \\ \\ \\ \\ \end{array}\right\} m\text{行}\end{array} \quad \cdots(7)$$

【００２７】

行列Aは、k行目までは単位行列であるため、出力ベクトルbのk行目までの要素b_0，…，b_{k-1}は入力ベクトルaの要素a_0，…，a_{k-1}と一致する。出力ベクトルbにおいて入力ベクトルaの要素と一致する要素をデータシェアと呼び、それ以外の要素をパリティシェアと呼ぶ。

【００２８】

この発明の秘密分散技術は、上述した誤り訂正符号を応用して情報理論型秘密分散を構成したものである。具体的には以下のようにして情報理論型秘密分散を構成することができる。まず、情報理論型秘密分散を、誤り訂正符号と同様に、行列Aを用いた線形変換と捉える。この発明の情報理論型秘密分散の分散処理では、入力ベクトルaは、$r_0,\cdots,r_{k-2}$を乱数とし、sを平文として、式（８）で表されるk次のベクトルとする。すなわち、入力ベクトルaは、k-1行目までの要素が乱数であり、k行目の要素が平文のベクトルである。

【００２９】

【数６】

$$a=\begin{pmatrix}r_0\\ \vdots\\ r_{k-2}\\ s\end{pmatrix} \quad \cdots(8)$$

【００３０】

出力ベクトルbは、誤り訂正符号の符号化と同様であり、式（９）で表されるn次のベクトルとする。

【００３１】

【数７】

$$b=\begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} \qquad \cdots(9)$$

【００３２】

誤り訂正符号の行列Aはk行目までが単位行列であるため、情報理論型秘密分散の入力ベクトルaを乗ずると、出力ベクトルbのk行目の要素がb_{k-1}=sとなる。秘密分散では秘匿性のために平文をそのままシェアとすることは禁じられる。そのため、情報理論型秘密分散の行列Aは、式（10）で表されるように、誤り訂正符号と異なり、k-1行目までが単位行列であり、k行目からファンデルモンデ行列となる。

【００３３】

【数８】

$$A_{ij}=\begin{cases} 1 & \text{if } i=j \text{ and } i<k-1 \\ 0 & \text{if } i\neq j \text{ and } i<k-1 \\ x^{(i-k-1)j} & \text{if } i\geq k-1 \end{cases} \qquad \cdots(10)$$

ただし、

$$i\in\{0,\ldots,n-1\}, j\in\{0,\ldots,k-1\}$$

【００３４】

つまり、行列Aは式（11）のようなn行k列の行列である。

【００３５】

【数９】

$$\underbrace{\left(\begin{array}{cccccc} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \hline 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & x & x^2 & \cdots & x^{k-2} & x^{k-1} \\ 1 & x^2 & x^4 & \cdots & x^{2(k-2)} & x^{2(k-1)} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & x^m & x^{2m} & \cdots & x^{m(k-2)} & x^{m(k-1)} \end{array}\right)}_{k\text{列}} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} k-1\text{行} \\ \left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} m+1\text{行} \end{matrix} \qquad \cdots(11)$$

【００３６】

この発明の情報理論型秘密分散の復元処理では、入力ベクトルaの各要素のうちk行目の要素に設定された平文sのみを復元できればよいので、1回のk次元線形結合で復元できる。復元に利用するk個のシェアb'_0，…，b'_{k-1}に対応する行を抜き出した行列A'を生成し、その行列A'の逆行列A'^{-1}のk行目と、k個のシェアb'_0，…，b'_{k-1}からなるベクトルとの内積により平文sを求めることができる。

【００３７】

以下、この発明の実施の形態について詳細に説明する。なお、図面中において同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

【００３８】

［第一実施形態］

第一実施形態の秘密分散システムは、図１に例示するように、n（≧3）台の秘密分散装置１_0,…,１_{n-1}を含む。この実施形態では、秘密分散装置１_0,…,１_{n-1}はそれぞれ通信網２へ接続される。通信網２は、接続される各装置が相互に通信可能なように構成された回

線交換方式もしくはパケット交換方式の通信網であり、例えばインターネットやLAN（Local Area Network）、WAN（Wide Area Network）などを用いることができる。なお、各装置は必ずしも通信網２を介してオンラインで通信可能である必要はない。例えば、秘密分散装置1_i（$i\in\{0,\cdots,n-1\}$）へ入力する情報を磁気テープやUSBメモリなどの可搬型記録媒体に記憶し、その可搬型記録媒体からオフラインで入力するように構成してもよい。

【００３９】

秘密分散装置１は、図２に例示するように、シェア記憶部１０、入力部１１、乱数生成部１２、行列生成部１３、シェア生成部１４、シェア選択部１５、逆行列生成部１６、および平文計算部１７を含む。この秘密分散装置１が、図３に例示する各ステップの処理を行うことにより第一実施形態の秘密分散方法が実現される。

【００４０】

秘密分散装置１は、例えば、中央演算処理装置（CPU: Central Processing Unit）、主記憶装置（RAM: Random Access Memory）などを有する公知又は専用のコンピュータに特別なプログラムが読み込まれて構成された特別な装置である。秘密分散装置１は、例えば、中央演算処理装置の制御のもとで各処理を実行する。秘密分散装置１に入力されたデータや各処理で得られたデータは、例えば、主記憶装置に格納され、主記憶装置に格納されたデータは必要に応じて中央演算処理装置へ読み出されて他の処理に利用される。秘密分散装置１の各処理部は、少なくとも一部が集積回路等のハードウェアによって構成されていてもよい。

【００４１】

秘密分散装置１の備えるシェア記憶部１０は、例えば、RAM（Random Access Memory）などの主記憶装置、ハードディスクや光ディスクもしくはフラッシュメモリ（Flash Memory）のような半導体メモリ素子により構成される補助記憶装置、またはリレーショナルデータベースやキーバリューストアなどのミドルウェアにより構成することができる。

【００４２】

図３を参照して、第一実施形態の秘密分散方法の処理手続きを説明する。

【００４３】

秘密分散方法は分散処理と復元処理とに分かれる。分散処理および復元処理は、n台の秘密分散装置1_0，…，1_{n-1}から任意に選択された1台の秘密分散装置1_i（$i\in\{0,\cdots,n-1\}$）のみが実行する。分散処理を実行する秘密分散装置と復元処理を実行する秘密分散装置は同一の装置であってもよいし、異なる装置であってもよい。以降の説明では、分散処理を行う秘密分散装置を分散装置と呼び、復元処理を行う秘密分散装置を復元装置と呼ぶ。

【００４４】

ステップＳ１１において、分散装置の入力部１１へ平文$s\in GF(x^q)$が入力される。平文sはシェア生成部１４へ送られる。

【００４５】

ステップＳ１２において、分散装置の乱数生成部１２は、k-1個の乱数r_0，…，$r_{k-2}\in GF(x^q)$を生成する。乱数r_0，…，r_{k-2}はシェア生成部１４へ送られる。乱数生成部１１は、逐一ランダムに乱数生成器を用いてk-1個の乱数r_0，…，r_{k-2}を生成してもよいし、事前に生成されメモリに格納されている複数個の値から所定の規則に従ってk-1個の値を選択して乱数r_0，…，r_{k-2}を生成してもよい。

【００４６】

ステップＳ１３において、分散装置の行列生成部１３は、式（12）で定義されるn行k列の行列Aを生成する。行列Aはシェア生成部１４へ送られる。行列Aはn，kが定まれば計算できるため、あらかじめ生成しておいてもよい。その場合、行列生成部１３は、あらかじめ生成し記憶しておいた行列Aを読み込むだけでよい。

【００４７】

【数１０】

$$A_{ij}=\begin{cases}1 & \text{if } i=j \text{ and } i<k-1\\ 0 & \text{if } i\neq j \text{ and } i<k-1\\ x^{(i-k-1)j} & \text{if } i\geq k-1\end{cases} \quad \cdots(12)$$

ただし、

$$i\in\{0,\ldots,n-1\}, j\in\{0,\ldots,k-1\}$$

【００４８】

ステップＳ１４において、分散装置のシェア生成部１４は、k次ベクトルa=(r_0，…，r_{k-2}，s)を生成し、ベクトルaと行列Aとの乗算を計算することでn次ベクトルb=(b_0，…，b_{n-1})を求める。ベクトルbの0番目からk-2番目の要素b_0，…，b_{k-2}には、乱数r_0，…，r_{k-2}がそのまま設定される。ベクトルbの残りの要素b_{k-1}，…，b_{n-1}には、m=n-kとし、i=0，…，m-1について式（13）を計算して得られる値c_0，…，c_{m-1}がそれぞれ設定される。

【００４９】

【数１１】

$$c_i=\sum_{0\leq j<k-1} r_j x^{ij}+sx^{i(k-1)} \quad \cdots(13)$$

【００５０】

シェア生成部１４は、ベクトルbの各要素をn個のシェアb_0，…，b_{n-1}として生成し、n台の秘密分散装置1_0，…，1_{n-1}へそれぞれ分散して送信する。シェアb_iを受信した秘密分散装置1_iは、シェアb_iをシェア記憶部１０へ記憶する。

【００５１】

以上で分散処理は完了となる。続いて復元処理を説明する。

【００５２】

ステップＳ１５において、復元装置のシェア選択部１５は、利用可能な任意のk個のシェアb_{p0}，…，b_{pk-1}を取得し、k次ベクトルb'=(b_{p0}，…，b_{pk-1})を生成する。ただし、p_0，…，p_{k-1}は復元に用いるシェアの番号であり、0以上n未満の整数から選択したk個の相異なる整数である。ベクトルb'は平文計算部１７へ送られる。p_0，…，p_{k-1}は逆行列生成部１６へ送られる。

【００５３】

ステップＳ１６において、復元装置の逆行列生成部１６は、行列Aのp_0，…，p_{k-1}行目を抜き出したk次正方行列を生成し、その逆行列A'^{-1}を計算する。逆行列A'^{-1}は平文計算部１７へ送られる。

【００５４】

ステップＳ１７において、復元装置の平文計算部１７は、逆行列A'^{-1}のk行目とベクトルb'=(b_{p0}，…，b_{pk-1})を乗算して、平文sを復元する。

【００５５】

Shamirの秘密分散では分散処理における乗算数が(k-1)nである。本形態の秘密分散システムでは分散処理における乗算数が(k-1)(n-k+1)である。したがって、本形態の秘密分散システムによれば秘密分散の計算量を低減することができる。

【００５６】

［第二実施形態］

a，b∈GF(2^{64})の乗算は、2つの63次多項式a，b（式（14））を掛けてから64次多項式fで割る操作である（式（15））。このとき、λ次の項の係数は式（16）となる。

【００５７】

【数１２】

$$a=\sum_{1<64}a_i x^i, b=\sum_{1<64}b_i x^i \quad \cdots(14)$$

$$\sum_{i<64}\sum_{j<64}a_i b_j x^{i+j} \bmod f \quad \cdots(15)$$

$$\oplus_{i+j=\lambda} a_i b_j \quad \cdots(16)$$

【００５８】

式（15）において、126次多項式をmod fして63次多項式にする処理をリダクションと呼ぶ。リダクションは、式（17）の同値関係を用いて処理する。

$f=x^{64}+x^4+x^3+x+1=0 \bmod f$ …（17）

【００５９】

式（17）を変形すると、式（18）に示すように64次項を4次式に落とす関係となる。

$x^{64}=x^4+x^3+x+1 \bmod f$ …（18）

【００６０】

式（19）に示すように、64次以上の項もすべて60次次数を下げられる。

$x^{64+n}=x^n(x^4+x^3+x+1) \bmod f$ …（19）

【００６１】

126次多項式を、63次多項式gと62次多項式hを用いて、式（20）のように表すことができる。

$g+x^{64}h=g+(x^4+x^3+x+1)h \bmod f$ …（20）

【００６２】

ある任意の要素aとx+1との乗算(x+1)aは、式（21）で表すことができる。

【００６３】

【数１３】

$$xa+a=xa\oplus a \quad \cdots(21)$$

【００６４】

また、$x^n a$はaの各項がn次高い項となるので、整数表現における2^n倍、もしくはnビット左シフトと等価である。したがって、式（22）のように表すことができる。

【００６５】

【数１４】

$$(x^4+x^3+x+1)h=(h<<4)\oplus(h<<3)\oplus(h<<1)\oplus h \quad \cdots(22)$$

【００６６】

hは62次多項式であるため、式（22）の

【００６７】

【数１５】

$$(h<<4)\oplus(h<<3)$$

【００６８】

は64次以上の多項式となり、再度次数を下げる必要がある。64次以上の部分は式（23）のようになる。

【００６９】

【数１６】

$$x^4(h_{62}x^{62}+h_{61}x^{61}+h_{60}x^{60})+x^3(h_{62}x^{62}+h_{61}x^{61})$$

$$=x^{64}((h>>60)\oplus(h>>61)) \quad \cdots(23)$$

【００７０】

64ビット整数内では64ビットを超えたビットは切り捨てられることを考慮すると、式（24）を計算すればよい。

【００７１】

【数１７】

$$x^{64}(h \oplus (h >> 60) \oplus (h >> 61))$$
$$= (x^4 + x^3 + x + 1)(h \oplus (h >> 60) \oplus (h >> 61))$$
$$= (x^3 + 1)(x + 1)(h \oplus (h >> 60) \oplus (h >> 61)) \quad \cdots(24)$$

【００７２】

乗算の際、片方が61ビット以内のとき（より正確には両方のビット数を足して125以下のとき）、式（25）が成り立つため、リダクションを効率化できる。

【００７３】

【数１８】

$$(h >> 60) \oplus (h >> 61) = 0 \quad \cdots(25)$$

【００７４】

したがって、リダクションまで含めて考えると、61ビット数で1ビットだけが立っている数、つまり0≦i≦60の範囲での2^iとの乗算は高速である。

【００７５】

この発明の秘密分散ではファンデルモンデ行列を用いてパリティシェアを生成する。ベクトルaをa=(a_0，…，a_{k-1}∈GF(x^q))と表すと、パリティシェアは式（26）により計算される。ただし、GF(x^q)は既約多項式f[X]により生成され、拡大次数をqとする拡大体である。xは既約多項式f[X]の元であり、f[X]=Xである。

【００７６】

【数１９】

$$\sum_{0 \le j < k} a_j x^{ij} \quad \cdots(26)$$

【００７７】

このとき、体がサイズの大きな拡大体のときには効率化ができる。既約多項式fのうち、最高次項を除いた多項式をf'とする。多項式f'の最高次項の次数をdとする。すると、(m-1)(k-1)≦q-dを満たすとき、乗算が以下のように通常よりも簡単になる。

【００７８】

iがq未満のとき、$x^i = X^i$である。入力aを式（27）とすると、多項式乗算の結果は、式（28）となる。

【００７９】

【数２０】

$$\sum_{j<q} a_j X^j \quad \cdots(27)$$

$$aX^i = \left(\sum_{j<q} a_j X^j\right) X^i \quad \cdots(28)$$

【００８０】

ここで次数がq次以上となるので、f≡0⇔X^q≡-f'を用いて、fによる剰余をとる。つまり、aX^iのうちq次未満の部分をg、q次以上の部分をX^qで割った多項式hとおくと、aX^i≡g-hf'と表される。拡大体乗算では通常、このような次数削減をg-hf'がq-1次となるまで繰り返す。このときiがq-d以下だと、aX^iの次数はたかだかq-1+q-d≡2q-d-1であり、hの次数はたかだかq-d-1となる。f'がd次多項式なので、hf'の次数はたかだかq-1となり、次数削減が1回で済む。

【００８１】

ステップＳ１４において、以下のように構成することで、より効率的に計算することが可能となる。なお、(m-1)(k-1)≦q-dが成り立つものとする。

【００８２】

ステップＳ１４において、分散装置のシェア生成部１４は、i∈{0，…，m-1}について、式（29）により値c_iを計算する。

【００８３】

【数２１】

$$c_i = \sum_{0 \le j < k-1} r_j x^{ij} + s x^{i(k-1)} \qquad \cdots(29)$$

【００８４】

値c_iのq次以上の部分をX^qで割った多項式h_iと、値c_iのq次未満の部分である多項式g_iとを生成する。この多項式h_iと多項式g_iとを用いて、$g_i - h_i f'$を計算し、値c_iを更新する。こうして求めた値c_0，…，c_{m-1}をベクトルbの要素b_{k-1}，…，b_{n-1}とする。

【００８５】

第二実施形態の分散方法では、$(m-1)(k-1) \leqq q-d$が成り立つため、すべての体乗算においてリダクションが1回で済むようになっている。そのため、リダクションを含めた乗算の処理量が低減する。

【００８６】

［第三実施形態］

第二実施形態では、$(m-1)(k-1) \leqq q-d$が成り立つ必要があった。第三実施形態では、$(m-1)(k-1) \leqq q-d$を満たさない場合でも体乗算の処理量を低減するように拡張する。

【００８７】

ステップＳ１４において、分散装置のシェア生成部１４は、$j \in \{0, \cdots, k-1\}$について、$a'_j = a_j$とする。また、$d_j = 0$とする。その後、$i \in \{0, \cdots, m-1\}$について、式（30）により値c_iを計算する。

【００８８】

【数２２】

$$c_i = \sum_{0 \le j < k} a'_j x^{ij-d_j} \qquad \cdots(30)$$

【００８９】

値c_iのq次以上の部分をX^qで割った多項式h_iと、値c_iのq次未満の部分である多項式g_iとを生成する。この多項式h_iと多項式g_iとを用いて、$g_i - h_i f'$を計算し、値c_iを更新する。そして、$i \in \{0, \cdots, m-1\}$，$j \in \{0, \cdots, k-1\}$について、$i \neq m-1$、かつ、$(i+1)j - d \geqq q-d$であれば、$a'_j := a'_j x^{\alpha}$，$d_j := d_j + \alpha$と更新する。ここで、αはq-d以下の正の整数である。こうして求めた値c_0，…，c_{m-1}をベクトルbの要素b_{k-1}，…，b_{n-1}とする。

【００９０】

第三実施形態では、第二実施形態ほどには処理量の削減はできないが、適切なαを設定すれば、十分高速化に有効である。

【００９１】

誤り訂正符号では入力をそのままシェアとすることができるが、秘密分散では入力をそのままシェアとすることができない。逆に、秘密分散であっても乱数をそのままシェアとしてもよい。この発明のポイントは、これらの点を考慮して、安全性を担保しながら演算を省いたことにある。

【００９２】

この発明は上述の実施形態に限定されるものではなく、この発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。上記実施形態において説明した各種の処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【００９３】

［プログラム、記録媒体］

上記実施形態で説明した各装置における各種の処理機能をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

【００９４】

この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録

しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等どのようなものでもよい。

【００９５】

また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

【００９６】

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

【００９７】

また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

【符号の説明】

【００９８】

１　秘密計算装置
１０　シェア記憶部
１１　入力部
１２　乱数生成部
１３　行列生成部
１４　シェア生成部
１５　シェア選択部
１６　逆行列生成部
１７　平文計算部

【要約】　（修正有）
【課題】任意のk,nに対応し、計算量を低減する秘密分散方法を提供する。
【解決手段】乱数生成部１２が、乱数$r_0,\cdots,r_{k-2}\in GF(x^q)$を生成する。シェア生成部１４が、乱数$r_0,\cdots,r_{k-2}$と平文$s\in GF(x^q)$を要素とするベクトル$a=(r_0,\cdots,r_{k-2},s)$と行列Aとの乗算を計算することでシェア$b_0,\cdots,b_{n-1}$を生成する。シェア選択部１５が、シェア$b_0,\cdots,b_{n-1}$から選択したk個のシェア$b_{p0},\cdots,b_{pk-1}$を要素とするベクトル$b'=(b_{p0},\cdots,b_{pk-1})$を生成する。逆行列生成部１６が、行列Aの$p_0,\cdots,p_{k-1}$行目からなるk次正方行列の逆行列$A'^{-1}$を生成する。平文計算部１７が、逆行列$A'^{-1}$のk行目とベクトルb'を乗算して平文sを復元する。
【選択図】図２

【図１】

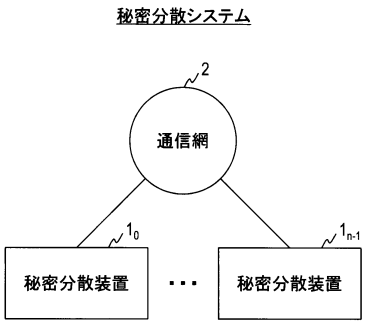

図1

【図２】

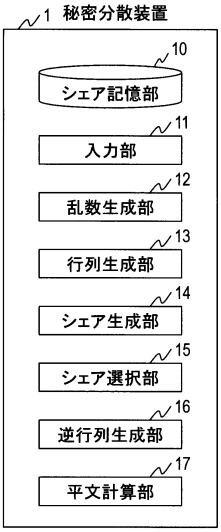

図2

【図３】

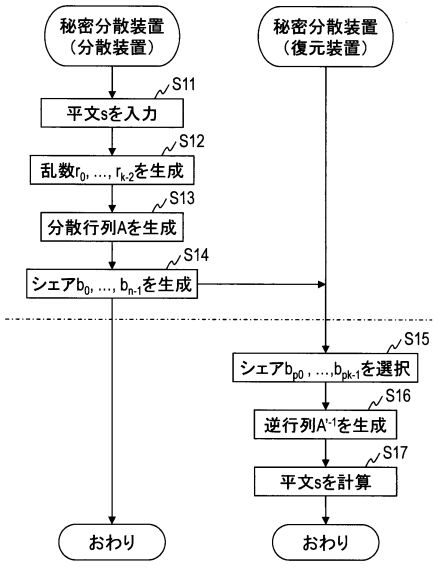

図3

フロントページの続き

(56)参考文献 特許第５９１８８８４（ＪＰ，Ｂ１）
特開２０１４－２１２３７（ＪＰ，Ａ）
蓑輪正，安全性と信頼性を両立した分散ストレージシステムの提案，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，２０１１年１１月１１日，Vol．111，No．309，pp．19-24
山嵜彰一郎，他，組織Ｒｅｅｄ－Ｓｏｌｏｍｏｎ符号を用いた秘密分散法とその応用について，電子情報通信学会技術研究報告，日本，一般社団法人電子情報通信学会，２０１４年 3月 3日，Vol．113，No．484，pp．215-220
川島千種，他，多重符号化を利用した階層的な秘密分散法の検討，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，２００７年 8月３１日，Vol．107，No．209，pp．17-23
五十嵐大，他，ＳＨＳＳ：オブジェクトストレージ向けの超高速秘密分散ライブラリ，情報処理学会研究報告，日本，情報処理学会，２０１５年 6月２５日，Vol．2015-CSEC-70，No．26，pp．1-8

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／００－ ９／３８